Cyberveiligheid in het mbo

Plan van aanpak om de digitale weerbaarheid en de privacybescherming van de mbo-instellingen te verhogen

MBO Digitaal & MBO Raad
Versie 1.7
2 september 2022

Aanleiding

De Universiteit van Maastricht kreeg op de valreep van 2019 te maken met een ransomware-aanval die de start is geweest voor veel discussie over cyberveiligheid in het onderwijs. 'Maastricht' markeerde terugkijkend ook het begin van een reeks andere cyberincidenten in onze sector, onder meer bij de Hogeschool Arnhem-Nijmegen (HAN), de Hogeschool van Amsterdam (HvA) en bij de Universiteit van Amsterdam (UvA). De onderwijssector is zoveel mogelijk transparant over cybercriminaliteit. Door onderling kwetsbaarheden, geleerde lessen en 'best practices' te delen, willen we als sector de weerbaarheid tegen cyberaanvallen vergroten. De aanvallen bij de HvA en UvA zijn uitvoerig gedocumenteerd in een rapportage en ook de Inspectie van het Onderwijs heeft onderzoek gedaan en haar bevindingen gepubliceerd in het rapport Binnen zonder Kloppen.

Bij de start van het schooljaar van 2021-2022 kreeg ROC Mondriaan te maken met een ransomware-aanval en daarmee werd voor het eerst ook een mbo-instelling op grote schaal geraakt.

De bovengenoemde cybercrises en de analyses ervan hebben veel losgemaakt, bij de onderwijsinstellingen, het ministerie van OCW en in de Tweede Kamer. Er zijn Kamervragen gesteld en naar aanleiding daarvan heeft de minister van OCW in de brief naar de Tweede Kamer een aantal maatregelen verwoord. Daarbij is afgesproken, dat de onderwijskoepels in het eerste kwartaal van 2022 met een plan van aanpak komen om de digitale weerbaarheid van de onderwijsinstellingen te verhogen.

Vanuit de MBO Raad en MBO Digitaal werken wij daar graag aan mee en zien we dit als een kans om focus te krijgen op knelpunten en oplossingen op het gebied van cyberveiligheid waarover al langer gesproken wordt binnen de mbo-sector.

Het gaat daarbij om veiligheid binnen alle ict-domeinen binnen het onderwijs:

- digitale leermiddelen en toetsen
- de leermiddelenketen (voor het ontsluiten en gebruiken van leermiddelen en toetsen)
- ict ter ondersteuning van de les, bv plagiaatsoftware, proctoring of videobellen en de elektronische leeromgeving.
- ict voor de bedrijfsvoering van een instelling, bijvoorbeeld administratiesystemen
- ict voor verantwoording en beleidsinformatie intern en extern

In dit plan nemen we ook de borging van de privacy mee. In de eerste plaats omdat privacy onlosmakelijk verbonden is met informatiebeveiliging. Daar komt bij de brief van de Autoriteit Persoonsgegevens aan de minister van OCW, naar aanleiding van de DPIA op Google G Suite for Education. Daarin adviseert de AP de minister van OCW om de aanpak van gegevensbescherming binnen het onderwijs meer te coördineren en zwaarder in te zetten op risicomanagement en de uitvoering van DPIA's op de veelgebruikte digitale middelen in het onderwijs. Ook deze onderwerpen zijn in ons plan geadresseerd.

Dit plan van aanpak is voor de komende jaren onze roadmap op het gebied van informatiebeveiliging en privacy, met een breed palet aan maatregelen om als mbo-sector weerbaarder te worden tegen cyberaanvallen en de privacy beter te borgen. Op basis van dit plan is een subsidieaanvraag gedaan voor de periode 2022-2027 en deze subsidie van totaal 23,8 miljoen voor de periode van 2022 – 2027 is inmiddels toegekend. We kunnen naar verwachting vanaf 1 oktober 2022 starten met het programma.

Over dit document

Dit plan komt tot stand in samenwerking met de netwerken van MBO Digitaal, met name het Netwerk IBP in het mbo, de Regiegroep IBP en het CSC-netwerk van SURF contactpersonen. Daarbij wordt intensief afgestemd met SURF en is er overleg met de onderwijskoepels VH en UNL.

We beginnen dit document met een situatieschets: waar staat het mbo op het gebied van cyberveiligheid. Vervolgens gaan we in op de manier waarop er wordt samengewerkt op het gebied van informatiebeveiliging en privacy. Daarna gaan we in op onze ambities op het gebied van cyberveiligheid. Die worden kernachtig verwoord in puntsgewijze opsommingen met actiepunten voor de mbo-instellingen zelf, voor MBO Digitaal, de MBO Raad en/of SURF. Vanuit die actiepunten hebben we 22 projectactiviteiten gedefinieerd. Deze projectactiviteiten zijn ondergebracht in 4 deelprojecten, die samen de basis vormen voor onze subsidieaanvraag.

Dit plan is op diverse momenten besproken met OCW en op basis daarvan zijn er subsidiebedragen gereserveerd voor de aanpak van cyberveiligheid en privacy in het mbo. De subsidieaanvraag wordt uitgewerkt en de eerste aanzet hiervoor is toegevoegd als bijlage.

Als in dit document de ‘we’-vorm wordt gebruikt dan bedoelen we daarmee de MBO Raad en het platform MBO Digitaal.

Waar staat het mbo op het gebied van cyberveiligheid

In het mbo speelt het *Netwerk Informatiebeveiliging en Privacy in het mbo* (Netwerk IBP) een belangrijke rol op het gebied van cyberveiligheid. Dit is een hecht netwerk waarin alle mbo-instellingen zijn vertegenwoordigd. Vanuit het netwerk IBP wordt sinds 2015 jaarlijks een benchmark uitgevoerd op het gebied van informatiebeveiliging, privacy en (digitale) examinering: de Benchmark IBP-E. Alle mbo-instellingen doen hieraan mee. De meest recente is in het najaar van 2021 afgenomen en de rapportage is in januari 2022 gepubliceerd.

De volwassenheid op het gebied van informatiebeveiliging en privacy wordt gemeten door middel van toetsingskaders, op een schaal van 1 tot 5, waarbij niveau 3 het ambitieniveau is. Niveau 3 wordt in het algemeen beschouwd als een goede balans tussen de veiligheid en de kosten van de maatregelen. Hoewel we ook in 2021 een lichte groei in volwassenheid zien, wordt niveau 3 als sectorgemiddelde in 2021 niet behaald. Op de onderdelen Informatiebeveiliging, Privacy en Examinering wordt gemiddeld respectievelijk 2,8, 2,9 en 2,8 gescoord. Daarmee vlakt de snelle volwassenheidsgroei die in de voorgaande zes jaren werd gerealiseerd wat af. Op zich is dat verklaarbaar omdat naarmate de volwassenheid stijgt, het lastiger wordt om verdere groei te realiseren. Maar het lijkt ook in tegenspraak met de toegenomen aandacht voor informatiebeveiliging en privacy in het afgelopen jaar. Na verdere analyse en discussie blijkt echter dat mbo's de dreigingen op dit gebied steeds beter in beeld hebben: een hoger risicobewustzijn leidt tot een meer kritische beoordeling van de volwassenheid en in individuele gevallen tot een verlaging van de volwassenheidsscore. Dat is een positief effect en een goede illustratie dat je de cijfers uit deze benchmarks niet te veel als rapportcijfers moet beschouwen.

Ontwikkelingen informatiebeveiliging

Het valt op dat er op het gebied van informatiebeveiliging grote verschillen in volwassenheid zijn: de top 10 scoort gemiddeld een 3,5 terwijl de tien instellingen aan de andere kant van het spectrum met gemiddeld een 2,1 maar net aan het binnen de sector overeengekomen minimum van 2,0 voldoen. Dit biedt kansen voor verdere samenwerking binnen de mbo-sector omdat er veel geleerd kan worden van de instellingen die het al goed doen. Veel van de maatregelen in dit plan van aanpak richten zich dan ook op het samenwerken en het delen van kennis tussen de mbo-instellingen.

Verder komt het onderwerp *Controle en logging* al sinds 2015 als verbeterpunt naar voren vanuit de benchmark informatiebeveiliging. Logging is een cruciaal aspect van de weerbaarheid tegen cyberaanvallen. De ontwikkeling van SURFsoc, waarop inmiddels de eerste mbo-instellingen zijn aangesloten, is een antwoord hierop. De mbo-instellingen zien echter op tegen de hoge implementatiekosten en de benodigde formatie, niet alleen voor de implementatie maar vooral voor de structurele opvolging van logmeldingen.

Vooral kleine instellingen zijn steeds minder goed in staat om aan de toenemende eisen op het gebied van cyberveiligheid te voldoen. Dat komt naar voren uit het Netwerk IBP en dat beeld wordt bevestigd in de ICT Monitor 2022. Omdat de kleine instellingen over het algemeen minder expertise in huis hebben, is deelname aan het netwerk IBP voor hen

belangrijk voor toegang tot kennis en ervaringen op dit gebied. Daarbij is lidmaatschap van SURF ook voor kleine instellingen heel waardevol vanwege de expertise en diensten die SURF biedt en het kunnen samenwerken in de SURF-community.

