



Bewustwordingsinstrumenten informatiebeveiliging en privacy

*Onderzoek naar de beschikbare instrumenten voor bewustwording van
onderwijzend en onderwijskundig personeel in relatie tot het normenkader
informatiebeveiliging en privacy voor het funderend onderwijs*

29 FEBRUARI 2024

Inhoudsopgave

	Pagina
1. Inleiding	4
Een beschrijving van de context en aanleiding voor dit onderzoek.	
2. Aanpak	8
De vraagstelling van de opdrachtgever, afbakening van het onderzoek, de aanpak en het vervolgproces	
3. Normenkader IBP FO	14
Een korte toelichting op het normenkader en bewustwording binnen het normenkader en beschrijving van de relevante normen	
4. Resultaten	22
Een overzicht van de resultaten binnen de processtappen van het onderzoek	
5. Conclusies en aanbevelingen	38
Conclusies en aanbevelingen op basis van de resultaten van het onderzoek	

Managementsamenvatting

Informatiebeveiliging en privacy zijn randvoorwaardelijk voor de verdere digitalisering van het onderwijs. Het is dan ook van groot belang dat schoolbesturen zorgen voor een digitale veilige schoolomgeving. Het Programma Digitaal Veilig Onderwijs heeft Berenschot gevraagd te onderzoeken welke bewustwordingstools-, testen en –diensten (hierna: instrumenten) aanwezig zijn en in hoeverre dit aansluit bij het Normenkader Informatiebeveiliging en Privacy voor het Funderend Onderwijs (hierna: Normenkader IBP FO).

In dit onderzoek heeft Berenschot met input van de schoolbestuurders, informatiebeveiligings- en privacyfunctionarissen, experts op het gebied van bewustwording binnen en buiten de onderwijssector en leveranciers van instrumenten in kaart gebracht welke instrumenten er aanwezig zijn voor bewustwording op het gebied van informatiebeveiliging en privacy, hoe dit op een effectieve manier ingezet kan worden en of dit voldoende is om invulling te geven aan het Normenkader IBP FO.

Uit het onderzoek blijkt dat er veel verschillende instrumenten beschikbaar zijn in de markt in allerlei categorieën. Het simpelweg inkopen van een enkel instrument en deze inzetten, maakt echter niet dat voldaan wordt aan de eisen van het normenkader. Buiten de specifieke normen die vragen om een inhoudelijke verdieping van de bewustwording, vraagt het Normenkader IBP FO om een continu bewustwordingsprogramma. Dit betekent dat bewustwording een doorlopend proces voor schoolbesturen is en dat in de

loop van de tijd een spectrum van interventies ingezet moeten worden. Bovendien hebben de geïnterviewde experts duidelijk uiteengezet dat alleen het vergroten van de kennis niet zal leiden tot de gewenste gedragsverandering. Het is ook nodig dat er voldoende gelegenheid en motivatie is om het gewenste gedrag te kunnen vertonen.

Kortom, bewustwording met als doel om tot informatieveilig gedrag te komen, vraagt om een continu proces, met daarbij interventies zowel gericht op het bieden van kennis over informatiebeveiliging en privacy als het krijgen van de gelegenheid om dit toe te kunnen passen en het vinden van de motivatie hiervoor. Een visuele weergave van dit proces vindt u [hier](#).

Tot slot blijkt uit het onderzoek dat schoolbesturen behoefte hebben aan meer ondersteuning op het gebied van bewustwording van het belang van een digitaal veilige schoolomgeving. Zowel vanuit de bestuurders als vanuit de informatiebeveiligings- en privacyfunctionarissen is meermaals gedurende het onderzoek de wens geuit om te zorgen voor meer kennisdeling op dit gebied binnen de sector. Zowel in de vorm van handreikingen en het beschikbaar stellen van (overzichten van) instrumenten vanuit de overkoepelende organisaties als het ministerie van OCW, de PO-Raad en de VO-raad, Sivo en Kennisnet, als in de vorm van een kennisplatform waarop bijvoorbeeld ervaringen en bewustwordingscampagnes met elkaar uitgewisseld kunnen worden.



1. Inleiding

Inleiding

Het goed regelen van de informatiebeveiliging en privacy is voor veel organisaties een omvangrijke en ingewikkelde klus, zo ook voor onderwijsinstellingen in het primair en voortgezet onderwijs. De digitalisering heeft bovendien een enorme vlucht genomen door COVID-19. De afhankelijkheid van veilige, betrouwbare en toekomstbestendige dienstverlening is daarmee evenredig toegenomen. Tegelijkertijd nemen de risico's in de digitale omgeving toe.

Informatiebeveiliging en privacy zijn randvoorwaardelijk voor de verdere digitalisering van het onderwijs. Het is dan ook van groot belang dat schoolbesturen zorgen voor een digitaal veilige schoolomgeving. Om de schoolbesturen hierin te ondersteunen hebben het ministerie van Onderwijs, Cultuur en Wetenschap (OCW), Kennisnet, Sivon, de PO-Raad en de VO-raad de handen ineengeslagen middels het programma Digitaal Veilig Onderwijs.

In 2023 heeft het programma Digitaal Veilig Onderwijs het Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs (Normenkader IBP FO) opgesteld als een duidelijke richtlijn voor besturen binnen het funderend onderwijs. De implementatie van dit normenkader bij onderwijsinstellingen gaat bijdragen aan de gewenste digitaal veilige

schoolomgeving. In de komende jaren gaat het programma Digitaal Veilig Onderwijs schoolbesturen ondersteunen bij het implementeren van het Normenkader IBP FO.

Voorliggend rapport is een stap in die ondersteuning van het programma Digitaal Veilig Onderwijs. Belangrijk onderdeel van het Normenkader IBP FO is immers dat schoolbesturen geëquipeerd zijn om het bewustzijns- en het kennisniveau van hun medewerkers te meten en om deze, indien nodig, te kunnen verhogen. Om bestuurders daarbij te helpen, heeft het programma Digitaal Veilig Onderwijs aan Berenschot gevraagd een onderzoek te doen naar bewustwordingstools, -testen en -diensten (hierna: instrumenten) voor onderwijzend en onderwijsondersteunend personeel (hierna: OOP).



Vraagstelling

Doel van dit onderzoek is het in kaart brengen van de reeds aanwezige mogelijkheden die er zijn om het bewustzijn van OOP te vergroten. Als basis voor bewustwording gelden de normen uit het Normenkader IBP FO.

De hoofdvraag van het onderzoek, geformuleerd door het programma Digitaal Veilig Onderwijs is:

'In hoeverre sluit het huidige aanbod van bewustwordingstools, -testen en -diensten (instrumenten) aan bij de eisen van het Normenkader IBP FO?'

Daarnaast heeft het programma de volgende subvragen opgesteld:

1. Welke categorieën instrumenten zijn er al beschikbaar in de markt en bij publieke partijen?
2. Hoe verhouden deze beschikbare instrumenten zich tot het Normenkader IBP FO en tot elkaar?
3. Wat mist er nog in het huidige aanbod?



Wat is bewustwording?

De Van Dale zegt over bewustwording:

be·wust·wor·ding (de; v) **1** het inzicht krijgen in een situatie

Dit laat zien hoe breed het begrip bewustwording is. Binnen de kaders van dit onderzoek definiëren we bewustwording dan ook bewust breed:

Bewustwording gaat om alle activiteiten die bijdragen aan het inzicht geven om gewenst gedrag op het gebied van informatiebeveiliging en privacy te vertonen

Bewustwording beperkt zich daarmee niet tot alleen tot de inzet van instrumenten. In het rapport zult u terugzien dat experts ook breder naar het begrip kijken dan dat. De landschapsanalyse die we maakten richt zich daar wel primair op, in lijn met de vraagstelling. In de conclusies en aanbevelingen kijken we vanuit de brede blik naar het onderwerp, omdat de kracht van laagdrempelige bewustwording juist ook ligt in die bredere context van het begrip.





2. Aanpak

Onderzoeksaanpak

Voor de uitvoering van dit onderzoek is een aanpak in vijf stappen toegepast. De onderzoeksactiviteiten zijn uitgevoerd in drie delen. Dit hoofdstuk beschrijft per deel de aanpak in meer detail.



NB: Voor de uitvoering van dit onderzoek is gebruik gemaakt van een relatief kleine steekproef bestaande uit experts, leveranciers, bestuurders en deelnemers aan de vragenlijst. De steekproef is om die reden beperkt representatief. De resultaten van dit onderzoek kunnen niet worden geïnterpreteerd als een volledig representatieve weergave van de werkelijkheid.

Deel 1. Normen en landschapsanalyse

Om de normen voor bewustwording in het Normenkader IBP nadere duiding te geven, hebben we gesprekken gevoerd met vier experts uit het IBP-netwerk van het funderend onderwijs. De gesprekken waren gericht op het in beeld brengen en vaststellen van de eisen voor bewustwording op het gebied van digitale veiligheid bij onderwijzend en onderwijsondersteunend personeel in het funderend onderwijs. We zijn onder andere ingegaan op de betekenis van bewustwording en welke eisen daarbij horen.

Een selectie van de vragen die aan de **experts uit het IBP-netwerk** zijn voorgelegd:

- *Wat betekent bewustwording op het gebied van informatiebeveiliging en privacy voor u?*
- *In hoeverre is dat veranderd door het normenkader?*
- *Wat zijn voor u de belangrijkste aspecten als het gaat om bewustwording?*
- *Welke tools, testen en diensten heeft u in de afgelopen jaren ingezet?*

Documentstudie

Publiek beschikbare bronnen vormden de basis voor de landschapsanalyse. Deze bronnen zijn gevonden door in eerste instantie

via verschillende zoekmachines een overzicht te creëren van de meest voorkomende instrumenten. Door zoektermen te gebruiken zoals 'bewustwordingstools informatiebeveiliging', 'bewustwordingsinstrumenten privacy', 'informatiebeveiliging onderwijs' of 'programma digitaal veilig onderwijs' is een beeld ontstaan van het landschap van beschikbare instrumenten.

Vervolgens hebben we op basis van de gevonden instrumenten verder gezocht. Een voorbeeld van een gebruikte zoekterm is 'informatiebeveiliging phishingsimulaties'. Door verder te zoeken op de gevonden instrumenten werd duidelijk welke variaties van deze instrumenten er bestaan. Bovendien leidden deze zoektermen naar websites met meer informatie over bestaande instrumenten, waardoor we het overzicht nog verder konden aanvullen.

Resultaat

De uitkomsten van de documentstudie en de gesprekken met de vier experts uit het IBP-netwerk, aangevuld met de kennis van de onderzoekers, resulteerde in een zo compleet mogelijk overzicht van bestaande bewustwordingsinstrumenten.

