PRIVACY OP SCHOOL

DECEMBER 2024

Het Normenkader IBP:

Hoe krijgen we dit (wél) voor elkaar?

Privacy op School is dagelijks bezig om schoolbesturen in het primair- en voortgezet onderwijs (PO en VO) te begeleiden bij de implementatie van het Normenkader IBP. We zien met enig mededogen aan hoe het onderwijs worstelt met dit beveiligingsvraagstuk. Of is het vooral een uitvoeringsvraagstuk? Graag delen we met jullie onze ervaringen over hoe het onderwijs hiermee omgaat, waar zij (en wij) tegenaan lopen, maar vooral wat het onderwijs nodig heeft om dit wél voor elkaar te krijgen.

Waar komt het Normenkader IBP vandaan?

Laten we beginnen bij het ontstaan van het Normenkader IBP. Jaren geleden is SURF (de tegenhanger van SIVON in het Hoger onderwijs en MBO) begonnen met een eerste versie van het toetsingskader en de zogenaamde SURFaudit. Dit kader was gebaseerd op de internationale standaard voor informatiebeveiliging ISO27001. Het MBO ging na de aansluiting bij SURF vanaf 2015 voortvarend mee in dit kader.

Grote datalekken in het Hoger Onderwijs (Universiteit van Maastricht, 2019) en het MBO (ROC Mondriaan, 2021), bevestigden het belang van deze aanpak.
Vreemd genoeg gebeurde er in die periode in het PO en VO nog weinig op het gebied van kwaliteitseisen voor informatiebeveiliging, terwijl in deze sectoren de mate van digitalisering groter is dan in de rest van het onderwijs.

In 2021 stapte het MBO in navolging van het Hoger Onderwijs over naar een nieuw toetsingskader, gebaseerd op het groeimodel van de Nederlandse Beroepsvereniging van Accountants (NBA). De accountants werden steeds kritischer op het thema informatiebeveiliging, vanwege de financiële risico's rondom ransomware en overige aansprakelijkheden. De toename van zowel de digitalisering in het onderwijs als het aantal cyberdreigingen en -incidenten in de coronapandemie hebben hier ongetwijfeld aan bijgedragen.

Schoolbesturen in het PO en VO waren sinds 25 mei 2018 vooral druk om de AVG-compliance op orde te brengen.
Er waren wel schoolbesturen, met name in het VO, die last hadden van DDOS-aanvallen[1], maar door het toenemen van het gebruik van cloudbased software-as-a-service, werd dit een steeds minder groot risico. Schoolbesturen bleven last houden van phishing en ransomware aanvallen, die soms tot vervelende gevolgen leidden. De weerstand tegen het gebruik van multifactorauthenticatie maakte duidelijk hoe men in het onderwijs tegen beveiligingsmaatregelen aankeek.
Inmiddels wordt dit overigens breed geaccepteerd.

[1] Met een (Distributed) Denial-of-Service-aanval (DDoS-aanval) wordt de capaciteit van onlinediensten of de ondersteunende servers en netwerkapparatuur aangevallen. Het resultaat van deze aanval is dat diensten slecht of helemaal niet meer bereikbaar zijn voor gebruikers.

Schoolbesturen, met name in het basisonderwijs, hebben evenals hun ICT-beheer ook informatiebeveiliging aan ICT-leveranciers uitbesteed. De meeste schoolbesturen in het PO en VO waren – los van MFA - zelf nog weinig bezig met informatiebeveiliging. In tegenstelling tot het MBO en Hoger Onderwijs ontbrak in 2021 een duidelijke beveiligingsstandaard voor schoolbesturen in het PO en VO. De Onderwijsinspectie maakte zich inmiddels steeds meer zorgen. Zij hadden namelijk in 2021 onderzoek gedaan naar de stand van zaken rondom informatiebeveiliging (Binnen zonder kloppen, 2021[2]) en vonden dit aanleiding om rondetafelgesprekken te voeren met bestuurders in het PO en VO.

Bij de PO- en VO-raad kwam steeds meer de roep om meer duidelijkheid voor schoolbesturen rondom IBP-eisen binnen.