Ontwikkelingen privacy

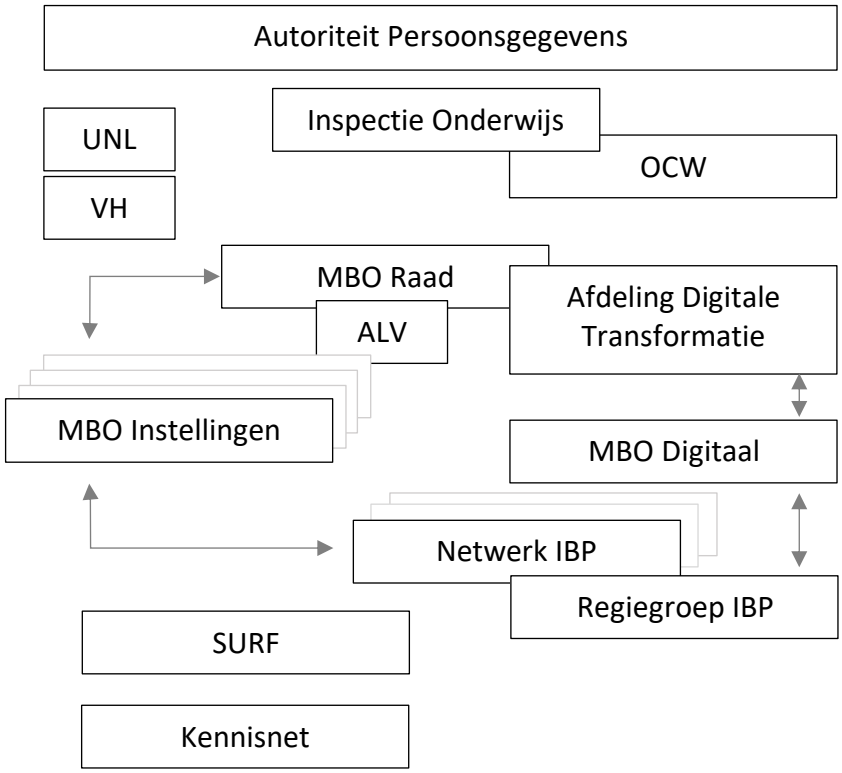
Hoewel informatiebeveiliging een belangrijke basis vormt voor de bescherming van persoonsgegevens is er meer nodig voor een goede bescherming van de privacy van studenten en medewerkers. Daarom kennen we naast het toetsingskader Informatiebeveiliging een toetsingskader met aanvullende statements op het gebied van privacy. Bij de vorige benchmark werd gemiddeld een 2,9 gescoord op het Privacykader. Ook hier lopen de scores sterk uiteen: de top 10 scoort gemiddeld een 3,5 en de laatste 10 in de ranking gemiddeld een 2,3. Daarmee wordt duidelijke dat er behoefte is aan ondersteuning op het gebied van privacy.
Het toetsingskader privacy is in 2016 door de mbo-sector zelf ontwikkeld, als een 'pluscluster' bovenop het toetsingskader informatiebeveiliging. Na zes jaar is het privacykader aan een update toe. Ook in het HO wordt een nieuw privacykader onderzocht en we zijn vanuit het mbo aangesloten bij dit onderzoek en de pilots. De ambitie is om ook op het gebied van het privacykader samen te werken met het hoger onderwijs.

Samenvattend kunnen we stellen dat de mbo-instellingen grote risico's lopen maar dat er ook al veel gebeurt op het gebied van cyberveiligheid en de bescherming van privacy in het mbo.
Daarbij wordt door een toenemend aantal instellingen geoefend op het gebied van cybercrises: aan OZON 2021 hebben 11 mbo-instellingen actief deelgenomen en aan de tabletop oefening NOZON 2022 hebben 20 mbo-instellingen meegedaan.

Belangrijke succesfactor is het Netwerk IBP in het mbo, waarin 170 medewerkers op het gebied van IBP samenwerken en kennis delen. Er is veel collegialiteit en een groot verantwoordelijkheidsgevoel naar elkaar toe. De mbo's zijn zich ervan bewust dat ze de uitdagingen op het gebied van informatiebeveiliging en privacy alleen samen kunnen oplossen. Die positieve energie moeten we gebruiken bij alles wat we in dit plan bedenken om de weerbaarheid van de mbo-instellingen te verhogen. Een belangrijk uitgangspunt hierbij is dat we het niet *voor* de instellingen doen, maar *met* de instellingen.

Samenwerking op het gebied van informatiebeveiliging en privacy

Er wordt intensief samengewerkt op het gebied van informatiebeveiliging en privacy en door recente ontwikkelingen wordt deze samenwerking verder versterkt. Zo wordt de relatie met het hoger onderwijs sterker door gebruik van hetzelfde normenkader Informatiebeveiliging. Op het gebied van privacy wordt samen met het hoger onderwijs een nieuw toetsingskader onderzocht. Die samenwerking krijgt verder vorm door gezamenlijke deelname aan de *Innovatiezone state of the Art Cyberveiligheid* in SURF-verband en door overkoepelende afstemming naar aanleiding van onze plannen van aanpak op het gebied van cyberveiligheid. Hieronder een overzicht van de belangrijkste stakeholders voor het mbo.



Met behulp van dit plaatje beschrijven we de samenwerking tussen de MBO Raad, de ALV, de afdeling Digitale Transformatie, het platform MBO Digitaal, de regiegroep IBP, het Netwerk IBP, SURF en de mbo-instellingen.

Op het gebied van informatiebeveiliging en privacy wordt sinds 2014 intensief door de mbo-instellingen samengewerkt in het Netwerk IBP. MBO Digitaal faciliteert dit netwerk en de Regiegroep IBP fungeert als stuurgroep. Op dit moment zijn hierin tien mbo-instellingen afgevaardigd, aangevuld met een expert vanuit SURF, de MBO Raad en MBO Digitaal. De Regiegroep bepaalt de agenda en de activiteiten voor het Netwerk IBP. Initiatieven op het gebied van de Benchmark IBP-E, de peer review en besluiten over de toetsingskaders worden door de Regiegroep IBP, in afstemming met het Netwerk IBP genomen. Overkoepelende besluitvorming in SURF verband gebeurt via afvaardiging van een regiegroeplid in het SCIPR-bestuur en -werkgroepen.

Besluitvorming in het Netwerk IBP heeft tot nu toe op basis van consensus succesvol gewerkt. Op deze manier voelen de leden zich eigenaar van de problemen en oplossingen op het gebied van IBP: een krachtige en breed gedragen aanpak.
Consensus is echter niet meer genoeg. De IBP-vraagstukken worden complexer en de komende tijd staat de mbo-sector voor ingrijpende besluiten, met soms ook financiële of organisatorische consequenties voor de individuele instellingen. Waar tot nu toe de Regiegroep en het Netwerk IBP samen konden besluiten, zal in het vervolg het MBO Raad-bestuur en/of de ALV hierin een belangrijke rol gaan spelen.

De cyberdreiging in het onderwijs wordt ook steeds vaker in de politiek besproken. Het is belangrijk dat het ministerie van OCW goed op de hoogte is van de actuele stand van zaken op IBP-gebied in het mbo. Een van de gremia waarbinnen het onderwerp IBP regelmatig wordt geagendeerd is de Informatiekamer. Kennisnet en SURF spelen een rol bij de voorbereiding van dit overleg en ook MBO Digitaal zal daar vanaf nu nadrukkelijker bij betrokken worden. Daarmee wordt geborgd dat de ontwikkelingen vanuit het mbo goed aan bod komen.

Daarnaast hebben de onderwijssectoren afzonderlijk overleg met hun contactpersonen binnen het ministerie van OCW. Nu er meer wordt samengewerkt tussen het mbo en het hoger onderwijs, wordt afstemming en samenhang nog belangrijker. De overlegstructuur tussen de koepels en OCW die is ontstaan bij het uitwerken van deze plannen willen we structureel voortzetten.

De samenwerking met SURF is heel goed. SURF is vertegenwoordigd in de Regiegroep IBP en er wordt intensief samengewerkt in de *Innovatiezone State of the Art Cyberveiligheid*. Vrijwel alle mbo-instellingen zijn lid van SURF en met de mbo's die nog geen lid zijn, worden gesprekken gevoerd om te onderzoeken welke drempels worden ervaren en hoe die kunnen worden weggenomen. Het is in het belang van de hele mbo-sector dat alle instellingen aangesloten zijn bij SURF, al was het maar om in een crisissituatie tijdig informatie te kunnen delen via SURFcert.

De rol van Kennisnet op het gebied van IBP neemt de laatste jaren af binnen het mbo omdat de problematiek in het funderend onderwijs wezenlijk anders is dan in het mbo. Kennisnet faciliteerde in 2021 overigens nog wel een aantal activiteiten voor het mbo, waaronder de Benchmark IBP-E en de Ict-monitor. Daarnaast neemt een aantal mbo-instellingen met een VO-poot diensten af van Kennisnet/SIVON.

Onze ambities op het gebied van cyberveiligheid in het mbo

In dit onderdeel over onze ambities op het gebied van cyberveiligheid in het mbo wordt de indeling van het NIST-Cybersecurity Framework gevolgd: *identify, protect, detect, respond* en *recover*. Vanwege de grote afhankelijkheid van SaaS-diensten voegen we hier het onderwerp leveranciersmanagement aan toe.

1. Identificeren van dreigingen en risico's (*identify*)
    a. Dreigingen, risico's en maatregelen
    b. Verantwoording van de volwassenheid
2. Beschermen tegen cyberrisico's (*protect*)
    a. De factor 'mens'
    b. De factor 'techniek'
3. Detecteren van onregelmatigheden (*detect*)
4. Reageren op incidenten (*respond*)
5. Herstellen van incidenten (*recover*)
6. Leveranciersmanagement

Veel van de onderwerpen uit dit plan van aanpak komen ook aan bod in de *Innovatiezone State of the Art Cyberveiligheid* van SURF. Het mbo is goed aangesloten bij deze roadmap en bij het verder uitwerken van de Innovatiezone Cyberveiligheid door SURF wordt ook naar ons plan van aanpak en de plannen van de andere onderwijskoepels gekeken.

1. Het identificeren van risico's en het verantwoorden van de volwassenheid (*identify*)

De eerste stap in het verhogen van de digitale weerbaarheid van scholen, is het identificeren van de risico's. Een belangrijke informatiebron voor het onderwijs is het Cyberdreigingsbeeld. Deze jaarlijkse survey die door SURF wordt georganiseerd is in het najaar van 2021 door ongeveer de helft van de mbo-instellingen ingevuld. De resultaten worden door de scholen gebruikt als input voor de risicoanalyse op het gebied van informatiebeveiliging en privacy.

Voor het in kaart brengen van risico's en de daarbij passende mitigerende maatregelen wordt in het mbo met ingang van 2022 het NBA Volwassenheidsmodel Informatiebeveiliging gebruikt. Dit model is geschikt om binnen de instelling te gebruiken als roadmap op het gebied van informatiebeveiliging; het omvat voor 69 statements de risico's, de huidige volwassenheid, de gewenste volwassenheid en de maatregelen die daarvoor genomen moeten worden. Naast het gebruik van dit NBA-model als roadmap, kunnen de scores voor de 69 statements eenvoudig worden geëxporteerd ten behoeve van de benchmark. Het NBA-volwassenheidsmodel wordt namelijk vanaf 2022 gebruikt als toetsingskader Informatiebeveiliging voor de Benchmark IBP-E.