Deel 2. Verdiepende gesprekken met experts en leveranciers

Experts

Deel 2 van dit onderzoek bestond uit interviews met zes experts om het overzicht van instrumenten uit de landschapsanalyse aan te vullen. Deze experts zijn afkomstig uit verschillende disciplines. Twee experts zijn zelf ook leverancier van bewustwordingsinstrumenten. Deze hebben we gesproken vanuit hun brede expertise binnen de onderwijssector op dit gebied. Drie van de geïnterviewde experts richten zich vanuit de psychologie op gedragsverandering en de toepassing van bewustwordingsinstrumenten op het gebied van informatiebeveiliging en privacy, al dan niet in het onderwijs.

Dit is de selectie van de vragen die aan de experts zijn voorgelegd:

- *Bewustwording wordt weleens het fundament van informatiebeveiliging en privacy genoemd, in hoeverre bent u het hiermee eens?*
- *Het uiteindelijke doel van bewustwording is (vaak) om gedragsverandering te bewerkstelligen. Op welke wijze kan een school voor gedragsverandering bij medewerkers zorgen op het gebied van informatiebeveiliging en privacy?*
- *Hoe bepaal je de effectiviteit van de bewustwording? Welke indicatoren bieden inzicht? Hoe kun je meten of dat wat je doet ook het gewenste effect heeft?*

Leveranciers

Naast experts hebben we ook vijf vertegenwoordigers van leveranciers van bewustwordingsinstrumenten geïnterviewd om de landschapsanalyse aan te scherpen. Deze vertegenwoordigers zijn werkzaam voor bedrijven die bewustwordingsinstrumenten ontwikkelen en/of aanbieden.

Twee van de geïnterviewden zijn werkzaam bij een leverancier die zich specifiek richt op het onderwijs en drie bij leveranciers die ook tools, testen en diensten voor andere sectoren leveren.

Hierbij een selectie van de vragen die aan de leveranciers zijn gesteld:

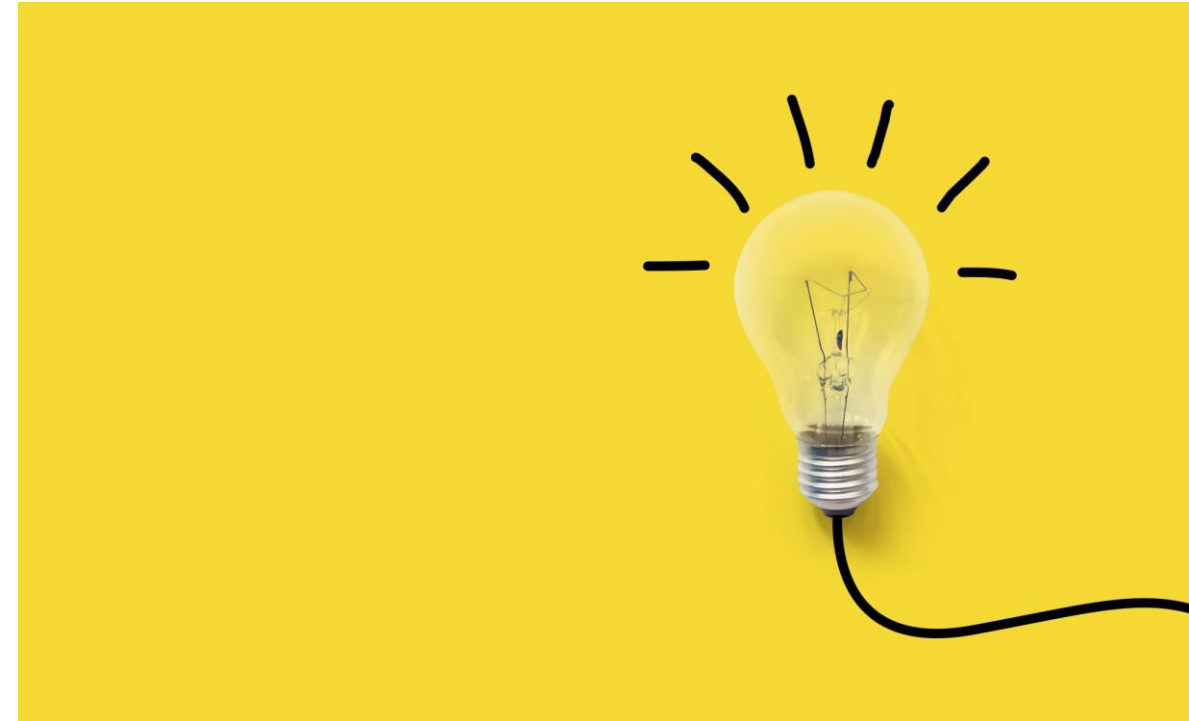
- *Kunt u meer vertellen over uw instrument(en) gericht op bewustwording van informatiebeveiliging en privacy?*
- *In welke sectoren bent u actief en in hoeverre bent u bekend met de sector onderwijs?*
- *Wat maakt uw instrument(en) effectief?*
- *Hoe reageren klanten op uw instrument(en)?*

Deel 3. (a) Invullen vragenlijst door experts uit het IBP-netwerk

In dit deel van het onderzoek zijn experts uit het IBP-netwerk uitgenodigd om een vragenlijst in te vullen. Het doel van deze vragenlijst was om meer informatie in te winnen over de wijze waarop scholen invulling geven aan de bewustwording. Het doel was ook om het overzicht van bewustwordingsinstrumenten in de landschapsanalyse te valideren en compleet te maken, door te inventariseren welke instrumenten men kent en welke men nog mist.

Een selectie van de vragen die aan de **experts** zijn voorgelegd:

- *Welke van de volgende typen instrumenten voor bewustwording op het gebied van digitale veiligheid heeft u wel eens gebruikt?*
- *Geef aan in hoeverre u het eens bent met de volgende stelling: 'de gebruikte typen instrumenten hebben positief bijgedragen aan de bewustwording op het gebied van digitale veiligheid bij onderwijsondersteunend en onderwijzend personeel.'*
- *Hoeveel uur is acceptabel om van onderwijzend en onderwijsondersteunend personeel te vragen voor bewustwordingsactiviteiten op jaarbasis?*



Deel 3: (b) Validatiegesprekken met bestuurders

De volgende stap na de vragenlijst voor experts uit het IBP-netwerk was het voeren van validatiegesprekken met bestuurders. Een belangrijk doel van deze gesprekken was om een beeld te vormen van de mate waarin en de manier waarop schoolbesturen al werken aan het bevorderen van bewustwording. Daarnaast hadden de gesprekken als doel om op te halen in hoeverre bestuurders behoefte hebben aan en gebruik maken van ondersteunende bewustwordingsinstrumenten. Aanvullend is bestuurders gevraagd op welke manier een overzicht hiervan hen het beste kan helpen om bewustwording onder onderwijzend en onderwijsondersteunend personeel te bevorderen.

Een selectie van de vragen die aan de **bestuurders** zijn voorgelegd:

- *Hebben er binnen uw schoolbestuur in de afgelopen drie jaar bewustwordingsactiviteiten plaatsgevonden? Zo ja, welke?*
- *Welke van de gebruikte instrumenten heeft u als effectief ervaren?*
- *Hoeveel tijd heeft onderwijzend en onderwijsondersteunend personeel jaarlijks voor bewustwordingsactiviteiten? Welke tijdsinvestering vindt u passend hiervoor voor uw medewerkers?*



Normenkader informatiebeve en privacy

3. Normenkader IBP FO

voor het Funderend Onderwijs

Normenkader IBP FO

In het funderend onderwijs werkt men veel met persoonsgegevens. Een deel hiervan is extra privacy gevoelig, omdat het hier gaat om de gegevens van een minderjarige doelgroep. Het is belangrijk dat er goed wordt omgegaan met deze informatie. Dit valt onder de verantwoordelijkheid van schoolbesturen en hun medewerkers.

Het [Normenkader Informatiebeveiliging en Privacy voor het Funderend Onderwijs](#) is een initiatief van het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad. Het biedt handvatten voor schoolbestuurders, schoolleiders en IBP'ers om hun informatiebeveiliging te versterken en de bescherming van persoonsgegevens te verbeteren. Het bestaat momenteel uit 69 normen die schoolbesturen inzicht geven in de maatregelen die nodig zijn voor een zo goed mogelijke informatiebeveiliging. De normen voor privacy zijn hierin nog niet opgenomen en maken dus geen (expliciet) onderdeel uit van dit onderzoek. Wel wordt bewustzijn op het gebied van privacy in algemene zin meegenomen, met de AVG als kader.

De **69 normen** in het normenkader zijn op de volgende manier beschreven:

- 1. Beschrijving van de normen.** Voor elke norm wordt toegelicht waarom deze belangrijk is.
- 2. Toetsingskader.** Dit kader bestaat uit punten die samen het minimumniveau vormen waar de sector en schoolorganisaties naartoe werken.
- 3. Voorbeeldmaatregelen.** Voor de normen worden een aantal activiteiten en toepassingen voorgesteld waarmee een schoolbestuur aan het toetsingskader kan voldoen.

Voorbeeldpagina uit het normenkader

Deel 1 Normenkader informatiebeveiliging

Deel 2 Normenkader privacy

 Begrippenlijst

1.1 Strategie

NORM

GO.01

Een strategie en visie op informatie- en cybersecurity is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging.

Waarom doen we dit?

Het hebben van een strategie leidt tot gepaste zakelijke en beveiligingsbeslissingen, tot samenhang in beveiligingsbeslissingen en tot een passend antwoord op veranderingen in de bedrijfsomgevingen.

TOETSINGSKADER

- Strategie en visie zijn goedgekeurd door het bevoegd gezag.
- Strategie en missie worden actief gecommuniceerd naar medewerkers, leveranciers en businesspartners.

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft een strategie en visie geformuleerd op informatiebeveiliging en cybersecurity. De opbouw van deze strategie en visie bevat de elementen die aangereikt worden in de Handreiking Strategie en Visie vanuit het ondersteuningsaanbod. Er kan gebruikgemaakt worden van het Format Strategie en Visie.
2. Het bevoegd gezag heeft de strategie en visie vastgesteld.
3. De strategie en visie zijn (digitaal) beschikbaar, bijvoorbeeld via de website en het intranet.

Bewustwording binnen het Normenkader IBP FO

Bewustwording komt op verschillende wijzen terug binnen het normenkader IBP FO. De meest duidelijke wijze is de norm 4.6 over veiligheidsbewustzijn:

HR.06

Er is een bewustwordingsprogramma om gebruikers bewust te maken van hun verantwoordelijkheid om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie (middelen) te beschermen.

Waarom doen we dit?

Door medewerkers duidelijk te instrueren over hun verantwoordelijkheden met betrekking tot informatiebeveiliging, kunnen zij effectief bijdragen aan het beperken van informatiebeveiligingsrisico's.