Een ICT-regiegroep met schoolbestuurders adviseerde in 2022 om heldere kwaliteitsnormen voor IBP in het PO en VO te formuleren en toe te werken naar een minimale beveiligingsstandaard[3]. Het ministerie van OCW greep deze kans aan om minister Wiersma in 2022 een brief te laten sturen naar alle schoolbesturen in het PO en VO om een Normenkader IBP aan te kondigen in lijn met het nieuwe kader in het Hoger onderwijs en MBO[4]. Het grote verschil met deze sectoren was dat het ministerie aankondigde dat de aanpak in het PO en VO onderwijs niet vrijblijvend zou zijn. 'We werken toe naar een verplichting van dit Normenkader met extra toezicht en externe audits daarop', aldus de toenmalige minister.

[2]https://www.onderwijsinspectie.nl/documenten/themarapporten/2021/09/15/digitale-weerbaarheid-in-het-hoger-onderwijs

[3]https://www.vo-raad.nl/artikelen/advies-waarom-regie-op-ict-geen-uitstel-duld

[4]https://www.rijksoverheid.nl/documenten/kamerstukken/2022/07/14/verhogen-digitale-veiligheid-onderwijs-en-onderzoek

Het Normenkader IBP is er, maar de strategie ontbreekt

Het Ministerie kondigde aan een programma in te richten om scholen te helpen bij het realiseren van digitaal veilig onderwijs. Vanaf 2023 gaat er tot en met 2027 zes miljoen euro per jaar naar dit programma, dat wordt uitgevoerd door Kennisnet in samenwerking met SIVON en de PO- en VO-raad. In totaal ontvangt het PO- en VO-onderwijs indirect dertig miljoen euro voor digitaal veiliger onderwijs.

Bijna een jaar later, op 19 april 2023, werd na verschillende bijstellingen in de planning het Normenkader IBP voor het PO en VO gelanceerd, dat wil zeggen alleen het deel voor informatiebeveiliging. Het deel voor privacy zou ruim een jaar later verschijnen. Met de lancering ging een belangrijk momentum verloren. Veel scholen stonden in 2023 in de startblokken, maar het aangekondigde ondersteuningsaanbod in de vorm van voorbeelddocumenten, was op dat moment niet gereed. De voorbeelddocumenten die inmiddels gedeeltelijk zijn verschenen, sluiten nog onvoldoende aan op de praktijk van het onderwijs.

Sinds 6 juni 2024 hebben we een nieuwe versie van het Normenkader IBP inclusief het privacydeel, maar schoolbesturen zijn per saldo nog te weinig opgeschoten met de implementatie. Uit nulmetingen van Privacy op School blijkt dat de gemiddelde score van schoolbesturen op het beveiligingsdeel van het normenkader 1,7 bedraagt.

De nulmetingen maken pijnlijk zichtbaar hoeveel werk er nog te doen is bij de schoolbesturen. In 2027 dienen schoolbesturen een minimale score van 3,0 bereikt te hebben. Een ruwe schatting van experts is dat er 1000-4000 uur incidenteel en jaarlijks 300-600 uur per schoolbestuur benodigd is. Steeds vaker wordt de vraag gesteld of het behalen van niveau 3,0 van het normenkader IBP in 2027 wel haalbaar is.

Schoolbesturen in het PO en VO hebben te kampen met personeelstekorten. De kennis en capaciteit op het gebied van privacy en security is daarnaast schaars. Het Normenkader is dus naast een beveiligingsvraagstuk steeds meer een uitvoeringsvraagstuk geworden.

Hoe moet het nu verder?

Tonny Plas
Directeur Operations

Wat is het Normenkader (niet)?

Graag delen we enkele gedachten om met elkaar het gesprek aan te gaan over de noodzakelijke randvoorwaarden die van belang zijn voor een succesvolle implementatie van het Normenkader IBP. Tot slot willen we een strategie presenteren die het bereiken van de baseline in 2027 wél mogelijk maakt.

1. Het Normenkader IBP is geen doel op zich

Het normenkader is bedoeld om risico's beheersbaar te maken. Laten we dit vooral niet uit het oog verliezen. Het geeft namelijk aan waarom we bepaalde zaken, zoals MFA, moeten doorvoeren. Elke norm dekt bepaalde risico's af. Als men niet snapt wat het risico is, dan stuit elke norm of maatregel op weerstand. Je zult als onderwijsorganisatie dan ook je risico's moeten kennen voordat je kunt bepalen welke normen voor jouw organisatie van belang zijn. Zodra je dit weet, kun je ook beter prioriteiten stellen. Schoolbesturen dienen hun risicomanagement dus op orde te hebben. De AVG vraagt van organisaties om een risicogebaseerde aanpak te hanteren. Het normenkader is een hulpmiddel om hieraan gestructureerd en cyclisch (PDCA) te werken.