De statements binnen dit NBA-model zijn in principe allemaal van belang voor de bescherming van de privacy; informatiebeveiliging is hiervoor immers een randvoorwaarde. Toch zijn er een aantal statements die voor privacybescherming extra aandacht verdienen. Het NBA-domein Governance bijvoorbeeld, is ook voor privacy cruciaal. Niet voor niets

hebben veel onderwijsinstellingen een integraal IBP-beleid. Ook het domein *Supply Chain Management* verdient voor de bescherming van privacy extra aandacht, bijvoorbeeld op het gebied van verwerkersovereenkomsten of het uitvoeren van DPIA's en audits. Het ligt dus voor de hand om voor een aantal NBA-statements de scope uit te breiden met privacy-aspecten en/of hogere eisen te stellen aan het gewenste volwassenheidsniveau voor die statements. Deze streefniveaus per statement worden overkoepelend vastgesteld binnen de SURFaudit Maturity-werkgroep. Dat proces is inmiddels in gang gezet.

Evengoed blijft er behoefte aan een aanvullend toetsingskader op het gebied van privacy. Hiervoor is in 2016 binnen het mbo het toetsingskader Privacy ontwikkeld. De Privacy-benchmark wordt gelijktijdig met de bovengenoemde benchmark Informatiebeveiliging afgenomen. Met deze Privacy-benchmark wordt beoordeeld in hoeverre de processen voor een goede privacybescherming -en daarmee het voldoen aan de AVG- goed zijn ingeregeld. Het Privacy-toetsingskader bestaat uit 21 statements en ook hier wordt de volwassenheid van de organisatie beoordeeld op een schaal van 1-5. Het toetsingskader Privacy is echter toe aan een update en daarom is het mbo aangesloten bij een pilot in SURF-verband om een nieuw privacy toetsingskader te onderzoeken.

De resultaten van deze benchmarks op het gebied van IB en P zullen worden gebruikt om verantwoording af te leggen over de staat van de informatiebeveiliging en de borging van de privacy, zowel op instellingsniveau als sectorbreed. Hoe dat toezicht wordt vormgegeven is onderwerp van het Bestuurlijk Overleg tussen de minister van OCW en de onderwijskoepels. Omdat de nieuwe toetsingskaders informatiebeveiliging en privacy ook in het hoger onderwijs wordt gebruikt, kunnen de verschillende sectoren beter met elkaar vergeleken worden en kunnen ze van elkaar leren en samen optrekken, bijvoorbeeld op het gebied van trainingen en het inrichten van maatregelen.

a. Het identificeren van dreigingen, risico's en maatregelen

De mbo-instellingen:

- Leveren input voor het cyberdreigingsbeeld en gebruiken de gesignaleerde trends voor hun risicoanalyse.
- Hebben de risico's en de mate waarin de organisatie hiertegen bestand is in beeld, op basis van het NBA-volwassenheidsmodel en het Privacy toetsingskader.
- Hebben een roadmap waarin streefvolwassenheidsniveaus zijn bepaald inclusief de prioritering/tijdpad per onderdeel.
- Beoordelen de noodzaak voor het uitvoeren van DPIA's aan de hand van een gestandaardiseerde DPIA-checklist.
- Dienen een verzoek in voor centrale uitvoering van DPIA's via het Expertisecentrum Privacy.
- Indien centrale uitvoering niet haalbaar is voeren zij zelf DPIA's uit aan de hand van een gestandaardiseerde DPIA-aanpak.
- Gaan planmatig om met het inzetten van mitigerende maatregelen.

MBO Digitaal:

- Stimuleert deelname van de mbo's aan het SURF Cyberdreigingsbeeld en werkt mee aan de (mbo-specifieke) analyse en duiding.
- Ondersteunt de mbo's met een modelaanpak op het gebied van risicomanagement op basis van het NBA-model.
- Onderzoekt samen met SURF de mogelijkheden voor het laten ontwikkelen/aanbesteden van ondersteunende software op het gebied van risicomanagement en het documenteren van de volwassenheid en mitigerende maatregelen op het gebied van informatiebeveiliging en privacy (een ISMS-oplossing).
- Organiseert in samenwerking met SURF trainingen in het werken met het NBA-volwassenheidsmodel/toetsingskader.
- Neemt deel aan onderzoeken en pilots om te komen tot een nieuw toetsingskader voor privacy.
- Ontwikkelt samen met SURF een generieke DPIA-checklist en -aanpak.
- Organiseert/faciliteert via het Expertisecentrum Privacy de centrale uitvoering van DPIA's op veelgebruikte applicaties in het mbo.
- Onderhoudt een framework met modeldocumenten en 'good practices'.
- Organiseert kennisdeling via het netwerk IBP.

b. Het verantwoorden van de volwassenheid op het gebied van IBP

De mbo-instellingen:

- Leveren op basis van het NBA-toetsingskader en het Privacy-toetsingskader hun actuele volwassenheidsniveau ten behoeve van de jaarlijkse Benchmark IBP-E.
- Werken mee aan de onafhankelijke beoordeling van hun scores in de vorm van peerreviews of externe audits.
- Rapporteren volgens een vastgesteld format over hun volwassenheid in hun jaarrapportage.

MBO Digitaal:

- Stemt af met de Regiegroep IBP in het mbo en het ministerie van OCW over het streef-volwassenheidsniveau en het tijdpad om dat te bereiken en laat dit vaststellen door de ALV van de MBO Raad.
- Organiseert jaarlijks de Benchmark IBP-E.
- Organiseert aansluitend de (peer)review.
- Faciliteert inzet van IT-auditors voor het uitvoeren van reviews en externe audits, zo mogelijk samen met SURF.
- Verzorgt de rapportage en deelt de sector-brede bevindingen en trends met het Netwerk IBP en andere stakeholders.
- Stemt af met het ministerie van OCW en de MBO Raad over een uniform rapportageformat t.b.v. de IBP-jaarrapportage van de mbo-instellingen. Met name de vertrouwelijkheid van deze gegevens is een aandachtspunt. Dit rapportageformat wordt vastgesteld door de ALV van de MBO Raad.

2. Het beschermen tegen cyberrisico's (*protect*)

De dreigingen zijn heel divers en informatiebeveiliging bestrijkt dus vele gebieden. Het eerdergenoemde Volwassenheidsmodel Informatiebeveiliging omvat 15 domeinen, van Governance, Risk Management en Human Resources tot Security Management en Supply Chain Management. Dat betekent dat er zowel aan bewustwording als aan harde techniek moet worden gewerkt. De medewerkers in de mbo-instellingen moeten zich ervan bewust zijn dat cyberveiligheid geen exclusieve IT-aangelegenheid is maar een onderwerp waarbij iedereen in de organisatie een rol heeft. Parallel aan dit programma worden daarom activiteiten opgestart die zich concentreren op de professionalisering van docenten op het gebied van digitaal veilig onderwijs. Binnen dat programma wordt bijvoorbeeld een Onderzoekswerkplaats Digitale Veiligheid opgezet. Waar mogelijk wordt de verbinding gemaakt met ons programma Cyberveiligheid in het mbo.
Tegelijkertijd worden er van de IT-afdeling state-of-the-art oplossingen verwacht op het gebied van netwerksegmentering, backup-strategieën, SIEM/SOC oplossingen enzovoort.

a. De factor 'mens'

De mbo-instellingen:

- Borgen dat hun senior-management (bestuur, lijn- en onderwijsmanagers) actief betrokken is bij de informatiebeveiliging en de bescherming van privacy, vooral waar het gaat om risicomanagement.
- Werken planmatig aan de awareness van hun medewerkers, zowel op het gebied van informatiebeveiliging als privacy, op alle niveaus en afdelingen van de organisatie, rekening houdend met actuele trends en dreigingen.
- Ondersteunen docenten bij de inzet van educatieve tools om daarbij verantwoorde keuzes te kunnen maken op het gebied van de bescherming van de privacy van docenten en studenten.

MBO Digitaal:

- Informeert bestuurders over ontwikkelingen op het gebied van cyberveiligheid via ALV- en regiobijeenkomsten.
- Stimuleert de deelname aan awarenessprogramma's zoals Cybersave Yourself (SURF).
- Organiseert (nul-)metingen met betrekking tot awareness, deelt deze bevindingen met de mbo-instellingen en gebruikt deze om accenten te leggen binnen dit programma.
- Faciliteert kennisdeling over awareness-activiteiten op het gebied van informatiebeveiliging en privacy via het Expertisecentrum Privacy en het Netwerk IBP.
- Stimuleert kennisuitwisseling tussen de netwerken op het gebied van onderwijs en ict en het netwerk IBP.
- Ontwikkelt het Toolwiel voor onderwijs-apps.

b. De factor 'techniek'

De mbo-instellingen:

- Hebben sleutelfuncties en/of -rollen op het gebied van IBP belegd (zoals de CISO).
- Hebben hun netwerkinfrastructuur en applicatielandschap volledig in beeld, bij voorkeur aan de hand van de mbo-referentiearchitectuur MORA.

- Hebben hun basis op orde: toegangsbeveiliging, backup-, patchmanagement etc.
- Nemen op basis van hun risicoanalyse de benodigde mitigerende maatregelen.
- Controleren hun weerbaarheid, o.a. door de inzet van pentests en red team oefeningen en nemen de bevindingen mee in een verbetercyclus.

MBO Digitaal en SURF:

- Bieden concrete ondersteuning voor de mbo's op het gebied cyberveiligheid en privacy via een Expertisecentrum Informatiebeveiliging.
- Stellen sleutelrollen zoals een (C)ISO of een IT-auditor "as a service" beschikbaar, zodat deze rollen gedeeld kunnen worden door meerdere instellingen.
- Ondersteunen de mbo's bij het uniform beschrijven van hun netwerkinfrastructuur en applicatielandschap.
- Faciliteren kennisdeling op het gebied van mitigerende maatregelen.
- Stimuleren de inzet van vulnerability scans, pentests en red teaming oefeningen door hiervoor diensten aan te besteden, te bemiddelen of deze zelf te organiseren.
- Werken sectorbreed aan de veilige uitwisseling van gegevens in de (leermiddelen)keten, bijvoorbeeld door het ondersteunen van de Open Onderwijs API.