TOETSINGSKADER

- Er is een security awareness-programma opgenomen in het informatiebeveiligingsplan en dit wordt organisatiebreed uitgevoerd.
- Het programma is in lijn met (informatie)beveiligingsbeleid.

Uit deze norm blijkt dat bewustwording een continu proces is waar elke medewerker en dus ook elke OOP mee in aanraking dient te komen. Met andere woorden, een eenmalige actie voor bewustwording is onvoldoende om op dit punt te voldoen.

Minder expliciet komt bewustwording naar voren in norm 11.12, waarin staat dat medewerkers zich bewust moeten zijn van beleid om malware-aanvallen te voorkomen, en in norm 4.5 die zich richt op kennis en vaardigheden die nodig zijn bij specifieke systemen.

Impliciet zit bewustwording echter verweven door het hele normenkader, doordat een belangrijke factor bij informatiebeveiliging in meer generieke zin de 'human factor' is. Uiteindelijk zijn de meeste incidenten te herleiden tot menselijk handelen (bewust dan wel onbewust). Dit is dan ook de reden dat vanuit het informatiebeveiligingsbeleid hier expliciet aandacht voor moet zijn en in het ondersteuningsproduct hiervoor vanuit Kennisnet het volgende is opgenomen:

"5.4 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de FG, en de Security Officer met het bestuur als eindverantwoordelijke."

Op de volgende pagina's is uitgewerkt welke andere normen direct een doelgroep binnen OOP raken en daarmee vanuit die implicietere factor relevant zijn voor bewustwording van de doelgroep.

Specifieke normen onderwijzend personeel

In deze paragraaf staat beschreven welke normen een (direct) effect (zouden moeten) hebben op de bewustwording van de doelgroep onderwijzend personeel. Daarmee bedoelen we de normen die aandacht behoeven in bewustwordingsprogramma's voor deze doelgroep.

Kenmerkend voor deze personen is dat ze in aanraking komen met gegevens van leerlingen en vanuit dat perspectief moeten weten op welke wijze zij veilig om moet gaan met persoonsgegevens. Die gegevens kunnen ook medische informatie bevatten. Verder gebruiken deze personen relatief weinig bijzondere applicaties, maar ze hebben wel de rechten om gebruik te kunnen maken van applicaties als het leerlingvolgsysteem. Ze hebben echter in principe alleen toegang tot die informatie die zij voor het werk nodig hebben, maar ze hebben geen beheerrechten.

Een bijzonder aspect voor het onderwijzend personeel is dat zij een voorbeeldrol hebben richting leerlingen voor wat betreft het veilig omgaan met gegevens. Ook geldt dat een deel van deze groep graag innoveert en vanuit dit perspectief handvatten nodig heeft om veilig te innoveren met digitale middelen.

- Norm 1.1 Strategie: strategie en visie dienen uitgedragen te worden naar medewerkers.
- Norm 1.2 Beleid: het informatiebeveiligingsbeleid moet bekend zijn bij medewerkers en dit moet onderdeel zijn van het bewustwordingsprogramma.
- Norm 3.2 Risicobeoordeling: medewerkers moeten begrijpen dat afwegingen op informatiebeveiliging plaatsvinden op basis van risicomanagement
- Norm 4.5 Kennisdeling: het op peil houden van kennis en vaardigheden van alle eindgebruikers van systemen om zo veilig gebruik te bevorderen.
- Norm 6.1 Incident management: elke medewerker moet op de hoogte zijn van het proces en weten wanneer en hoe incidenten gemeld moeten worden.
- Norm 7.1 Change management: medewerkers dienen te begrijpen dat wijzigingen conform een proces worden doorlopen en hierdoor wijzigingen meer tijd kunnen kosten dan voorheen.
- Norm 9.2 Classificatie: elke medewerker moet bekend zijn met het dataclassificatieschema en de classificatierichtlijnen.

Specifieke normen onderwijzend personeel

- Norm 9.5 Uitwisseling van (gevoelige) gegevens: ook onderdeel van 1.2 Beleid, maar gezien de hoeveelheid persoonsgegevens binnen scholen, en de uitwisseling met niet alleen ouders, maar ook mogelijke hulpinstanties, van wezenlijk belang voor medewerkers.
- Norm 9.6 Verwijdering van data: van groot belang voor onderwijzend personeel wanneer devices aan leerlingen worden uitgeleend in de klas.
- Norm 10.1 Toegangsrechten: gericht op generieke bewustwordingsaspect van veilig omgaan met wachtwoorden en begrip hebben voor de eisen die aan wachtwoorden worden gesteld.
- Norm 11.3 Mobiele apparaten en telewerken: kennis van wat er verwacht wordt van medewerkers bij telewerken en mobiele apparaten.
- Norm 12.1 Fysieke beveiligingsmaatregelen: begrijpen als medewerker hoe je zelf bijdraagt aan de fysieke beveiliging van je organisatie.



Specifieke normen onderwijsondersteunend personeel

In deze paragraaf staat beschreven welke normen een effect (zouden moeten) hebben op de bewustwording van de doelgroep onderwijsondersteunend personeel. Onderwijsondersteunend personeel is een breed begrip voor alle medewerkers binnen scholen die op enige wijze ondersteunend zijn aan het primaire proces. Het is daarmee een meer gedifferentieerde groep dan het onderwijzend personeel. Onder de doelgroep vallen bijvoorbeeld onderwijsassistenten, administratief medewerkers en conciërges. We laten hierbij de (veelal) bovenschoolse bedrijfsvoeringsmedewerkers als HR-medewerkers, inkopers en IT-medewerkers buiten beschouwing. Het Normenkader IBP heeft wel directe invloed ook op deze bedrijfsvoeringsmedewerkers. Mogelijk is niet voor elke school of elk schoolbestuur deze indeling gelijk aan de praktijk. Voor dit onderzoek is de scope echter de onderwijsondersteunende medewerker op schoolniveau.

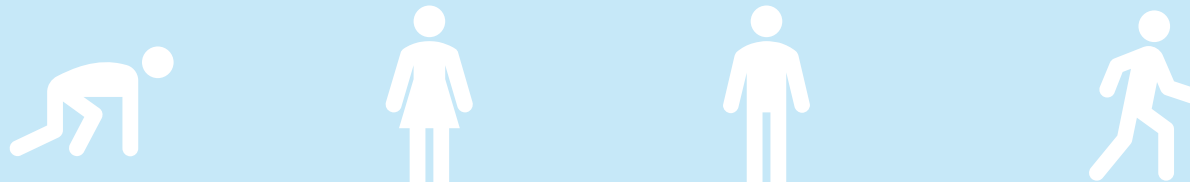
De onderwijsondersteunende medewerker verwerkt in bepaalde gevallen, zoals de administratief medewerker, grotere hoeveelheden persoonsgegevens van leerlingen en ook persoonsgegevens van medewerkers. Een orthopedagoog op een school heeft toegang tot medische gegevens van leerlingen, of in elk geval gezondheidsgegevens. Daarnaast is een rol als conciërge bijvoorbeeld verschillend van aard

ingericht binnen scholen. In de ene school heeft de conciërge meer aandacht voor de fysieke beveiliging van een schoolgebouw, maar bij een andere school is het van belang dat een conciërge juist de toegang heeft tot veel medische informatie van leerlingen in verband met het helpen bij het innemen van medicatie. Dit maakt het lastig om een eenduidig passend beeld te geven. Op hoofdlijnen gelden de hierna uitgewerkte normen als specifiek voor deze doelgroep.

- Norm 1.1 Strategie: strategie en visie dienen uitgedragen te worden naar de medewerkers.
- Norm 1.2 Beleid: het informatiebeveiligingsbeleid moet bekend zijn bij de medewerkers en dit moet onderdeel zijn van het bewustwordingsprogramma.
- Norm 3.2 Risicobehoedeling: medewerkers moeten begrijpen dat afwegingen op het gebied van informatiebeveiliging plaatsvinden op basis van risicomanagement
- Norm 4.2 Certificering, training en scholing: met name voor medewerkers met beheerrechten dient aandacht te zijn voor training, zodat zij in staat zijn op de juiste wijze met applicaties om te gaan en zo incidenten te voorkomen.

Specifieke normen onderwijsondersteunend personeel

- Norm 4.4 Verandering of beëindiging van de functie: kennisoverdracht bij cruciale plekken moet eigenlijk al voor er sprake is van vertrek vanzelfsprekend zijn, zodat ook bij uitval van medewerkers door anderen het werk overgenomen kan worden. Dit is met name op functies met meer IT-rechten dan standaard van belang.
- Norm 4.5 Kennisdeling: het op peil houden van kennis en vaardigheden van alle eindgebruikers van systemen om zo veilig gebruik te bevorderen.
- Norm 6.1 Incidentmanagement: elke medewerker moet op de hoogte zijn van het proces en weten wanneer en hoe incidenten gemeld moeten worden.
- Norm 7.1 Change management: medewerkers dienen te begrijpen dat wijzigingen conform een proces worden doorlopen en hierdoor het aanbrengen van wijzigingen meer tijd kunnen kosten dan voorheen.
- Norm 9.2 Classificatie: elke medewerker moet bekend zijn met het dataclassificatieschema en de classificatierichtlijnen.
- Norm 9.5 Uitwisseling van (gevoelige) gegevens: ook onderdeel van 1.2 Beleid, maar gezien de hoeveelheid persoonsgegevens binnen scholen, en de uitwisseling met niet alleen de ouders, maar ook met mogelijke hulpinstanties, van wezenlijk belang voor de medewerkers.
- Norm 10.1 Toegangsrechten: gericht op generieke bewustwordingsaspect van veilig omgaan met wachtwoorden en begrip hebben voor de eisen die aan wachtwoorden worden gesteld.
- Norm 10.3 Superusers: zij vormen feitelijk een aparte doelgroep binnen deze doelgroep waarbij aandacht moet zijn voor veilig gebruik binnen de extra autorisaties die zij hebben binnen een systeem.
- Norm 11.3 Mobiele apparaten en telewerken: kennis van wat er verwacht wordt van medewerkers bij telewerken en mobiele apparaten.
- Norm 12.1 Fysieke beveiligingsmaatregelen: begrijpen als medewerker hoe je zelf bijdraagt aan de fysieke beveiliging van je organisatie.



Specifieke normen medewerkers met een IBP-rol

Naast de normen voor onderwijzend en onderwijsondersteunend personeel, zijn er nog enkele normen die direct van invloed zijn op de werkzaamheden van een medewerker met een IBP-rol. Deze normen zijn daarom geen herhaling van de normen zoals vermeld op de voorgaande pagina's. Het gaat hier puur en alleen om de extra de normen die betrekking hebben op deze groep medewerkers met een IBP-rol.