2. Het Normenkader IBP is geen ICT-feestje

Veel risico's rondom digitaal veilig onderwijs kunnen technisch worden opgelost. Het normenkader kan en mag echter geen technisch of ICT-feestje worden. De organisatorische kant van informatiebeveiliging vormt veruit de grootste uitdaging. Zolang de procesverantwoordelijken (leidinggevenden of 'het management') zich niet bekommeren om risico's rondom informatiebeveiliging en privacy, heeft het geen zin om met het normenkader aan de slag te gaan. De proceseigenaren zijn namelijk verantwoordelijk voor de implementatie van technische, maar ook organisatorische maatregelen. Denk hierbij aan het beleid en de procedures in processen met betrekking tot inkoop, facilitair, administratie en personeelsmanagement. Schoolbesturen moeten dus aan de slag met eigenaarschap en governance.

3. Het Normenkader IBP is geen afrekenmodel

De oorspronkelijke naam van het normenkader is het 'Volwassenheidsmodel informatiebeveiliging'. Laten we het dus vooral gebruiken als een groeimodel. De AVG vraagt van organisaties dat ze werken aan continue verbetering van het beschermingsniveau. In het onderwijs kennen we al genoeg vinklijstjes. Laten we dus kijken naar de groei van onderwijsorganisaties, in plaats van de schoolbesturen af te rekenen op een score. Overigens kan die volwassenheid ook gerust van elkaar verschillen, omdat onderwijsorganisaties nu eenmaal van elkaar verschillen. Ook hier geldt dat de passende maatregelen met betrekking tot de bescherming van persoonsgegevens niet alleen afgestemd moeten worden op de risico's, maar ook op de mogelijkheden die een organisatie heeft om hiervoor passende maatregelen te kunnen nemen.

4. Het Normenkader IBP is geen invuloefening

Bij het van kracht worden van de AVG in 2018 zagen we al veel papieren exercities. Een schoolorganisatie wordt hier per saldo niet veiliger van. Uiteraard moeten processen en afspraken goed beschreven zijn, maar laten we onze focus houden op de uitvoering en borging in de processen. Dit kan op meerdere manieren aantoonbaar gemaakt worden, dan alleen via het produceren van beleid. We zijn niet tegen beleid, maar wel tegen beleid dat alleen maar een papieren tijger is, veel weerstand oproept en niet bijdraagt aan borging.

> Het Normenkader is dus naast een beveiligingsvraagstuk steeds meer een uitvoeringsvraagstuk geworden.

Hoe dan wel? Een implementatiestrategie voor het Normenkader IBP

A. Maak afspraken met ICT-leveranciers

Eén derde van het normenkader dat betrekking heeft op informatiebeveiliging bestaat – zeker in het PO – uit processen die uitbesteed zijn aan leveranciers. Het verbaast ons dan ook dat er al 2 jaar lang niet actief met deze leveranciers hierover wordt gesproken. Ook omdat de 80% van de scholen in het PO die uitbesteed heeft bij de twee grootste leveranciers. Door met deze partijen afspraken te maken, kunnen scholen een fors deel van de vereisten invullen. Dit wil niet zeggen dat leveranciers eindverantwoordelijk zijn, in tegendeel. De ICT-leverancier voert het alleen namens de schoolbesturen uit. Een gemiddeld schoolbestuur heeft niet de expertise in huis om dit gesprek met hun ICT-leverancier te voeren. De ICT-leveranciers zoeken nu zelf naar invullingen en keuren hun eigen vlees. Er zou een onafhankelijk keurmerk moeten komen voor ICT-leveranciers waarmee schoolbesturen invulling kunnen geven aan het normenkader.

B. Zorg voor voldoende uitvoeringscapaciteit

Zoals gezegd hebben schoolbesturen – door de bank genomen - niet de mensen en kennis in huis om uitvoering te geven aan het normenkader. In de markt staan steeds meer partijen klaar om scholen te helpen, alleen de coördinatie ontbreekt. Wij pleiten daarom voor samenwerking en regie. Dit zou kunnen in de vorm van een taskforce IBP die volgens een vaste methodiek de scholen verder helpt en aangestuurd wordt, bijvoorbeeld vanuit een publieke regiefunctie binnen het programma Digitaal Veilig Onderwijs. Hierbij kan worden samengewerkt met de partijen die zich verenigd hebben in het IBP-platform voor het onderwijs (www.ibp-platform.nl).