3. Het detecteren van onregelmatigheden (*detect*)

Het is cruciaal om verdachte netwerkactiviteit in een vroeg stadium te signaleren door middel van SIEM/SOC oplossingen. Ook de mbo's kunnen daar niet omheen maar staan wel voor een uitdaging: de initiële kosten zijn hoog en er is expertise nodig om een SOC binnen de eigen organisatie te implementeren. Voor de opvolging van meldingen uit het SOC is structureel formatie nodig. We onderzoeken samen met SURF op welke manier ook kleinere instellingen gebruik kunnen maken van een SOC. Mogelijk kunnen mbo-instellingen ook op dit gebied samenwerken en kan de opvolging van de logging (gezamenlijk) als een service worden afgenomen. Een volledige beschrijving van de IT-omgeving en een zoveel mogelijk uniforme IT-inrichting helpen bij die samenwerking.

De mbo-instellingen:

- Hebben hun netwerkinfrastructuur en applicatielandschap volledig in beeld, bij voorkeur aan de hand van de mbo-referentiearchitectuur MORA.
- Sluiten zich aan op een SOC en richten voor de opvolging van de signalen een passende werkwijze in.

MBO Digitaal en SURF:

- Faciliteren kennisdeling op het gebied van de implementatie van een SOC.
- Nemen drempels voor toetreding tot SURFsoc weg, door het vergoeden van de entreekosten en het ondersteunen van de mbo-instellingen bij de implementatie.
- Onderzoeken aanvullende dienstverlening voor de opvolging van meldingen uit het SOC, bijvoorbeeld door dit gemeenschappelijk te regelen of het als een aanvullende service aan te bieden.

4. Het reageren op incidenten (*respond*)

Om snel te kunnen reageren op een cybercrisis is het belangrijk dat er een crisisplan klaarligt waarmee ook geoefend is. Veel mbo-instellingen hebben dit nog niet goed op orde en we gaan dit binnen de sector oppakken door kennis, 'best practices' en een modelaanpak te delen. Daarnaast stimuleren we de deelname aan trainingen voor het opzetten van crisismanagementteams. Het is vervolgens belangrijk om te oefenen op dit gebied; voor de instellingen zelf en voor de sector als geheel. Daarvoor worden jaarlijks de cybercrisisoefeningen OZON en NOZON georganiseerd door SURF.
Op het gebied van incidentrespons en cyber forensics is het belangrijk dat alle mbo's contracten afsluiten met dienstverleners op dit gebied.
Tenslotte is het cruciaal dat tijdens een cybercrisis de beschikbare informatie zoals de IoC's snel wordt gedeeld. SURFcert voorziet hierin als CERT voor de onderwijssector en het is alleen al daarom van essentieel belang dat alle mbo-instellingen lid zijn van SURF.

De mbo-instellingen:

- Hebben een cybercrisisplan.
- Hebben een cybercrisisorganisatie geformeerd en getraind.
- Voeren regelmatig cybercrisisoefeningen uit, bij voorkeur in OZON-verband.
- Hebben overeenkomsten afgesloten met externe partijen op het gebied van incidentrespons en cyber forensics.
- Zijn lid van SURF, zodat zij deel kunnen nemen aan cruciale diensten als SURFcert.

MBO Digitaal en SURF:

- Delen 'best practices' op het gebied van crisisorganisatie en crisisplannen via het Framework IBP.
- Faciliteren trainingen voor het opzetten van incident response teams, bijvoorbeeld de Transits-trainingen.
- Organiseren cybercrisisoefeningen (OZON/NOZON) en stimuleren de deelname hieraan door de mbo's.
- Faciliteren Red Teaming oefeningen en delen de geleerde lessen via het Netwerk IBP.
- Delen kwetsbaarheden, bijvoorbeeld via SURFcert en adviseren over mitigerende maatregelen (via het Expertisecentrum Informatiebeveiliging en Expertisecentrum Privacy).
- Gaan in gesprek met mbo-instellingen die nog geen lid zijn van SURF om te onderzoeken welke drempels er worden ervaren en hoe deze weggenomen kunnen worden.

5. Het herstellen van incidenten (*recover*)

Als een instelling slachtoffer is geworden van een cyberincident is het zaak om de schade te beperken en zo snel mogelijk weer door te kunnen werken. Binnen de onderwijssector wordt er in principe niet toegegeven aan afpersing en om dat waar te kunnen maken is het belangrijk om elkaar uitwijkopties te bieden. De uitwerking hiervan wordt binnen de MBO Raad op bestuurlijk niveau besproken. Ook onderzoeken we de mogelijkheden voor een calamiteitenfonds als alternatief voor cyberverzekeringen.
Verder is het belangrijk dat de 'lessons-learned' met elkaar worden gedeeld, waardoor de sector als geheel weerbaarder wordt. Een goed voorbeeld hiervan is de versnelde invoering

van multi-factor authenticatie (MFA) voor studenten bij veel mbo-instellingen, naar aanleiding van de geleerde lessen bij ROC Mondriaan.

De mbo-instellingen:
- Maken op bestuurlijk niveau afspraken over het elkaar bieden van uitwijkopties en andere vormen van ondersteuning bij een cybercrisis.
- Onderzoeken de mogelijkheid voor het oprichten van een calamiteitenfonds als alternatief voor cyberverzekeringen.
- Delen hun aanpak/ervaringen bij het herstellen van eventuele incidenten met de sector.

MBO Digitaal:
- Organiseert het proces voor de hierboven genoemde zaken en werkt e.e.a. uit in businesscases, convenanten, reglementen en dergelijke.
- Faciliteert kennisdeling, samenwerking en besluitvorming op het gebied van cyberincidenten op operationeel, tactisch en strategisch niveau.
- Neemt zo nodig en eventueel aanvullend op SURFcert een coördinerende rol bij sectorbrede incidenten, via het security- en/of Expertisecentrum Privacy.

6. Leveranciersmanagement

Omdat veel onderwijsinstellingen gebruikmaken van SaaS-oplossingen gelden veel van bovenstaande eisen ook voor deze dienstverleners. Goede contracten zijn cruciaal en op de naleving ervan moet worden toegezien. Ook moet er aandacht zijn voor de veiligheid van de gegevenskoppelingen met deze externe partijen. Aangezien veel mbo-instellingen voor hun kroonjuwelen gebruikmaken van dezelfde applicaties, ligt het voor de hand om hierin samen op te trekken. Vanuit ons netwerk zetten we in op het gebruik van standaard inkoopovereenkomsten en standaard verwerkersovereenkomsten, waarvan de bepalingen uit de beveiligingsbijlage voor de gehele sector met de leverancier worden onderzocht, onderhandeld en vastgelegd. Een en ander in overleg met het platform voor de educatieve keten Edu-K.
Om te toetsen of leveranciers zich houden aan de voorwaarden in deze verwerkersovereenkomsten gaan we de uitvoering van pentests en audits coördineren. Ook de DPIA's op veelgebruikte digitale leermiddelen worden centraal uitgevoerd. Voor de budgetten die gemoeid zijn met het centraal beoordelen van verwerkersovereenkomsten, het uitvoeren van audits, pentests en DPIA's wordt subsidie aangevraagd via OCW.
Om te kunnen bepalen voor welke applicaties (centraal) verwerkersovereenkomsten moeten worden voorbereid en welke leveranciers worden ge-audit is het belangrijk om inzicht te hebben in het gebruik van software door de mbo-instellingen. Dit wordt bij de start van dit programma geïnventariseerd en er wordt een structurele oplossing onderzocht in de vorm van een sectorbrede softwarecatalogus. Een dergelijke softwarecatalogus is ook belangrijk om snel de impact te kunnen bepalen en te kunnen reageren wanneer bij leveranciers calamiteiten optreden (bijvoorbeeld het incident met Log4J).

De mbo-instellingen:
- Brengen gezamenlijk in kaart welke applicaties worden gebruikt in de mbo-sector zodat een dekkend beeld ontstaat van de belangrijkste leveranciers.

MBO Digitaal en SURF:

- Inventariseren welke applicaties veel worden gebruikt binnen het mbo.
- Werken een programma van eisen uit voor een sectorbrede softwarecatalogus, die voor het mbo goed aansluit op de referentiearchitectuur (MORA) en onderzoeken op welke manier deze kan worden gerealiseerd.
- Ondersteunen de ontwikkeling van veilige koppelingen voor gegevensuitwisseling in de (leermiddelen)keten.
- Stemmen af met het Netwerk IBP over gezamenlijke audit-activiteiten en leggen deze vast in een audit-plan. Het beschikbaar maken van auditcapaciteit werd al eerder genoemd.
- Richten een centrale voorziening in voor het beoordelen van verwerkersovereenkomsten voor de veel gebruikte softwareapplicaties.
- Organiseren audits, pentests en DPIA's voor veelgebruikte softwarepakketten en stellen de bevindingen breed beschikbaar, inclusief adviezen over de opvolging van de uitkomsten van zo'n audit of DPIA.
- Organiseren een IT-auditvoorziening voor het onderwijs, die naast deze leverancier-audits ook een rol kan spelen bij de audits van de onderwijsinstellingen.

Uitwerking van de doelstellingen, maatregelen en activiteiten

Bij onze ambities op het gebied van cyberveiligheid in het mbo zijn bij elk van de zes onderwerpen een aantal doelstellingen, maatregelen en activiteiten benoemd. We geven hiermee een concreet beeld van onze ideeën, maar moeten er rekening mee houden dat accenten gaan verschuiven. Naar aanleiding van de casus Mondriaan stond het onderwerp MFA voor studenten opeens volop in de belangstelling en na de Log4J kwetsbaarheid kreeg leveranciersmanagement extra aandacht. Hoewel de waan van de dag nooit leidend mag zijn, is het wel belangrijk om dit plan van aanpak niet in beton te gieten en ruimte te laten voor nieuwe inzichten.

De belangrijkste activiteiten uit het vorige hoofdstuk die voor rekening van MBO Digitaal, MBO Raad en/of SURF komen hebben we samengevat in 22 projectactiviteiten. Deze vormen de basis voor ons programma en zijn verder uitgewerkt in bijlage A. In bijlage B zijn ze voor de subsidieaanvraag in vier categorieën gegroepeerd.