- 2.1 Eigenaarschap, rollen en verantwoordelijkheden: voor de IBP-er moet duidelijk zijn hoe de governance in elkaar steekt en wat dit betekent voor zijn of haar eigen rol (bevoegdheden, verantwoordelijkheden en taken).
- 3.1 Raamwerk voor informatierisicomanagement: de IBP-er moet in staat zijn dit raamwerk toe te passen en hierin getraind zijn (dit heeft effect op de uitvoering van norm 3.2 en 3.3 (risicobeoordeling en behandeling / beperking van risico's).
- Norm 6.1 Incidentmanagement: in aanvulling op onderwijzend en onderwijsondersteunend personeel, dient de IBP-er ook getraind te zijn in de wijze waarop afhandeling van een incident dient plaats te vinden. Dit heeft mede effect op de uitvoering van norm 6.2 en 6.3 (incident escalatie en incident response).
- Norm 9.3 Beveiligingseisen voor datamanagement: de IBP-er moet in voorkomende gevallen in staat zijn op basis van het beleid de beveiligingseisen toe te passen binnen de school.
- Norm 12.1 Fysieke beveiliging: de IBP-er moet in staat zijn te toetsen of de fysieke beveiliging conform beleid is en weten dat bij bijvoorbeeld de inzet van cameratoezicht de handreiking cameratoezicht moet worden toegepast. Ook dient de IBP-er mogelijk bij wijzigingen op het gebied van huisvesting te adviseren over de te nemen maatregelen op het gebied van fysieke beveiliging.
- Norm 14.1 Bedrijfscontinuïteitsmanagement: de IBP-er moet op de hoogte zijn van het bedrijfscontinuïteitsplan binnen de school op basis van de plannen op bestuursniveau.
- 14.5 Crisismanagement: op basis van de inhoud van de plannen op het gebied van crisismanagement, kan een training over crisismanagement ook onderdeel uitmaken van de IBP-rol.



4. Resultaten

Resultaten

In dit hoofdstuk gaan we uitgebreid in op de resultaten van dit onderzoek. De resultaten zijn verkregen op basis van de stappen die in Hoofdstuk 2 – Aanpak vermeld staan.

Deel 1: landschapsanalyse, waarbij in beeld is gebracht wat er beschikbaar is aan bewustwordingsinstrumenten op het gebied van informatiebeveiliging en privacy.

Deel 2: interviews met experts en leveranciers, om de landschapsanalyse aan te vullen en te verifiëren.

Deel 3 (a): invullen vragenlijst door experts uit het IBP-netwerk, om meer informatie te ontvangen over de wijze waarop scholen invulling geven aan bewustwording en om het overzicht van bewustwordingsinstrumenten in de landschapsanalyse te valideren.

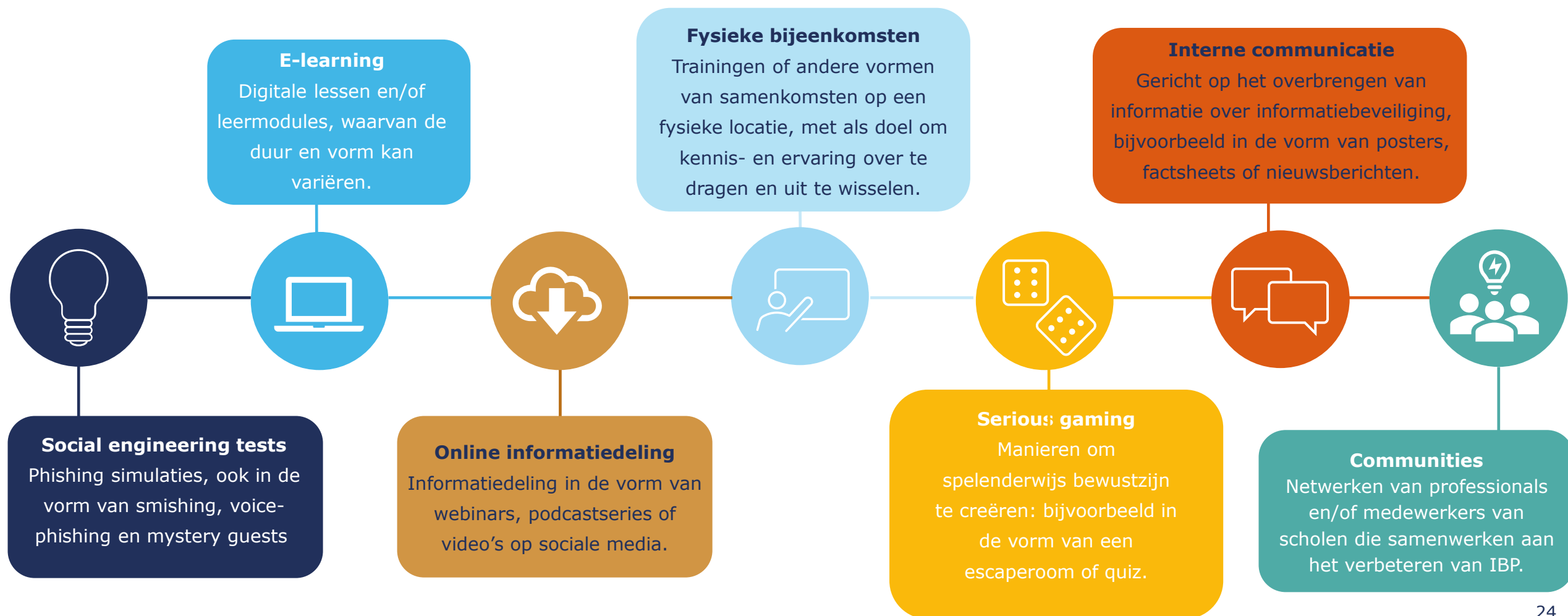
Deel 3 (b): validatiegesprekken met bestuurders, om inzicht te krijgen in de mate waarin en de manier waarop schoolbesturen al werken aan het bevorderen van bewustwording.

In dit hoofdstuk is per stap van het onderzoek beschreven welke resultaten de onderzoeksactiviteiten opleverden. Aan het eind van dit hoofdstuk benoemen we de rode draden van al deze resultaten als opmaat naar de conclusies en aanbevelingen.



Resultaten landschapsanalyse

Om de beschikbare bewustwordingsinstrumenten in kaart te brengen is een landschapsanalyse uitgevoerd. De documentstudie op basis van publiek beschikbare bronnen, de kennis van de onderzoekers en gesprekken met experts en leveranciers leidden tot een overzicht van het huidige aanbod. De verschillende typen instrumenten zijn ingedeeld in de volgende zeven categorieën.



Overzicht bewustwordingsinstrumenten

In de volgende illustratie geven we een korte nadere duiding welk specifiek type instrument ingedeeld is in welk van de zeven categorieën.



Resultaten verdiepende gesprekken met experts en leveranciers

De landschapsanalyse is in de loop van het onderzoek verder aangevuld met bevindingen uit de gesprekken met vijf experts op het gebied van IBP en met vijf leveranciers van bewustwordingsinstrumenten. De interviewleidraad bestond uit vragen die gerelateerd zijn aan de definitie van bewustwording, de manier waarop gedrag beïnvloed kan worden om bewustwording te bevorderen en zowel de ervaring met als de effectiviteit van de inzet van bewustwordingsinstrumenten. In deze paragraaf hebben we de belangrijkste bevindingen uit deze gesprekken weergegeven.

Voor wat betreft de **definitie van bewustwording** blijkt dat de meerderheid van de geïnterviewden van mening is dat bewustwording niet een einddoel moet zijn. Geïnterviewden geven aan dat het slechts een middel is om (informatie)veilig gedrag te bewerkstelligen. Hierbij wordt benoemd dat dit gedrag pas gerealiseerd kan worden als aan drie aspecten wordt voldaan.

- 1. Capaciteit (kennis en ervaring).** De mate waarin medewerkers op basis van kennis en ervaring begrijpen waarom het belangrijk is om veilig te handelen op het gebied van informatiebeveiliging en privacy.
- 2. Motivatie.** De mate waarin medewerkers zich bewust zijn van het belang van veilig handelen en om die reden ook daadwerkelijk zo willen handelen (daarvoor ook intrinsiek gemotiveerd zijn).
- 3. Gelegenheid.** De mate waarin medewerkers gefaciliteerd worden (zo goed mogelijk de gelegenheid krijgen en hebben) om veilig gedrag te vertonen en daar zelf de kansen voor zien.

Deze drie aspecten zijn onderdeel van [het COM-B model](#) van gedragsverandering. Het model is ontwikkeld door Britse wetenschappers en wordt veel gebruikt door de experts die we spraken. Een goede toepassing van dit model zie je ook terug in de zorg: het programma '[Informatieveilig gedrag in de zorg](#)'.

Resultaten verdiepende gesprekken met experts en leveranciers

Ook wordt een aantal keer benoemd dat bij het inzetten van instrumenten om veilig gedrag rondom informatiebeveiliging en privacy te bewerkstelligen, de eerste stap zou moeten zijn om te bepalen welk(e) aspect(en) beïnvloed moet(en) worden. Soms ontbreekt het aan het aspect gelegenheid, maar is er wel genoeg capaciteit en is de motivatie aanwezig bij de medewerkers. Een voorbeeld hiervan is een blauwe papierbak voor het veilig weggooien van (vertrouwelijke) informatie die is geplaatst aan het eind van een doodlopende gang, waar medewerkers nauwelijks komen. Een interventie kan dan zijn om deze papierbak op een plek dichtbij en meer in het zicht van medewerkers te plaatsen, zoals in de docentenkamer.

Tijdsbesteding

De antwoorden over de tijdsbesteding, die volgens experts en leveranciers minstens nodig is om bewustwording bij OOP op peil te houden, lopen uiteen. De tekst in het blauwe kader licht dit in meer detail toe.

IBP-tijdsbesteding per medewerker

Alle geïnterviewden geven aan dat het aantal uren dat medewerkers per jaar (zouden moeten) besteden aan bewustwording op het gebied van informatiebeveiliging en privacy afhankelijk is van een aantal factoren. De volgende factoren werden genoemd:

- Het IBP-volwassenheidsniveau van de school.
- De urgentie bij het schoolbestuur om het onderwerp IBP op de agenda te zetten.

Op sommige scholen wordt er een dagdeel per jaar besteed aan bewustwording, terwijl dit op andere scholen meer ad hoc georganiseerd is en (nog) niet in uren per jaar te kwantificeren is. De antwoorden variëren van twee uren tot twee dagen per medewerker per jaar om IBP onder de aandacht te houden van de medewerkers.