C. Werk in samenwerkingsverbanden aan de ontwikkeling van beleid

Wij pleiten voor samenwerking met andere schoolbesturen binnen de regio voor het ontwikkelen van beleid, maar ook voor het uitwisselen van kennis en ervaringen op het gebied van implementatie en het uitwisselen van capaciteit. Inmiddels zijn er al mooie praktijkvoorbeelden waarbij dit gebeurt. De ervaringen vanuit deze samenwerkingen zouden meer gedeeld kunnen worden. Dit zou een belangrijke bijdrage kunnen leveren aan het gebrek aan kennis en capaciteit bij individuele schoolbesturen. Zou het landelijk budget ook niet hierin geïnvesteerd moeten worden?

Samenwerking Topgroep Noord-Holland

Privacy op School heeft met 14 VO-besturen in Noord-Holland een programma opgezet om samen te werken aan de ontwikkeling en implementatie van het Normenkader IBP. Binnen het programma is een team aan het werk met experts van scholen en externe CISO's die de proceseigenaren van de scholen in zogenaamde netwerkgroepen begeleidt bij de ontwikkeling en implementatie.

D. Zorg dat het landelijke ondersteuningsaanbod beter aansluit bij de praktijk

Er wordt al 1,5 jaar gewerkt aan het landelijk ondersteuningsaanbod. Dit komt nog steeds niet goed van de grond. Materialen ontbreken of sluiten onvoldoende aan op de praktijk van het onderwijs. Ontwikkel daarom het voorbeeldbeleid niet zonder schoolbesturen en experts in de markt, maar doe het samen, waardoor het beter aansluit bij de onderwijsorganisatie. Ook hierbij kan gedacht worden aan publiek-private samenwerking met het IBP-platform. Daarbij kan ook gedacht worden aan betere tools om beleid vorm te geven en actueel te houden.

E. Zorg voor borging van ondersteuning na 2027

Het is duidelijk dat we in 2027 nog niet klaar zijn. Sterker nog, de meeste scholen hebben dan pas de eerste implementatiestappen gezet. Het houdt dus niet op in 2027, het echte werk begint dan pas. Er zal nu al nagedacht moeten worden over de plannen om schoolbesturen na 2027 blijvend te ondersteunen en/of te voorzien van eigen middelen, zodat ze dit meer en meer zelf kunnen gaan regelen.

F. Zorg dat het normenkader wordt beheerd

Zoals bij wetgeving, loopt ook het normenkader alweer achter op nieuwe ontwikkelingen. Denk hierbij aan de komst van AI en de gevolgen die deze technologie heeft voor IBP. Het normenkader moet daarom met regelmaat vernieuwd en geactualiseerd worden. Zorg voor duidelijk beheer van het normenkader en een goed proces om nieuwe eisen in te dienen dan wel vragen te kunnen stellen over implementatie, ook na de looptijd van het programma.

Samen kunnen we werken aan digitaal veilig onderwijs. Wilt u meer weten of reageren op dit artikel? Mail dan naar info@privacyopschool.nl of kijk op www.privacyopschool.nl.

Beleidshandboek Normenkader IBP

Privacy op School werkt aan een beleidshandboek waarin al het beleid rondom het Normenkader IBP (beveiligingsdeel) is beschreven en dat vanaf februari 2025 ook ontsloten zal worden in de beleidsmodule Schoolkwaliteit van Topicus. Hierin zijn ook andere beleidsthema's opgenomen zoals het onderwijsbeleid, etc. Een schoolbestuur kan hiermee snel en effectief zijn eigen beleid op orde krijgen.

Over Privacy op School

Privacy op School is een organisatie die álle organisaties in het onderwijs wil helpen en ondersteunen bij privacy en informatiebeveiligingsvraagstukken.

Onze missie luidt: Wij zijn dé experts op het gebied van privacy in het onderwijs. Vraagstukken worden steeds complexer. Niet alleen schoolbesturen hebben behoefte aan ondersteuning, maar ook organisaties om het onderwijs heen.

Denk bijvoorbeeld aan samenwerkingsverbanden, kinderopvangorganisaties en onderwijsleveranciers. Ook zij komen inmiddels naar Privacy op School met vragen over het privacy compliant aanbieden van hun dienstverlening.

Privacy op School bedient met een team van 35 experts meer dan 250 onderwijsorganisaties.

> Wij zijn dé experts op het gebied van privacy in het onderwijs.

privacyopschool.nl

PRIVACY OP SCHOOL