1. Aanscherpen mbo-sectorbeeld en verder concretiseren van dit plan
2. Wegnemen drempels voor lidmaatschap SURF
3. Aanpassen en uitbreiden Framework IBP
4. Trainingen NBA-volwassenheidsmodel en toetsingskader
5. Tooling voor het NBA-volwassenheidsmodel/benchmark
6. Onderzoek nieuw privacykader
7. Onderzoek cybercrisis-convenant mbo
8. Onderzoek calamiteitenfonds cyberincidenten
9. Centraal uitvoeren van DPIA's
10. Centraal beoordelen van verwerkersovereenkomsten/beveiligingswaarborgen
11. Gecoördineerd uitvoeren van audits en pentests bij leveranciers
12. Beschikbaar maken van auditcapaciteit voor benchmarks/reviews en IT-audits
13. Gezamenlijk aanbesteden vulnerability scans en pentests
14. Gezamenlijk aanbesteden security incident response en cyber forensics
15. Gezamenlijk uitvoeren van cybercrisisoefeningen
16. Ondersteunen bij de invoering van SURFsoc
17. Onderzoek naar een sectorbrede softwarecatalogus
18. Onderzoek en ontwikkeling van veilige koppelingen voor gegevensuitwisseling in de (leermiddelen)keten.
19. Doorontwikkelen van het Toolwiel voor onderwijsapps
20. Afstemmen ambitieniveau en uniforme IBP-rapportage voor verantwoording
21. Oprichten van een Expertisecentrum Informatiebeveiliging voor het mbo*
22. Oprichten van een Expertisecentrum Privacy voor het mbo*

* Vanuit het Expertisecentrum Informatiebeveiliging en het Expertisecentrum Privacy worden veel van de genoemde activiteiten aangestuurd of uitgevoerd.

Verantwoording van de resultaten

Het effect van deze projectactiviteiten meten bij voorkeur door goed zicht te houden op de volwassenheid van de scholen op basis van het NBA Volwassenheidsmodel en het Privacykader. We sturen er daarom op dat de instellingen deze kaders niet alleen gebruiken als toetsingskaders voor de benchmarks, maar daarnaast als instrument om actuele stand van de volwassenheid en maatregelen te documenteren. Op die manier kan ook tussentijds voortgang worden gemeten en kunnen knelpunten op specifieke onderdelen van het programma worden gesignaleerd. Het dynamische sectorbeeld dat op deze manier ontstaat kan dienen als input voor de gesprekken over cyberveiligheid, die de minister van OCW tweemaal per jaar wil voeren met de branches van onderwijsinstellingen.

Tijdpad voor de volwassenheid Informatiebeveiliging

Het mbo start dit jaar met het nieuwe NBA-toetsingskader informatiebeveiliging en sluit daarmee aan bij het hoger onderwijs, waar het al sinds 2019 gebruikt wordt. Ook qua ambitieniveau voor de volwassenheid wil het mbo samen met het hoger onderwijs optrekken. Zo is de doelstelling van het hoger onderwijs dat in het voorjaar van 2024 elke instelling minimaal een gemiddeld volwassenheidsniveau van 3,0 scoort op het toetsingskader informatiebeveiliging. Voor het mbo geldt eveneens het ambitieniveau van 3,0 waarbij we nog onderzoeken wat voor het mbo een realistisch tijdpad is. Ervaringen uit de pilots die binnen het mbo met het nieuwe toetsingskader zijn uitgevoerd in het najaar van 2021 laten zien dat er voor ongeveer een derde van de 69 criteria veel werk verzet moet worden binnen de mbo-instellingen, bijvoorbeeld omdat ze in het oude toetsingskader niet voorkwamen. Wat dat betreft loopt het hoger onderwijs twee jaar voor op het mbo. Omdat het mbo de benchmark jaarlijks uitvoert kan in meerdere stappen naar het ambitieniveau in 2024 worden toegewerkt. Eerst stellen we het tussendoel vast voor het voorjaar van 2023 en daarna -als we beter kunnen inschatten wat haalbaar is- het niveau dat de mbo’s in het voorjaar van 2024 gemiddeld bereikt moeten hebben. Mocht niveau 3 dan nog niet haalbaar zijn, kunnen we in ieder geval wel de uitspraak doen wanneer dat wel het geval zal zijn.
Om historisch te kunnen vergelijken zijn de statements in het nieuwe toetsingskader gekoppeld aan de clusterindeling van het oude toetsingskader. Zo blijft met het nieuwe toetsingskader de ontwikkeling van de scores vanaf 2015 op clusterniveau zichtbaar.

Tijdpad voor de volwassenheid Privacy

Op basis van het huidige toetsingskader Privacy lijkt het haalbaar dat in het voorjaar van 2024 elke instelling minimaal een gemiddeld volwassenheidsniveau van 3,0 scoort op het toetsingskader privacy. Echter wordt nu voor dit toetsingskader onderzocht of een gezamenlijk privacykader met het hoger onderwijs mogelijk is. Mocht er in 2023 worden overgestapt naar een nieuw privacykader dan lijkt het niet realistisch om al een doelstelling voor de volwassenheid vast te stellen voor 2024.

De governance van het programma

Het programma Cyberveiligheid mbo dat zal worden opgestart naar aanleiding van dit plan van aanpak wordt als volgt aangestuurd.

Programmamanager

- Voor de algehele coördinatie van dit programma wordt een programmamanager aangetrokken.

Stuurgroep

- Bert Beun (bestuur MBO Raad): neemt namens de mbo-sector deel aan het Bestuurlijk Overleg met OCW.
- Martijn Timmer (MBO Raad): namens het MT van de MBO Raad
- Hans Louwhoff (SURF): namens het MT van SURF
- Programmamanager (vacature)

Kernprojectgroep

- Martijn Bijleveld (MBO Digitaal)
- Peter Vermeijs (MBO Raad)
- Programmamanager (vacature)

Projectteams

- Voor de grootschalige activiteiten, zoals het Expertisecentrum Informatiebeveiliging, het Expertisecentrum Privacy of een omvangrijk project zoals de sectorbrede softwarecatalogus worden afzonderlijke projectteams opgestart.

Klankbordgroepen

- Regiegroep netwerk IBP
- FG-groep netwerk IBP
- Contactpersonen SURF (CSC's)

Voor de afstemming met de VH en de UNL (en SURF) is wordt 4x per jaar overlegd, of vaker indien nodig.

Voor de afstemming van dit programma met de Innovatiezone Cyberveiligheid van SURF hebben de programmamanagers regelmatig overleg. Daarbij is een lid van de regiegroep IBP afgevaardigd in de regiegroep van de Innovatiezone.

We hebben in het hoofdstuk over samenwerking in de mbo-sector al aangegeven dat de besluitvorming over IBP binnen het mbo met ingang van 2022 anders wordt georganiseerd. Voor belangrijke besluiten, zoals over het ambitieniveau of een cyberconvenant, kan de stuurgroep bepalen dat hierover door de ALV van de MBO Raad een besluit moet worden genomen.

Conclusie

We hebben in dit plan van aanpak aangegeven waar we als mbo-sector staan op het gebied van cyberveiligheid, naar welke doelen wij gezamenlijk willen toewerken en op welke manier we die voortgang willen verantwoorden, individueel, naar elkaar toe en richting het ministerie van OCW. We doen dat aan de hand van het volwassenheidsniveau van de mbo-instellingen op basis van de toetsingskaders op het gebied van informatiebeveiliging en privacy. Voor het onderdeel informatiebeveiliging is dat het NBA Volwassenheidsmodel Informatiebeveiliging. Dit nieuwe toetsingskader wordt in 2022 voor het eerst breed gebruikt in het mbo. Voor de volwassenheid van de organisatie op het gebied van de privacybescherming wordt het privacy-toetsingskader gebruikt, waarvoor een nieuwe versie wordt onderzocht in het najaar van 2022.

Als ambitieniveau voor de Benchmark IBP-E hanteert de mbo-sector op dit moment een gemiddelde volwassenheid van 3,0 gemeten over alle instellingen, over alle statements van de toetsingskaders. De mbo's komen in 2021 op het gebied van informatiebeveiliging met een ruime 2,8 gemiddeld genomen dicht in de buurt van dat ambitieniveau. Diezelfde ambitie geldt voor het privacy-kader. In 2021 kwamen de mbo's gezamenlijk voor privacy gemiddeld uit op een 2,9.

Voor het nieuwe NBA-toetsingskader voor informatiebeveiliging geldt eveneens het ambitieniveau van 3,0 maar moeten we rekening houden met een aanvankelijke, tijdelijke terugval in volwassenheid vanwege het gebruik van deze nieuwe meetlat. We willen 2022 gebruiken als overgangsjaar en in het voorjaar van 2023 een besluit nemen over een realistisch streefniveau voor het voorjaar van 2024.

Voor het privacykader is nog geen besluit genomen over een nieuwe versie. Voorlopig gaan we uit van het gebruik van de huidige mbo-versie, die al sinds 2016 in gebruik is. Het ambitieniveau van 3,0 gemiddeld voor elke mbo-instelling lijkt een haalbare doelstelling voor 2024. Mocht echter worden besloten voor eerdere invoering van een nieuw privacykader kunnen we ons nog niet committeren aan een minimaal volwassenheidsniveau.

De mbo's staan voor een flinke uitdaging om de cyberveiligheid te verhogen en aan het ambitieniveau van 3,0 te voldoen. Dit vergt de komende jaren een enorme inspanning die niet zonder meer met de bestaande middelen kan worden gerealiseerd. Dit plan voorziet in die ondersteuning. Door centraal een budget voor de hele mbo-sector te organiseren kan meer impact gemaakt worden en worden we uitgedaagd om dit gezamenlijk op te lossen.

Dit is een plan van- en voor meer dan 50 individuele mbo-instellingen, die ieder hun eigen verantwoordelijkheid hebben op het gebied van cyberveiligheid. Het is een uitdaging om hen allen op dit plan aangesloten te krijgen; dit vergt een gezamenlijke verantwoordelijkheid van de mbo-instellingen en een gedeelde visie vanuit het ministerie van OCW, zodat we deze belangrijke missie samen succesvol kunnen aanpakken.

Bijlage A: (project)activiteiten

In het hoofdstuk over onze ambities op het gebied cyberveiligheid zijn diverse oplossingen genoemd om de cyberveiligheid te verhogen. We hebben de belangrijkste hier bij elkaar gezet en enigszins uitgewerkt. Veel van de activiteiten vergen nader onderzoek en afstemming en zullen als afzonderlijke projecten/programma's worden uitgewerkt. Veel van de activiteiten zullen worden uitgevoerd binnen het Expertisecentrum Informatiebeveiliging (21) en het Expertisecentrum Privacy (22).