Resultaten verdiepende gesprekken met experts en leveranciers

Aansluiten op doelgroep is belangrijk voor positief effect

Bewustwordingsinstrumenten zijn volgens het merendeel van de geïnterviewden effectief als deze goed aansluiten bij de belevingswereld van medewerkers. Dit kan bijvoorbeeld bereikt worden door het inzetten van 'ambassadeurs' binnen afdelingen of teams, die het nut en de noodzaak van IBP kunnen uitdragen op een manier die past bij de cultuur en de werkvorm van de betreffende afdeling of het team.

Ook kan het helpen om bij het werken aan bewustwording op het gebied van IBP gebruik te maken van leermomenten van medewerkers, zoals situaties waarin (al dan niet gemelde) datalekken zijn ontstaan. Deze leermomenten kunnen tijdens trainingen of e-learnings anoniem gepresenteerd worden als casus. Een realistische, echt gebeurde casus helpt om beter te begrijpen waarom het belangrijk is om veilig te handelen. Hiermee wordt het bewustzijn vergroot.

Herhaaldelijke inzet van instrumenten van belang

De instrumenten moeten volgens de meeste geïnterviewden herhaaldelijk worden ingezet binnen een organisatie. Het eenmalig inzetten achten zij minder effectief voor het duurzaam veranderen van gedrag. Door meerdere keren in een jaar instrumenten in te zetten wordt volgens de geïnterviewden het bewustzijn en de kennis van de medewerkers op IBP-gebied continu onderhouden en is de kans groter dat zij veilig omgaan met gevoelige informatie.

Goed voorbeeldgedrag door leidinggevenden essentieel

Goed voorbeeldgedrag is volgens een aantal geïnterviewden onmisbaar. Het gaat hier met name om managers, bestuurders en andere leidinggevenden in een organisatie die de keuze maken om bewustwordingsinstrumenten in te zetten. Volgens de geïnterviewden is dit van essentieel belang om medewerkers gemotiveerd te houden zelf ook (informatie)veilig gedrag te vertonen. Het helpt als leidinggevenden veilig gedrag stimuleren en hieraan aandacht besteden in bijvoorbeeld teamoverleggen. De geloofwaardigheid en het effect van regels en afspraken over IBP op school neemt volgens de geïnterviewden af als leidinggevenden dit weinig of niet serieus nemen.

IBP als vast onderwerp van gesprek in de gehele organisatie

De dialoog over IBP moet volgens een groot deel van de geïnterviewden een vast onderdeel zijn tijdens zowel teamvergaderingen en studiedagen als bij het koffiezetapparaat en in de wandelgangen. Door hier integraal aandacht aan te besteden, worden inzichten gedeeld en gaat IBP leven in de organisatie. Het delen van kennis en ervaring en het bewust aangaan van het gesprek met OOP leidt tot veiliger gedrag. Het gesprek kan op meerdere manieren op gang worden gebracht: door posters op te hangen, trainingen te geven en/of door een platform te organiseren waarin (al dan niet op speelse wijze of in wedstrijdvorm) de voortgang van de organisatie of medewerkers gemonitord kan worden.

Resultaten verdiepende gesprekken met experts en leveranciers

Inzetten op een combinatie van instrumenten

Het is volgens het merendeel van de geïnterviewden belangrijk om een mix van bewustwordingsinstrumenten in te zetten bij de versterking van de IBP-bewustwording. Als bijvoorbeeld een postercampagne gecombineerd wordt met een e-learning of training kan de effectiviteit vergroot worden. Instrumenten kunnen een versterkend effect hebben op elkaar. Als medewerkers een e-learning hebben gevolgd en er is op school een poster of infographic zichtbaar met de kernboodschappen uit de lesstof, zal dit sneller blijven hangen.

Positieve benadering van medewerkers

Een aantal geïnterviewden benoemt dat het belangrijk is dat medewerkers positief worden benaderd tijdens IBP-activiteiten. Instrumenten worden interessanter om te volgen als medewerkers de benadering als positief en motiverend ervaren.

Slimme inzet van e-learning

De meerderheid van de geïnterviewde leveranciers biedt e-learnings aan. Zij geven aan dat e-learning slim ingezet kan worden door deze op te bouwen met zeer korte lessen of modules (van maximaal 3 minuten) die worden herhaald gedurende het jaar. Daarbij is het belangrijk dat de korte lessen of modules op elkaar aansluiten. Als bijvoorbeeld een module gaat over het belang van tweestapsverificatie en hoe dit

ingesteld kan worden, is het slim om in de eerstvolgende module een vraag op te nemen waarin aan de deelnemer wordt gevraagd: 'Heeft u al een tweestapsverificatie voor toegang tot uw email ingesteld?'.

Starten met het in beeld brengen van het IBP-volwassenheidsniveau van de organisatie

Omdat instrumenten het beste werken als ze aansluiten bij een organisatie, is het volgens een aantal experts en leveranciers belangrijk om eerst het IBP-volwassenheidsniveau van een organisatie in beeld te brengen. Dit kan bijvoorbeeld door het uitvoeren van een nulmeting waarin duidelijk wordt waar de organisatie staat ten opzichte van de doelstellingen op het gebied van IBP.

Het belang van handelen versus het kennisniveau van medewerkers

De meerderheid van de geïnterviewden benadrukt dat het, bij de ontwikkeling van e-learning of een methode voor een nulmeting, met name van belang is om na te gaan hoe medewerkers handelen op IBP-gebied. Inzicht in de manier waarop medewerkers zich gedragen op dit vlak is volgens hen belangrijker informatie dan het kennisniveau van IBP-gerelateerde definities en termen.

Resultaten verdiepende gesprekken met experts en leveranciers

Duidelijke taal

Volgens het merendeel van de geïnterviewden kan jargon op het gebied van informatiebeveiliging en privacy het beste worden vermeden, ook door medewerkers die deze jargontaal goed kennen en regelmatig in hun werkzaamheden gebruiken. Het is belangrijk dat iedereen in een organisatie gesprekken over IBP kan begrijpen, het spreken van dezelfde (zo simpel mogelijke) taal helpt daarbij.

Effectiviteit van phishingsimulaties

De experts verschillen van inzicht als het gaat om de effectiviteit van phishingsimulaties. Een aantal van hen benoemt dat phishingsimulaties alleen tijdelijk effectief kunnen zijn of als de uitkomsten van een simulatie direct worden opgevolgd, bijvoorbeeld door een module van een e-learning te tonen als er op de link wordt geklikt. Anderen geven aan phishingsimulaties over het algemeen als niet effectief te zien. Redenen hiervoor zijn volgens hen dat medewerkers phishingsimulaties op een negatieve manier kunnen ervaren, als 'toets' waar men voor moet slagen. Zij geven aan dat phishingsimulaties als effect kunnen hebben dat medewerkers (tijdelijk) banger zijn om in de 'val' te trappen van een simulatie dan in de 'val' van een echte phishingmail.



Resultaten vragenlijst IBP-netwerk

Onder experts uit het IBP-netwerk is een vragenlijst verspreid om informatie op te halen over de wijze waarop scholen invulling geven aan bewustwording en om het overzicht van bewustwordingsinstrumenten completer te maken. Deze vragenlijst is in totaal door 29 respondenten ingevuld.

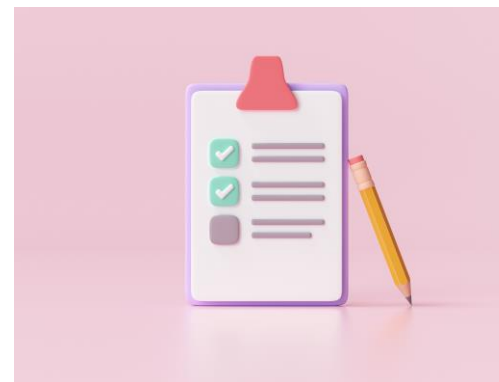
Kenmerken van de respondenten

24% van de respondenten is werkzaam voor een klein schoolbestuur (1-4 instellingen onder bestuur), 52% van de respondenten is werkzaam voor een middelgroot schoolbestuur (5-20 instellingen onder bestuur), en ook 24% van de respondenten is werkzaam voor een groot schoolbestuur (>20 instellingen onder bestuur).

De vragenlijst is ingevuld door IBP'ers (21%), IT-managers (21%), FG's (14%), IT-specialisten (7%) en een CISO (3%). De overige respondenten (34%) geeft aan een andere functie te vervullen. Onder deze groep vallen bijvoorbeeld beleidsmedewerkers, privacy officers en bestuurssecretarissen.

Voor het grootste deel van de respondenten geldt dat het schoolbestuur voorziet in voortgezet onderwijs (65%) en/of primair onderwijs (52%). 21% van de respondenten geeft aan dat de organisatie waar zij werkzaam zijn ook voorziet in speciaal voortgezet onderwijs en 14% ook in speciaal primair onderwijs.

Volgend op de vragen over de functies van de respondenten en het type school waar zij voor werken, is er gevraagd of de respondenten in de afgelopen drie jaar bewustwordingsactiviteiten hebben uitgevoerd. Indien de vraag werd beantwoord met 'nee', werd de vragenlijst direct afgesloten. Voor de respondenten die 'ja' hebben geantwoord werden verdere vragen zichtbaar over de inzet van tools, testen en diensten. 31% van de respondenten gaf aan in de afgelopen drie jaar geen bewustwordingsactiviteiten te hebben uitgevoerd. Voor 69%, oftewel twintig respondenten, was dit wel het geval.



Resultaten vragenlijst IBP-netwerk

Inzet van bewustwordingsactiviteiten

De respondenten konden over de volgende instrumenten aangeven of ze deze hebben ingezet en of ze deze als positief en effectief hebben ervaren:

1. Phishingtesten en simulaties
2. Medewerkersbijeenkomsten (denk aan: voorlichting tijdens een teamvergadering)
3. Online informatiedeling (denk aan: podcasts, webinars, YouTube-filmpjes)
4. Interne communicatiemiddelen (denk aan: posters, nieuwsbrieven, stickers, muismatjes, intranetberichten)
5. Serious gaming
6. Eenmalige e-learning
7. Terugkerende e-learning

Vrijwel alle respondenten geven aan gebruik te hebben gemaakt van medewerkersbijeenkomsten, en achten deze ook effectief. Interne communicatiemiddelen zijn ook door vrijwel alle respondenten ingezet, waarvan een zeer klein deel aangeeft dit niet effectief te vinden.

Phishingtesten en –simulaties zijn door ongeveer de helft van de respondenten ingezet en worden door vrijwel iedereen als effectief ervaren. Online informatiedeling wordt ook door ongeveer de helft ingezet, waarvan het overgrote merendeel dit instrument effectief acht.

Zowel eenmalige als terugkerende e-learnings worden door weinig respondenten gebruikt, maar worden door de gebruikers hiervan wel als effectief ervaren. Serious gaming wordt door geen van de respondenten ingezet.

Bewustwordingsactiviteiten nieuwe medewerkers

De respondenten is ook gevraagd of nieuwe medewerkers bewustwordingsactiviteiten moeten uitvoeren als zij op een school komen werken. De helft van de respondenten geeft aan bewustwordingsinstrumenten in te zetten voor nieuwe medewerkers, waarbij het voornamelijk gaat om AVG-trainingen of een e-learning.

Bepalende aspecten in besluit bewustwordingsactiviteiten

Ook is aan de respondenten gevraagd welke aspecten zij meenemen in het besluit over welke bewustwordingsactiviteiten ingezet worden. Hierbij geven alle respondenten aan dat tijdsbesteding voor medewerkers een belangrijk aspect is. De meesten geven aan dat de effectiviteit van de activiteiten meespelen, ook geeft het overgrote deel aan dat kosten en kwaliteit een belangrijke rol spelen in de overweging, en iets meer dan de helft geeft aan dat ook de tijdsbesteding voor implementatie en/of voorbereiding van de activiteit meespeelt.

Resultaten vragenlijst IBP-netwerk

Tijdsbesteding

Ook is in de vragenlijst gevraagd naar het aantal uur dat acceptabel wordt gevonden om op jaarbasis te vragen van onderwijzend en onderwijsondersteunend personeel voor bewustwordingsactiviteiten. De antwoorden hierop lopen erg uiteen. Voor onderwijzend personeel geldt dat van de respondenten iets minder dan de helft aangeeft dat dit minder dan vijf uur moet zijn. Voor onderwijsondersteunend personeel loopt het aantal uren iets op, maar nog steeds vindt iets meer dan de helft dat dit niet meer dan tien uur moet zijn. Er zijn echter ook uitschieters (40 uur voor onderwijzend personeel en 80 uur voor onderwijsondersteunend personeel) en een aantal respondenten geeft aan dat het afhankelijk is van bijvoorbeeld de prioriteit en het budget die de activiteiten krijgen.

Aspecten die een bewustwordingsinstrument nuttig maken

Ook de antwoorden die ingevuld worden bij de vraag over welke aspecten een instrumenten nuttig maken, lopen uiteen. Twee keer wordt benoemd dat de activiteit herhaaldelijk moet worden ingezet. Ook wordt vier keer aangegeven dat de activiteit kortdurend moet zijn. Tot slot wordt vier keer te kennen gegeven dat de activiteit zo concreet mogelijk moet zijn en gericht op de praktijk.

Wat is er nodig om bewustwording de aandacht te geven die vanuit het Normenkader IBP gevraagd wordt?

Ook hebben we gevraagd wat de respondenten nodig hebben om bewustwording de aandacht te geven op de wijze die in het normenkader staat aangegeven: deze vraag werd gesteld in de vorm van een open vraag. 'Budget' wordt hier drie keer genoemd en 'tijd' wordt vijf keer genoemd. Daarbij valt het op dat de respondenten aangeven dat ze behoefte hebben aan bijvoorbeeld een overzicht van effectieve bewustwordingsactiviteiten die kunnen worden ingezet, bijvoorbeeld vanuit de overheid of Kennisnet. Ook hulpmiddelen en richtlijnen bij het inzetten van de activiteiten zijn gewenst. Een enkele respondent geeft aan het fijn te vinden als er landelijk bewustwordingsinstrumenten aangeboden worden die schoolbesturen in kunnen zetten.

Resultaten validatiegesprekken bestuurders

Om het overzicht van bewustwordingsinstrumenten in de landschapsanalyse te valideren en compleet te maken, en ook de andere bevindingen uit het onderzoek te toetsen, zijn we in gesprek gegaan met vijf schoolbestuurders. Deze gesprekken gaven meer inzicht in het daadwerkelijk gebruik van bestaande bewustwordingsinstrumenten en van wat er nog mist. Op deze slide wordt toegelicht hoe de gesproken bestuurders denken over de instrumenten die zij inzetten en hoe zij hierop kunnen reflecteren.

Phishingsimulaties. De reacties hierop zijn wisselend: ze kunnen effectief zijn, maar een risico kan zijn dat medewerkers zich in de maling genomen voelen.

Kennissessies en fysieke bijeenkomsten. Het organiseren van een specifieke bijeenkomst of kennissessie op school (al dan niet een externe spreker die op een inspirerende manier kort en bondig de kern van IBP in de praktijk toelicht), draagt volgens bestuurders bij aan de bewustwording bij de medewerkers. Hierbij is het volgens hen van belang om zo goed mogelijk aan te sluiten bij de belevingswereld van de doelgroep.

Nulmetingen. Verschillende schoolbestuurders geven aan dat een extern bureau is ingeschakeld om het volwassenheidsniveau op het gebied van IBP in kaart te brengen, zodat op basis van de resultaten verdere activiteiten ondernomen kunnen worden, onder meer op het gebied van bewustwording.

Brochures. Het uitdelen van brochures met concrete handvatten wordt wel genoemd als optie door bestuurders, maar de bestuurders hebben geen sterke mening over de effectiviteit ervan.

Digitale toetsen en e-learning. Toetsen voor (nieuwe) medewerkers om op een bepaald IBP-kennisniveau te komen, worden door een enkeling ingezet. Hier is geen sterke mening over naar voren gekomen.

De bestuurders noemen **concrete stappen** die ze hebben gezet om de school digitaal veiliger te maken. Voorbeelden zijn de digitalisering van het papieren archief, het nemen van technische maatregelen om toegang tot applicaties en authenticatie te verbeteren en het bewuster omgaan met privacygevoelige informatie en hier afspraken over maken (zoals publicatie van schoolfoto's).

Resultaten validatiegesprekken bestuurders

Ook hebben we met de bestuurders gesproken over welke ruimte zij zien om met bewustwording aan de slag te gaan. Hierbij zijn we verder ingegaan op wat bewustwordingsinstrumenten effectief maken. Ook hebben we gesproken over het budget en de tijd die schoolbesturen voor dit thema vrijmaken, de invloed van het normenkader en over de aanwezigheid van dit thema in de opleidingen.

Effectiviteit van bewustwordingsinstrumenten

Meerdere bestuurders benadrukken dat het inzetten van instrumenten alleen niet voldoende is om veilig gedrag te bewerkstelligen. Ze geven hierbij aan dat ze pas effectief worden als medewerkers doorhebben dat het een belangrijk thema is: schoolbestuurders moeten dus **duidelijk communiceren** over het belang en uitleggen waarom ze bepaalde maatregelen treffen.

Ook geven meerdere schoolbestuurders aan dat bewustwordingsinstrumenten aan moeten sluiten bij de **belevingswereld** van onderwijzend personeel. Zij zijn hoofdzakelijk bezig met het primair proces, en technische taal en het normenkader staat hier ver vanaf. In plaats hiervan zou aangesloten kunnen worden bij zaken als bijvoorbeeld de veiligheid van (gegevens van) leerlingen.

Tot slot geeft een van de schoolbestuurders aan dat instrumenten pas werken als deze een **persoonlijke benadering** hanteren: een berichtje op het intranet wordt niet gelezen, terwijl het wél werkt om het erover te hebben tijdens bijvoorbeeld teamoverleggen. Daarbij moet informatiebeveiliging en privacy volgens meerdere bestuurders **positief** worden benaderd, het benadrukken van fouten roept slechts weerstand op.

Investeringsen

De geïnterviewde bestuurders geven aan dat zij een bedrag voor digitaal onderwijs budgetteren. Hier vallen de thema's informatiebeveiliging en privacy onder. De vraag hoeveel budget er daadwerkelijk naar dit thema gaat, vinden de schoolbestuurders al lastig te beantwoorden, laat staan dat men dit kan inschatten voor het realiseren van specifiek bewustwording.



Resultaten validatiegesprekken bestuurders

Bewustwording van informatiebeveiliging en privacy begint al in opleidingen

Meerdere geïnterviewde bestuurders geven aan dat het belangrijk is dat al in de lerarenopleiding aandacht besteed wordt aan informatiebeveiliging en privacy. Daarbij wijzen zij erop dat veel bestuurders weinig tot geen ervaring hebben met informatiebeveiliging en privacy. Hiervoor zou in de opleidingsprogramma's voor bestuurders dan ook meer aandacht moeten zijn.

Invloed publicatie van het normenkader op de dagelijkse praktijk

De publicatie van het normenkader IBP FO brengt volgens een aantal bestuurders bij OOP weinig teweeg, omdat zij zich voornamelijk bezighouden met het primaire proces. Eén van de bestuurders geeft aan dat dit niet erg hoeft te zijn, zolang het bij de bestuurders wel wat teweeg brengt en deze samen met de IBP-verantwoordelijke aan de slag gaan. Drie bestuurders geven aan dat het fijn is dat het normenkader het belang van informatiebeveiliging en privacy op de kaart zet. Een aantal bestuurders geeft aan dat zij voorzien dat het onderwerp daardoor hoger op de agenda komt in de bestuurskamer en er meer geïnvesteerd zal worden in dit thema.

IBP-werkgroep met vertegenwoordiging meerdere scholen

Eén van de bestuurders geeft aan dat er een werkgroep is opgezet in de organisatie, waar vanuit iedere school een vertegenwoordiger aan deelneemt. Deze werkgroep is verantwoordelijk voor de implementatie van IBP-beleid en het versterken van digitaal veilig handelen.

Tijdsbesteding

Alle bestuurders vinden het lastig om het aantal uren dat OOP per jaar zou moeten besteden aan IBP-bewustwording in te schatten. De antwoorden lopen uiteen van twee uren per jaar tot twee uren per maand. Ook geven zij aan dat het per jaar kan verschillen, omdat het ook per jaar verschilt hoeveel en welke instrumenten er worden ingezet.



Rode draden van de resultaten

Effectiviteit van bestaande instrumenten

Er zijn veel verschillende bewustwordingsinstrumenten beschikbaar. Deze verschillen van elkaar op het gebied van vorm, inhoud, tijdsbesteding en interactiviteit.

De ervaren effectiviteit van een instrument wordt onder andere bepaald door de mate waarin deze aansluit op de dagelijkse praktijk, de tijdsbesteding die het vergt en de mate waarin deze herhaaldelijk kan worden toegepast. Tot slot is de effectiviteit van instrumenten afhankelijk van hoe deze met elkaar worden gecombineerd.