1. Aanscherpen mbo-sectorbeeld en verder concretiseren van dit plan
2. Wegnemen drempels voor lidmaatschap SURF
3. Aanpassen en uitbreiden Framework IBP
4. Trainingen NBA-volwassenheidsmodel en toetsingskader
5. Tooling voor het NBA-volwassenheidsmodel/benchmark
6. Onderzoek nieuw privacykader
7. Onderzoek cybercrisis-convenant mbo
8. Onderzoek calamiteitenfonds cyberincidenten
9. Centraal uitvoeren van DPIA's
10. Centraal beoordelen van verwerkersovereenkomsten/beveiligingswaarborgen
11. Gecoördineerd uitvoeren van audits en pentests bij leveranciers
12. Beschikbaar maken van auditcapaciteit voor benchmarks/reviews en IT-audits
13. Gezamenlijk aanbesteden vulnerability scans en pentests
14. Gezamenlijk aanbesteden security incident response en cyber forensics
15. Gezamenlijk uitvoeren van cybercrisisoefeningen
16. Ondersteunen bij de invoering van SURFsoc
17. Onderzoek naar een sectorbrede softwarecatalogus
18. Ontwikkeling van koppelingen voor gegevensuitwisseling in de (leermiddelen)keten.
19. Doorontwikkelen van het Toolwiel voor onderwijsapps
20. Afstemmen ambitieniveau en uniforme IBP-rapportage voor verantwoording
21. Oprichten van een Expertisecentrum Informatiebeveiliging voor het mbo
22. Oprichten van een Expertisecentrum Privacy voor het mbo

1. Aanscherpen sectorbeeld en verder concretiseren van dit plan

Om te zorgen dat dit plan goed aansluit bij de behoeften vanuit de mbo-instellingen organiseren we vanuit MBO Digitaal een uitvraag naar de belangrijkste knelpunten op het gebied van informatiebeveiliging en privacy. Daarbij betrekken we ook de strategische sleutelrollen op het gebied van cyberveiligheid: CIO's, CISO's, FG's en bestuurders. We stemmen dit plan daarop verder af. Voor de coördinatie van dit plan zal een programmamanager worden aangetrokken.

➢ Uitgevoerd door: MBO Digitaal.

2. Wegnemen drempels voor lidmaatschap SURF

Het is in ieders belang dat alle mbo-instellingen lid zijn van SURF. Naast het kunnen deelnemen aan de communities van SURF, het kunnen afnemen van diensten als SURFsoc is

ook de toegang tot SURFcert cruciaal. SURF overlegt met de mbo-instellingen die nog geen lid zijn, welke drempels eventueel kunnen worden weggenomen.

- Uitgevoerd door: SURF

3. Aanpassen en uitbreiden Framework IBP

Sinds 2015 beheren we binnen het netwerk IBP een documentenbibliotheek: het Framework IBP. Hierin zijn modeldocumenten, invulformats, handreikingen en good practices op het gebied van informatiebeveiliging en privacy overzichtelijk bij elkaar gebracht. Een groot deel van deze documenten is verouderd, zeker nu we binnen de mbo-sector overstappen naar een nieuw toetsingskader voor informatiebeveiliging. Voor een succesvolle invoering van het NBA-toetsingskader is een actueel Framework IBP cruciaal en we zetten daarom in op een grondige update.

- Uitgevoerd door: MBO Digitaal en SURF, aangevuld met externe inhuur

4. Trainingen NBA-volwassenheidsmodel en toetsingskader

In samenwerking met SURF worden sinds medio 2021 één- en tweedaagse trainingen verzorgd over het nieuwe toetsingskader informatiebeveiliging, volgens het NBA-model. Deze trainingen worden ook in 2022 doorgezet, waarbij ze ook gericht worden op andere doelgroepen, zoals FG's en privacy-officers, interne auditors en lijnmanagers. De trainingen worden (door)ontwikkeld door MBO Digitaal en SURF en worden kostendekkend uitgevoerd door SURF.

- Uitgevoerd door: MBO Digitaal en SURF

5. Tooling voor het NBA-volwassenheidsmodel/benchmark

We onderzoeken samen met SURF de mogelijkheden voor de inzet van laagdrempelige tooling voor het beheren van risico's, volwassenheidsniveaus en maatregelen door de mbo-instellingen, zowel op het gebied van informatiebeveiliging als privacy. Deze tool helpt de instellingen bij het plannen en bewaken van maatregelen en het documenteren van hun volwassenheid. Daarbij kan de software, in een gestandaardiseerd format, eenvoudig de scores voor benchmark IBP aanleveren. Op deze manier kan die uitwisseling ook meerdere keren per jaar plaatsvinden, waardoor de ontwikkeling van de volwassenheid, desgewenst op domein- of statementniveau, sectorbreed gemonitord kan worden.

- Uitgevoerd door: MBO Digitaal en SURF (Innovatiezone Cyberveiligheid)

6. Onderzoek nieuw privacykader

In samenwerking met SURF wordt onderzoek gedaan naar een nieuw privacykader. Het huidige mbo-privacykader is aan een update toe en er is behoefte om ook op privacygebied samen op te trekken met het hoger onderwijs.

- Uitgevoerd door: MBO Digitaal en SURF (SURFaudit)

7. Onderzoek cybercrisis-convenant mbo

We onderzoeken de wenselijkheid voor een convenant waarbinnen op bestuurlijk niveau afspraken gemaakt worden over hoe de mbo-sector wil handelen bij een cybercrisis, bijvoorbeeld over niet-betalen bij afpersing en/of elkaar uitwijkopties bieden.

- Uitgevoerd door: MBO Raad

8. Onderzoek calamiteitenfonds cyberincidenten

We inventariseren de behoefte aan een calamiteitenfonds voor cyberincidenten, vervolgens wordt onderzocht op welke manier deze voorziening juridisch kan worden geborgd, welke omvang benodigd is en welke eisen passend zijn voor deelname aan het calamiteitenfonds.

- Uitgevoerd door: MBO Raad

9. Centraal uitvoeren van DPIA's

De scholen komen zelf onvoldoende toe aan het uitvoeren van DPIA's en voor de grote systemen is dat voor individuele instellingen ook niet haalbaar. Dit vraagt om het centraal uitvoeren van DPIA's. De coördinatie wordt belegd bij het nog op te richten Expertisecentrum Privacy. Uitvoering van de DPIA's gebeurt bij voorkeur door/samen met SURF, met inschakeling van externe partijen. Waar mogelijk treken we samen op met het funderend onderwijs en het hoger onderwijs.
Voor de leveranciers die op kleinere schaal in het mbo vertegenwoordigd zijn ontwikkelen we een gestandaardiseerde DPIA-aanpak, waarmee de scholen deze kleinschalige DPIA's zelf kunnen uitvoeren.

- Uitgevoerd door: MBO Digitaal en SURF (Innovatiezone Cyberveiligheid)

10. Centraal beoordelen van verwerkersovereenkomsten/beveiligingswaarborgen

We gaan het proces om te komen tot een goede verwerkersovereenkomst, inclusief de bepalingen in de beveiligingsbijlage, centraal organiseren voor de veelgebruikte softwarepakketten in het mbo. Het gaat dan om afstemming/onderhandeling over certificering, audits, aansprakelijkheid en het zover mogelijk invullen van deze modelovereenkomsten. Deze centrale aanpak is efficiënt voor de scholen en de leveranciers. Deze werkzaamheden worden uitgevoerd binnen het nog op te richten Expertisecentrum Privacy.

- Uitgevoerd door: MBO Digitaal en SURF (Innovatiezone Cyberveiligheid)

11. Gecoördineerd uitvoeren van audits en pentests bij leveranciers

Omdat het merendeel van onze applicaties in de cloud draait, is het belangrijk om de beveiligingswaarborgen van deze leveranciers goed te monitoren. Hierbij gaat het om audits en pentests. We leggen een lijst aan van leveranciers en maken een auditplan. Dit wordt gecoördineerd vanuit het nog op te richten Expertisecentrum Privacy. Samen met SURF zoeken we partijen om deze activiteiten uit te voeren.

- Uitgevoerd door: MBO Digitaal en SURF (Innovatiezone Cyberveiligheid)

12. Beschikbaar maken van auditcapaciteit voor benchmarks/reviews en IT-audits

De behoefte aan een onafhankelijke beoordeling van de benchmarks neemt toe en daarbij houden we rekening met de mogelijkheid om (een deel van) de instellingen extern te laten auditen. We onderzoeken op welke manier we de inzet van auditors laagdrempeliger beschikbaar kunnen maken voor de mbo-instellingen, mogelijk kunnen we zelf auditors aannemen en ze inzetten via het cyber/Expertisecentrum Privacy.

- Uitgevoerd door: MBO Digitaal en SURF (Innovatiezone Cyberveiligheid)

13. Gezamenlijk aanbesteden vulnerability scans en pentests

Om de weerbaarheid van de scholen goed te kunnen beoordelen is het belangrijk om regelmatig op kwetsbaarheden te scannen. SURF heeft hiervoor in het verleden een aanbesteding gedaan, waaraan beperkt door mbo-instellingen is deelgenomen. We gaan de mbo-instellingen informeren en in overleg SURF opnieuw een interessepeiling en zo nodig een nieuwe aanbesteding uitvoeren.

- Uitgevoerd door: MBO Digitaal en SURF (Innovatiezone Cyberveiligheid)

14. Gezamenlijk aanbesteden security incident response en cyber forensics

Als een instelling wordt getroffen door een cyberaanval is het belangrijk om snel expertise te kunnen inschakelen om de schade te beperken en (forensisch) onderzoek te doen. Hiervoor is eerder een aanbesteding gedaan, we onderzoeken welke scholen nog niet voorzien zijn en organiseren samen met SURF een passend aanbod voor deze scholen.

- Uitgevoerd door: MBO Digitaal en SURF (Innovatiezone Cyberveiligheid)

15. Gezamenlijk uitvoeren van cybercrisisoefeningen

Om beter te zijn voorbereid op een cybercrisis is het belangrijk om te oefenen. Ongeveer een vijfde van de mbo's doet mee aan crisisoefening (N)OZON. We gaan de deelname van de mbo's verhogen door de mbo's vanuit MBO Digitaal te stimuleren en waar nodig te ondersteunen bij de voorbereiding van (N)OZON. Daarnaast gaan we Red Teaming oefeningen organiseren, zo mogelijk binnen de Innovatiezone Cyberveiligheid.
De belangrijkste lessen vanuit deze oefeningen worden door MBO Digitaal verzameld en gedeeld binnen het netwerk IBP.

- Uitgevoerd door: MBO Digitaal en SURF (Innovatiezone Cyberveiligheid)

16. Ondersteunen bij de invoering van SURFsoc

Voor veel mbo-instellingen zijn de benodigde expertise en de kosten voor SURFsoc een te hoge drempel. We onderzoeken samen met SURF en de mbo-instellingen welke ondersteuning voor de mbo-instellingen nodig is, zowel bij de implementatie als voor de meer structurele opvolging van de meldingen uit het SOC. We ondersteunen de mbo-instellingen bij de implementatie en dragen financieel bij in de opstartkosten.

- Uitgevoerd door: MBO Digitaal en SURF (Innovatiezone Cyberveiligheid)

17. Onderzoek naar een sectorbrede softwarecatalogus

Om inzage te krijgen in de door de instellingen gebruikte softwarepakketten is er behoefte aan een sectorbrede onderwijscatalogus. Op die manier kan de informatievoorziening en samenwerking tussen instellingen en met leveranciers worden bevorderd. Doordat er inzicht is in het gebruik van softwarepakketten kan worden bepaald voor welke pakketten met voorrang DPIA's, audits en/of pentests centraal moeten worden georganiseerd. Mocht er een kwetsbaarheid in een applicatie naar voren komen dan kan snel gecommuniceerd en ingegrepen worden.

- Uitgevoerd door: MBO Digitaal, SURF en Kennisnet/SIVON

18. Ontwikkelen van koppelingen voor gegevensuitwisseling in de (leermiddelen)keten.

Meedenken/werken aan de veilige gegevensuitwisseling in de leermiddelenketen, in samenhang met de (mbo) sectorarchitectuur. Een concreet voorbeeld hiervan is de Open Onderwijs API. We ondersteunen de ontwikkeling van de OOAPI als good-practice van vruchtbare samenwerking tussen leveranciers en de mbo-instellingen. Daarnaast zijn we betrokken bij diverse landelijke ontwikkelingen op het gebied van de digitale leermiddelenketen, zoals de Digitaliseringsimpuls Digitale leermaterialen.

- Uitgevoerd door: MBO Digitaal

19. Doorontwikkelen van het Toolwiel voor onderwijsapps

Het Toolwiel is een instrument om docenten te helpen veilige keuzes te maken bij de inzet van digitale tools in de les. Een eerste versie is opgeleverd en zal de komende periode worden doorontwikkeld. Het is belangrijk om de taken en verantwoordelijkheden hiervoor beleggen. We gaan afspraken maken met Kennisnet of SURF over doorontwikkeling en technische ondersteuning. Daarbij wordt onderzocht of de brongegevens kunnen worden beheerd binnen de sectorbrede softwarecatalogus (zie hierboven). De inhoudelijke analyse van de tools en het up to date houden van de gegevens wordt uitgevoerd door externe inhuur en/of het Expertisecentrum Privacy.

- Uitgevoerd door: MBO Digitaal, Kennisnet en SURF

20. Afstemmen ambitieniveau en uniforme IBP-rapportage voor verantwoording

We kennen binnen de mbo-sector een ambitieniveau van 3,0 als gemiddelde volwassenheid voor de toetsingskaders informatiebeveiliging en privacy. Dat gemiddelde werd in 2021 door ruim de helft van de mbo-instellingen niet gehaald. Nu we voor informatiebeveiliging overstappen op een nieuw toetsingskader moeten we er rekening mee houden dat het gemiddelde van de eerstvolgende benchmark IB zelfs fors lager zal uitvallen. We gaan onderzoeken wat realistische doelen zijn voor de komende jaren. Daarbij doen we een voorstel op welke manier de scholen hierover -zowel individueel als sectorbreed- terugkoppelen richting OCW. Deze besluiten laten we vaststellen door de Algemene Ledenvergadering.

- Uitgevoerd door: MBO Digitaal en MBO Raad

21. Oprichten van een Expertisecentrum Informatiebeveiliging

In deze notitie wordt op diverse plekken een Expertisecentrum Informatiebeveiliging genoemd. Dit idee komt ook terug in de Innovatiezone Cyberveiligheid van SURF (als security-expertisecentrum SEC). Daarbij denken wij -in het kader van ons plan- aan een expertisecentrum dat concrete ondersteuning aan de instellingen kan bieden bij het nemen van de benodigde technische maatregelen die voortvloeien uit de benchmarks, audits en oefeningen. Bijvoorbeeld door het beschikbaar maken van IT-consultants en -specialisten. We onderzoeken of en op welke manier onderdelen van deze dienstverlening door SURF worden uitgevoerd.

- Uitgevoerd door: MBO Digitaal en SURF (Innovatiezone Cyberveiligheid)

22. Oprichten van een Expertisecentrum Privacy

Er is veel behoefte aan advies en dienstverlening op het gebied van privacy, bijvoorbeeld het centraal onderzoeken van verwerkersovereenkomsten, het ontwikkelen van een centrale

DPIA-aanpak, het coördineren van centraal uitgevoerde DPIA's enzovoort. Ook het onderhouden van een centraal informatiepunt met actuele ontwikkelingen en veelgestelde vragen over privacybescherming wordt belegd bij de Expertisecentrum Privacy.
Het Expertisecentrum Privacy speelt ook een adviserende rol bij diverse landelijke ontwikkelingen, zoals de activiteiten die worden opgestart binnen de Digitaliseringsimpuls Digitale leermaterialen of de gegevensuitwisseling in de leermiddelenketen. Ook de ethische kant van de digitalisering van het onderwijs krijgt hier aandacht, bijvoorbeeld door het opzetten van een ethische raad, samen met SURF.

- Uitgevoerd door: MBO Digitaal en SURF (Innovatiezone Cyberveiligheid)

Bijlage B: begroting op hoofdlijnen

Op basis van dit plan heeft OCW bedragen voor cyberveiligheid en privacy opgenomen in de Voorjaarsnota. Het gaat vooralsnog om de volgende bedragen (mln euro).

Onderwerp	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Totaal**	**Str**
Cybersecurity + Privacy	**3,3**	**4,1**	**4,1**	**4,1**	**4,1**	**4,1**	**23,8**	**1,2**
Cybersecurity	**1,6**	**2**	**2**	**2**	**2**	**2**	**11,6**	**0,6**
a. Aansluiting van alle mbo-instellingen op SOC	*0,8*	*1*	*1*	*1*	*1*	*1*	*5,8*	
b. Inhuur experts voor ondersteuning instellingen	*0,5*	*0,6*	*0,6*	*0,6*	*0,6*	*0,6*	*3,5*	*0,6*
c. Uitbreiding cybersecurity-crisisoefeningen	*0,3*	*0,4*	*0,4*	*0,4*	*0,4*	*0,4*	*2,3*	
Privacy	**1,7**	**2,1**	**2,1**	**2,1**	**2,1**	**2,1**	**12,2**	**0,6**
d. Gezamenlijk uitvoeren van DPIA's, audits en onderhandelingen met softwareleveranciers en uitgevers door SURF in opdracht van het mbo.*	*1*	*1*	*1*	*1*	*1*	*1*	*6*	*0,4*
e. Opstellen en coördinatie van het sectorbrede plan van Aanpak privacybescherming mbo	*0,1*	*0,1*	*0,1*	*0,1*	*0,1*	*0,1*	*0,6*	
f. Ondersteuning aan alle mbo-instellingen voor de uitvoering van het plan van aanpak	*0,4*	*0,8*	*0,8*	*0,8*	*0,8*	*0,8*	*4,4*	
g. Beschermen van privacy bij de uitwisseling van persoonsgegevens in de nationale leermiddelen ICT-infrastructuur van scholen-distribiteurs-uitgevers van leermiddelen.**	*0,2*	*0,2*	*0,2*	*0,2*	*0,2*	*0,2*	*1,2*	*0,2*

*SURF voert DPIA's uit in opdracht van de MBO Raad. De MBO Raad bepaalt namens de mbo-instellingen de prioritering van deze jaarlijkse DPIA-capaciteit bij SURF.

**Kennisnet voert deze activiteiten uit in opdracht van de MBO Raad. De MBO Raad kan op termijn besluiten de activiteiten bij een andere partij te beleggen indien daar aanleiding toe is.

In bijlage A: (project)activiteiten zijn de activiteiten benoemd die we de gaan uitwerken en uitvoeren binnen het programma Cyberveiligheid mbo. Deze activiteiten hebben wij ondergebracht in vier deelprojecten. Deze vier deelprojecten vormen de hoofdindeling van de begroting/subsidieaanvraag.

1. Coördinatie Cyberveiligheid mbo
2. Aansluiting van alle mbo-instellingen op een SOC
3. Expertisecentrum Informatiebeveiliging
4. Expertisecentrum Privacy

De vier deelprojecten worden hieronder verder toegelicht en de begroting wordt op hoofdlijnen uitgewerkt.

1. Coördinatie Cyberveiligheid mbo

Coördinatie van de activiteiten en organisatie van overkoepelende activiteiten.
Activiteiten o.a.:

- Coördinatie van alle activiteiten.
- Communicatie over/binnen het programma, strategisch en ondersteunend
- Organiseren conferenties en bijeenkomsten.
- Onderhouden diverse websites en media.
- Onderzoek/uitwerking sectorbeeld en inventarisatie van de ondersteuningsbehoefte vanuit de instellingen.
- Onderzoek/voorbereiden mbo-breed cybercrisisconvenant en calamiteitenfonds.
- Voorbereiden/laten accorderen van bestuurlijke afspraken over bijvoorbeeld verantwoording groei en streefvolwassenheidsniveaus.
- Overleg met SURF over lidmaatschap mbo-instellingen

Totaal 2,65 mln

2. Aansluiting van alle mbo-instellingen op een SOC

We gaan uit van gemiddeld 10 mbo-instellingen per jaar, om te kunnen versnellen is flexibiliteit in jaarbudget noodzakelijk.
Activiteiten, o.a.:

- Onderzoek SURFsoc i.r.t. aanbod SIEM/SOC oplossingen die deels al in gebruik zijn binnen de mbo-instellingen (via Microsoft)
- Onderzoek naar scenario's voor een 24/7-escalatiedienst.
- Vergoeding entreekosten SURFsoc per instelling.
- Kwartiermaker SURFsoc, ter ondersteuning van de mbo-instelling.
- Consultant voor IT-begeleiding, voor technische ondersteuning van de mbo-instelling.