De ervaren effectiviteit van instrumenten loopt uiteen en is afhankelijk van verschillende factoren, zoals aan welke doelstelling de interventies moeten bijdragen. Voor een aantal instrumenten geldt dat hier onder experts, leveranciers en bestuurders geen consensus over is. Zo stellen sommige experts dat e-learnings alleen effectief zijn als ze maximaal drie minuten duren, terwijl andere experts stellen dat deze alleen effectief zijn in combinatie met bijvoorbeeld een training. Ook over de effectiviteit van phishingsimulaties zijn de meningen verdeeld. Sommige geïnterviewden geven aan dat een vorm van phishing goed werkt om bewustwording te verbeteren, bijvoorbeeld in combinatie met e-learning.

Andere geïnterviewden stellen dat phishingsimulaties kunnen leiden tot wantrouwen van medewerkers richting het management en hen het gevoel kan geven dat zij ergens op afgerekend worden. Een positieve benadering of spel- of wedstrijdelement toevoegen kan dit wegnemen.

Digitaal veilig handelen

Uit de gesprekken komt naar voren dat bewustwording gaat om alle activiteiten die bijdragen aan het krijgen van inzicht om gewenst gedrag te vertonen. In aanvulling daarop benoemen experts en leveranciers dat medewerkers daarnaast gemotiveerd moeten zijn om daadwerkelijk veilig gedrag te vertonen en hier ook de gelegenheid toe krijgen.

Het is volgens de geïnterviewden belangrijk dat scholen op een positieve en begrijpelijke manier (zonder jargon) aan de slag gaan met informatiebeveiliging en privacy. Een positieve en begrijpelijke benadering zorgt voor intrinsiek gemotiveerde medewerkers, die zelf begrijpen en inzien waarom veilig gedrag nodig is. Bij het (effectief) inzetten van instrumenten of andere interventies om veilig gedrag te stimuleren, zijn het aansluiten bij de belevingswereld van medewerkers en het voorbeeldgedrag van leidinggevend en bestuurders essentieel.



5. Conclusies en aanbevelingen

Conclusies

We begonnen dit onderzoek met de volgende hoofdvraag:

'In hoeverre sluit het huidige aanbod van bewustwordingsinstrumenten aan bij de eisen van het Normenkader IBP FO?'

Hierbij zijn drie subvragen opgesteld. Deze worden in de volgende pagina's beantwoord, waarna antwoord kan worden gegeven op bovenstaande hoofdvraag.

Subvraag 1. Welke instrumenten zijn er al beschikbaar in de markt en bij publieke partijen?

Er zijn veel verschillende soorten bewustwordingsinstrumenten beschikbaar. Deze lopen uiteen van eenvoudige trainingen of korte e-learningmodules tot postercampagnes en bewustwordingsspellen. De instrumenten variëren in de mate van laagdrempeligheid, interactiviteit, herhaaldelijke inzetbaarheid en in de zwaarte van inzet. Zo zit er groot verschil in bijvoorbeeld een serieuze training waar deelnemers worden geconfronteerd met de consequenties van digitaal onveilig handelen of het spelen van een ludiek spel waarbij plezier krijgen in IBP als thema een strategie is om effect te bereiken.

Subvraag 2. Hoe verhouden deze beschikbare instrumenten zich tot het Normenkader IBP FO en tot elkaar?

Met voldoende budget en tijd kunnen schoolbestuurders allerlei instrumenten inzetten om onderwijzend en onderwijsondersteunend personeel bewust te maken van informatiebeveiliging en privacy. Door het diverse aanbod hiervan is gemakkelijk invulling te geven aan wat het normenkader vraagt van onderwijsinstellingen. Bewustwordingsinstrumenten zijn het meest effectief als deze gecombineerd worden ingezet. Zo is een postercampagne effectiever als deze doorpakt op het lesmateriaal uit trainingen, en is een phishingsimulatie effectiever als hier direct een e-learning aan verbonden is. Daarbij is het belangrijk dat de instrumenten meermaals worden ingezet gedurende een schooljaar. De bedoeling en het belang van IBP blijven dan goed hangen bij medewerkers waardoor de bewustwording wordt versterkt.

Conclusies

Subvraag 3. Wat mist er nog in het huidige aanbod?

Veel scholen en schoolbestuurders zouden meer hulp en ondersteuning willen krijgen op het gebied van bewustwording. Deze ondersteuning zou bijvoorbeeld de vorm kunnen krijgen van een landelijk overzicht aan bewustwordingsinstrumenten, waarin staat beschreven hoe deze werken en hoe effectief deze zijn en handreikingen geven hoe deze toe te passen. Ook bestaat er de wens om vanuit de overheid of landelijke organisaties instrumenten aangereikt te krijgen, zodat schoolbestuurders zich niet bezig hoeven te houden met de vraag welke instrumenten zij in gaan zetten. Daarnaast zijn schoolbestuurders dan niet meer afhankelijk van commerciële aanbieders. Het overzicht van de instrumenten, of de instrumenten zelf, zouden bijvoorbeeld aangereikt kunnen worden vanuit SIVON, de PO-Raad en de VO-raad, Kennisnet en/of vanuit het ministerie van OCW (of gezamenlijk). Daarbij kan de [infographic](#) die tijdens dit onderzoek is opgesteld, gebruikt worden als compact overzicht van het proces wat doorlopen moet worden en te bepalen welke bewustwordingsinstrumenten nuttig zijn in specifieke situaties.

Daarbij bestaat de wens om een landelijk kennisplatform te gebruiken, waarop bestuurders en IBP'ers kennis en goede voorbeelden op het gebied van bewustwording kunnen uitwisselen. Het wiel wordt nu vaak opnieuw uitgevonden, wat ten koste kan gaan van de tijd die schoolbestuurders in willen en kunnen zetten voor andere zaken. Het scheelt tijd als men gebruik maakt van een kennisplatform en dit is laagdrempeliger, wat ervoor zorgt dat instrumenten doelmatiger worden ingezet. De bestuurders en IBP'ers weten het platform 'Netwerk IBP' nog onvoldoende te vinden, maar het platform kan in de toekomst mogelijk hiervoor worden ingezet worden.

Hoewel het niet direct onderdeel is van de onderzoeksvraag, concluderen we dat het bewerkstelligen van digitaal veilig gedrag niet alleen afhankelijk is van bewustwordingsinstrumenten. Naast bewustzijn is het zeer belangrijk dat medewerkers gemotiveerd zijn om veilig te handelen en moeten zij hier ook de gelegenheid toe krijgen; het moet hen zo eenvoudig mogelijk worden gemaakt. In onze aanbevelingen gaan we hier verder op in.

Conclusies

Hoofdvraag. In hoeverre sluit het huidige aanbod van bewustwordingsinstrumenten aan bij de eisen van het Normenkader IBP FO?

Het huidige aanbod van bewustwordingsinstrumenten sluit goed aan bij de eisen van het Normenkader IBP FO. Het diverse aanbod aan instrumenten biedt voldoende mogelijkheden aan schoolbesturen om onderwijzend en onderwijsondersteunend personeel bewust te maken van informatiebeveiliging en privacy en hier een continu doorlopend bewustwordingsprogramma mee te ondersteunen, conform norm 4.6 van het Normenkader IBP FO. Daarnaast dient er, conform de uitwerking in hoofdstuk 3 van de normen die effect hebben op de bewustwording van OOP, ook aandacht te zijn voor het bekend maken van het geldende interne beleid en de procedures.

Alleen het gebruik van bewustwordingsinstrumenten is echter niet voldoende om volledig te voldoen aan de eisen van het Normenkader IBP FO. Hiervoor zijn de volgende aspecten noodzakelijk, in aanvulling op de bewustwordingsinstrumenten:

1. Samenwerking binnen de sector om kennis uit te wisselen, bijvoorbeeld door een landelijk platform op te zetten waarop bestuurders en IBP-ers kennis en goede voorbeelden met elkaar kunnen delen.
2. Medewerkers moeten zich bewust zijn van informatiebeveiliging en privacy, maar zij moeten ook gemotiveerd zijn om digitaal veilig te handelen en hier de gelegenheid toe krijgen. Met andere woorden, wij onderschrijven het COM-B-model dat aangedragen werd door experts. De drie aspecten samen zorgen er namelijk voor dat voldaan kan worden aan de eisen van het Normenkader IBP FO die voor de doelgroepen van toepassing zijn. Dat betekent dat het van belang is om niet alleen de kennis te vergroten met de instrumenten, maar ook samen met de medewerkers te bekijken wat maakt dat het gewenste gedrag niet aanwezig is. Is dit door een gebrek aan kennis (weet men dat het nodig is papier veilig weg te gooien en hoe men dat kan doen?), of dat men hier niet de gelegenheid wordt geboden (bijvoorbeeld door papierbakken op meer plekken neer te zetten om veilig weggooien gemakkelijker te maken) of door een gebrek aan motivatie (ziet men het nut van de maatregel in bijvoorbeeld door de potentiële gevolgen van niet veilig handelen te begrijpen)? Dit bepaalt de gewenste interventie.

Aanbevelingen

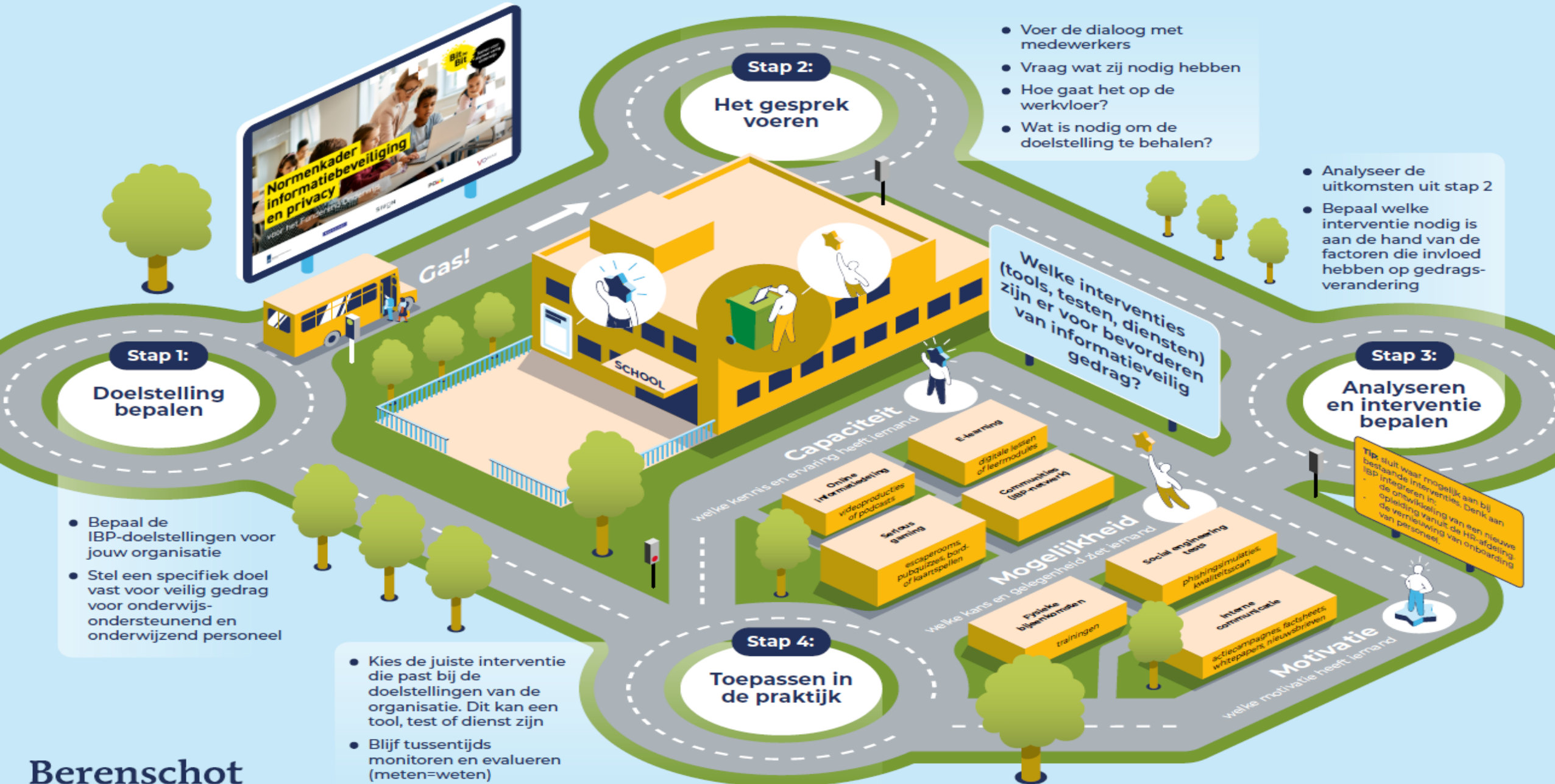
Dit hoofdstuk beschrijft een aantal concrete aanbevelingen om bewustwording van OOP op het gebied van IBP te versterken, op basis van de resultaten en conclusies uit dit onderzoek.

1) Op weg naar informatieveilig gedrag? Begin altijd met in kaart brengen van de stand van zaken.

Digitaal veilig gedrag realiseren gaat - naast het inzetten van de juiste instrumenten - vooral over grip krijgen op de drie factoren die gedrag beïnvloeden: 'capaciteit', 'motivatie' en 'gelegenheid'. Medewerkers op school moeten op een positieve manier gefaciliteerd worden om het juiste te doen. Om dit in de praktijk te brengen, is het belangrijk dat scholen concrete IBP-doelstellingen bepalen en vervolgens aan de slag gaan met het in kaart brengen van de stand van zaken. Door het volwassenheidsniveau scherp te krijgen, kan worden bepaald in hoeverre dit aansluit op de IBP-doelstellingen van een organisatie en wat er nog nodig is om hier te komen. Dit zou het startpunt moeten zijn voor elke organisatie bij het vormgeven van het bewustwordingsprogramma. Doorloop hiervoor de volgende stappen (zie ook de volgende pagina voor [de visuele weergave](#)):

- 1. Doelstelling bepalen.** Een of meerdere specifiek doelen voor veilig gedrag van onderwijzend en onderwijsondersteunend personeel moet(en) vastgesteld worden.
- 2. Voer het gesprek.** Door de dialoog te voeren met medewerkers wordt in kaart gebracht welke behoefte medewerkers hebben en wat er nodig is om de doelstelling te behalen.
- 3. Interventie kiezen.** Doordat bekend is wat er nodig is om veilig gedrag te bewerkstelligen, kan de juiste interventie worden gekozen om de doelen te bereiken. Hierbij is het belangrijk ervan bewust te zijn dat de factoren 'capaciteit', 'motivatie' en 'gelegenheid' alle drie aanwezig moeten zijn, en dat de gekozen interventie aansluit op hetgeen wat nog mist. Een voorbeeld hiervan is het direct veilig afvoeren van persoonsvertrouwelijke informatie: je kunt medewerkers de kennis geven dat dit nodig is in het kader van privacy, maar als de motivatie ontbreekt en er geen gelegenheid toe wordt geboden, dan is dit onvoldoende en zal digitaal veilig gedrag niet worden bewerkstelligd. Op het moment dat bijvoorbeeld papierbakken of shredders altijd binnen redelijk bereik aanwezig zijn (gelegenheid) en medewerkers het nut begrijpen van veilig weggooien, ontstaat er - door de capaciteit en het bieden van de gelegenheid - de motivatie, wat de kans groter maakt dat de medewerkers het juiste gedrag vertonen.
- 4. Toepassen.** De gekozen interventies kunnen toegepast worden, waarbij het belangrijk is om het proces te monitoren en tussentijds te evalueren.

Op weg naar informatieveilig gedrag in het Funderend Onderwijs



Aanbevelingen

2) Verken mogelijkheden om het uitwisselen van kennis en ervaring tussen scholen te versterken

Uit dit onderzoek komt naar voren dat schoolbesturen en IBP verantwoordelijken ervaren dat zij vaak (nog) zelf opnieuw het wiel uitvinden wat betreft het bevorderen van IBP-bewustwording van OOP in het funderend onderwijs. Deze doelgroep heeft een sterke wens om op een makkelijke, toegankelijke manier inzicht te krijgen in waar te beginnen en welke stappen te zetten om bewustwording te realiseren. Een aanbeveling aan het programma is om samen met deze doelgroep en de experts uit het IBP-netwerk te verkennen welke kansen er nog liggen om het uitwisselen van kennis (concrete en praktische handvatten, stappenplannen, referentiegidsen en/of leidraden voor IBP-bewustwording in de praktijk) en ervaring (best practices, wat werkt goed, wanneer zet je welke interventie in) te versterken. In de verkenning is het belangrijk om verder in kaart te brengen waar specifiek nog behoefte aan is in de praktijk en wat er nodig is om daar zo goed mogelijk op aan te sluiten. Inzicht in waar schoolbesturen moeten beginnen met het bewerkstelligen van digitaal veilig gedrag is hierbij cruciaal. Hierbij moet bijvoorbeeld gekeken worden naar wat er nog ontbreekt in een schoolorganisatie: de kennis, de motivatie en/of gelegenheid. Als scholen voor het bepalen van IBP-doelstellingen en passende interventies handreikingen of stappenplannen kunnen inzetten, helpt dit scholen om digitaal veilig gedrag te stimuleren.

3) Neem bewustwording voor IBP al mee in lerarenopleidingen en opleidingen van bestuurders

Uit het onderzoek blijkt dat onderwijzend en onderwijsondersteunend personeel zich na het volgen van de lerarenopleiding nog niet bewust zijn van het belang van informatiebeveiliging en privacy. Door dit bewustzijn wel meteen te creëren tijdens de lerarenopleiding, zullen zij in hun werk sneller geneigd zijn om digitaal veilig gedrag te vertonen. Ook voor nieuwe bestuurders geldt dat informatie over het belang van informatiebeveiliging en privacy nog niet opgenomen is in het opleidingsprogramma dat zij volgen om bestuurder te worden. Voor toekomstige bestuurders kan het van toegevoegde waarde zijn om dit wel op te nemen, zodat zij het belang hiervan inzien en anderen hier op gepaste wijze op kunnen aansturen.

Aanbevelingen

4) Zet instrumenten in als middel om een concreet doel voor IBP-bewustwording te realiseren

Om effectief te werken aan het versterken van IBP-bewustwording van OOP op scholen, is het belangrijk om de inzet van instrumenten in te zetten als ondersteuning en als middel om concrete IBP-doelstellingen voor bewustwording te bereiken. Het inzetten van instrumenten moet niet worden gezien als doel op zich. Deze aanbeveling luidt dan ook om altijd te beginnen met aanbeveling 1 (begin bij het in kaart brengen van de stand van zaken) om vervolgens de juiste interventies te kiezen, zoals de instrumenten die benoemd zijn in de landschapsanalyse van dit onderzoek.

De volgende drie aandachtspunten zijn in ieder geval van belang voor de juiste inzet van deze instrumenten als middel om IBP-doelstellingen voor bewustwording te bereiken:

- **Zorg dat instrumenten goed aansluiten bij de dagelijkse praktijk en belevingswereld van de doelgroep**

Op het moment dat instrumenten ingezet worden, is het belangrijk dat deze aansluiten bij de dagelijkse praktijk en belevingswereld van OOP. Door dit te doen, neemt de effectiviteit toe en is het voor OOP beter te begrijpen waarom en daardoor is het makkelijker om juist te handelen.

- **Benader de doelgroep op een positieve manier**

Het belang en de urgentie van een goed IBP-volwassenheidsniveau staat voor OOP niet altijd hoog op de agenda. De prioriteiten van een gemiddelde medewerker (OOP) liggen vooral bij het leveren van en ondersteunen bij kwalitatief goed onderwijs. IBP wordt soms meer als een bijzaak of een 'moetje' ervaren. Hierdoor krijgt IBP en daarmee (informatie)veilig handelen niet altijd de juiste aandacht. Daarom is het belangrijk dat bewustwordingsactiviteiten op een positieve manier onder de aandacht komen bij deze doelgroep. Het moet een positieve associatie bij medewerkers oproepen zodat zij bewustwordingsactiviteiten ervaren als iets wat hen helpt om hun rol op de juiste manier te vervullen.

Aanbevelingen

- **Combineer en herhaal de inzet van instrumenten**

Instrumenten zijn het meest effectief als deze met elkaar worden gecombineerd en als ze worden herhaald gedurende een langere periode. De instrumenten hebben een versterkende werking op elkaar en herhaling zorgt ervoor dat de informatie beter bij de doelgroep blijft hangen.

Daarnaast zou bewustwording geen eenmalige oefening moeten zijn, maar een periodiek proces – zeker in relatie tot het normenkader, te weten norm 4.6, die stelt dat er een bewustwordingsprogramma dient te zijn. Als medewerkers gedurende een schooljaar meerdere keren in aanraking komen met bewustwordingsactiviteiten in de vorm van instrumenten is de kans groter dat de informatie blijft hangen en dat zij digitaal veilig gedrag vertonen.

Contactgegevens onderzoekers



Rianne Zivali – de kievit

Projectleider / senior adviseur
informatiebeveiliging en privacy

r.zivali@berenschot.nl

06 50 25 42 42



Janneke Bootsma

Senior adviseur
informatiebeveiliging en privacy

j.bootsma@berenschot.nl

06 21 16 30 43



Sara Wildschut

Junior adviseur
sector onderwijs

s.wildschut@berenschot.nl

06 22 08 01 65



Berenschot

Berenschot
www.berenschot.nl
linkedin.com/berenschot