Totaal 4,21 mln

3. Expertisecentrum Informatiebeveiliging mbo

Binnen het Expertisecentrum Informatiebeveiliging mbo worden de activiteiten belegd op het gebied van informatiebeveiliging en informatiemanagement. De uitvoering ligt voor het grootste deel bij SURF, bijvoorbeeld binnen het security-expertisecentrum (onderdeel van de Innovatiezone Cyberveiligheid).

Activiteiten, o.a.:

- Organiseren mbo-brede nulmeting op het gebied van cyberweerbaarheid.
- Selectie en implementatie van een mbo-brede softwareoplossing voor risicomanagement, planning/bewaking van maatregelen en documenteren volwassenheid, inclusief benchmarkfunctie.
- Opstellen PvE, selectie en implementatie van een mbo-brede softwarecatalogus, mogelijk samen met PO/VO en HO.
- Ontwikkelen en onderhouden Framework IBP met modeldocumenten en good-practices op het gebied van informatiebeveiliging en privacy, aansluitend op de toetsingskaders.
- Onderhouden informatieplatform (website/teamsite) over cyberveiligheid.

- Ontwikkelen en uitvoeren IBP-scholings- en awarenessactiviteiten
- Integratie IBP met architectuur: bijdragen aan de (door)ontwikkeling van MORA/MOSA vanuit IBP-perspectief.
- Ondersteunen bij het ontwerpen/bouwen van veilige gegevensuitwisseling in de leermiddelenketen, bijvoorbeeld de Open Onderwijs API.
- Organiseren van cybercrisisoefeningen en red-teaming oefeningen.
- ISO as a service: beschikbaar maken van informatiebeveiligingsspecialisten voor concrete ondersteuning van de mbo-instellingen op het gebied van cyberveiligheid.
- MORA as a service: idem voor IT-architecten
- Audit as a service: beschikbaar maken van auditors voor audits van mbo-instellingen en advies over risico's en maatregelen, op instellingsniveau en mbo-breed.
- Coördinatie van de communicatie bij sectorbrede security-incidenten, samen met/aanvullend op SURFcert.

Totaal: 8,12 mln

4. Expertisecentrum Privacy mbo

Binnen het Expertisecentrum Privacy mbo worden de activiteiten belegd met betrekking tot de bescherming van de privacy in het mbo. Evenals bij het Expertisecentrum Informatiebeveiliging wordt de uitvoering voor het belangrijkste deel aan SURF uitbesteed.

Activiteiten van het Expertisecentrum Privacy mbo:

- Ontwikkelen/implementatie nieuw toetsingskader privacy, samen met het HO (SURF)
- Opzetten en bemensen van de mbo Expertisecentrum Privacy: een vraagbaak/helpdesk op het gebied van privacy-vragen vanuit de instellingen.
- Onderhouden informatieplatform (website/teamsite) over privacybescherming.
- Ontwikkelen en implementeren van een generieke DPIA-aanpak voor het mbo.
- Organiseren/coördineren van de uitvoering van DPIA's, uitgevoerd door SURF.
- Beoordelen/onderhandelen/afstemmen verwerkersovereenkomsten voor de belangrijkste mbo-leveranciers.
- Organiseren/coördineren van leverancier-audits (gebruikmakend van de auditcapaciteit van het Expertisecentrum Informatiebeveiliging).
- Organiseren/coördineren van pentests bij leveranciers.
- Onderzoek naar privacyaspecten van veelgebruikte online onderwijsapps en het beschikbaar maken van de bevindingen voor de onderwijssector.
- (Door)ontwikkelen van het 'Toolwiel' als presentatielaag van bovengenoemde privacyaspecten van onderwijsapps.
- Coördinatie van de communicatie bij sectorbrede privacy-incidenten, samen met/aanvullend op SURFcert.
- Meewerken aan het PvE bij het ontwerpen/bouwen van veilige gegevensuitwisseling in de leermiddelenketen (privacy by design), bijvoorbeeld bij de Open Onderwijs API.
- Betrokkenheid bij Digitaliseringsimpuls Digitale leermaterialen.
- Adviseren over privacyaspecten bij diverse landelijke initiatieven (bijvoorbeeld koppelingen, data-ondersteund onderwijs)
- Opzetten en faciliteren van een ethische raad, samen met SURF.

Totaal: 8,80 mln

Bijlage C: Adviezen AP en OCW

Hieronder de 4 adviezen van de Autoriteit Persoonsgegevens aan de minister van OCW. Daarop zijn door OCW 10 adviezen geformuleerd die wij hebben voorzien van een toelichting op welke manier deze een plek hebben gekregen in ons plan van aanpak.

AP Advies 1

Het structureel door de minister coördineren van de aanpak van gegevensbescherming binnen het onderwijs door het instellen, dan wel ondersteunen van organisaties en samenwerkingsverbanden die daarin voorzien.

Advies OCW

1. Organiseer governance en financiering voor het gezamenlijk uitvoeren van DPIA's waarbij zoveel mogelijk wordt opgetrokken met andere onderwijssectoren om te komen tot de groots mogelijke krachtenbundeling richting leveranciers.

➢ Het centraal uitvoeren van DPIA's is opgenomen in dit plan

2. Het gezamenlijk uitvoeren van DPIA's vereist ook een gezamenlijk leveranciersmanagement, waaronder ook gezamenlijk inkopen door instellingen.

➢ Gezamenlijk leveranciersmanagement is onderdeel van dit plan, een belangrijk aspect daarvan is de sectorbrede softwarecatalogus, de gecoördineerde beoordeling verwerkersovereenkomsten, uitvoeren audits, etc. Gezamenlijk inkopen is voor een belangrijk deel al georganiseerd via de SURF coöperatie.

3. Maak zichtbaar in het PvA hoe het mbo op alle vijf de ict-domeinen privacybescherming bevordert voor onderwijspersoneel en studenten. De vijf domeinen:
   - Digitale Leermiddelen en toetsen
   - De leermiddelenketen (voor het ontsluiten en gebruiken van leermiddelen en toetsen)
   - ICT ter ondersteuning van de les, bv plagiaatsoftware, proctoring of videobellen en de elektronische leeromgeving.
   - ICT voor de bedrijfsvoering van een instelling, bijvoorbeeld administratiesystemen
   - ICT voor verantwoording en beleidsinformatie intern en extern de instelling

➢ Deze indeling is ook benoemd als scope in dit plan, dus afhankelijk van de risico's/prioritering komen alle domeinen terug in het programma.

AP Advies 2a

Onderwijsinstellingen actief te informeren over de verantwoordelijkheden die zij hebben bij het bepalen van de risico's voor kinderen indien digitale middelen worden ingezet.

Advies OCW

4. Voor iedere achterblijvende instelling is een maatwerk PvA noodzakelijk voor de eigen instelling.
5. Er is een onafhankelijke dwarskijker nodig op het door de sector zelf bepaalde ambitieniveau en het tijdspad bij die ambitie.

- De mbo-instellingen zijn zich bewust van hun verantwoordelijkheden. In het toetsingskader informatiebeveiliging zijn risico's en maatregelen benoemd die te maken hebben met de bescherming van (persoons)gegevens. In het toetsingskader privacy worden expliciet de instrumenten voorgeschreven om de privacyrisico's in kaart te brengen en te mitigeren, bijvoorbeeld door het uitvoeren van DPIA's. Alle mbo-instellingen gebruiken deze toetsingskaders voor het invullen van de jaarlijkse benchmark IBP-E.
- Alle mbo-instellingen werken met een 'maatwerk PvA': een eigen roadmap op basis van de toetsingskaders informatiebeveiliging en privacy. Vanuit ons sectorplan onderzoeken we de mogelijkheid voor softwarematige ondersteuning voor het bijhouden van risico's, streef- en actueel volwassenheidsniveau, documentatie van genomen maatregelen enzovoort. Deze tool geeft de mbo-instelling voortdurend inzicht in de ontwikkeling van de volwassenheid en vereenvoudigt de samenwerking met interne en externe auditors.
- Het ambitieniveau en een realistisch tijdpad daarvoor worden mbo-breed in nauw overleg met alle betrokkenen uitgewerkt en het is zeker mogelijk om daar een onafhankelijke dwarskijker bij te betrekken. Het is overigens in niemands belang om de lat hiervoor te laag of te hoog te leggen. Daarbij gaan externe auditors een rol spelen bij de uitvoering of de beoordeling van de assessments en die vervullen die rol van onafhankelijke dwarskijker per definitie.

AP Advies 2b

Onderwijsinstellingen actief te stimuleren om privacy risicoanalyses uit te voeren of uit te laten voeren.

<u>Advies OCW</u>

6. Borg dat data-gedreven-onderwijs vernieuwingen binnen instellingen, en tussen instellingen, ook daadwerkelijk onder begeleiding van een FG worden uitgevoerd. En dat software wordt ingekocht die voldoet aan privacy-by-design.
7. Organiseer een structurele sectorbrede Ethische Raad waar door bestuurders, docenten, studenten en experts ethische casuïstiek wordt besproken. Zorg ook voor financiering van deze Raad.

- Een belangrijk instrument om privacy risicoanalyses uit te voeren is de DPIA. Met behulp van de toetsingskaders IB en P wordt het uitvoeren van DPIA's beoordeeld. In ons plan van aanpak is het ontwikkelen van een standaardaanpak voor de uitvoering van DPIA's opgenomen. Daarnaast worden in dit plan de DPIA's voor de meest gebruikte softwarepakketten centraal uitgevoerd (zoals dat al is gebeurd voor producten van Microsoft, Google en Zoom).
- Belangrijke AVG-principes als 'privacy by design' zijn onderdeel van het toetsingskader privacy: door op dit onderdeel te monitoren (en eventueel te auditen) kan worden beoordeeld in hoeverre deze principes zijn geborgd.
- Voor data-gedreven onderwijs geldt binnen de onderwijsinstelling de normale intake-procedure waarbij de privacy wordt bewaakt via een standaard proces van beoordelen/goedkeuren van verwerkersovereenkomsten, mogelijk aangevuld met een DPIA. Neemt niet weg dat het onderwerp extra aandacht behoeft op sectorniveau. Het Expertisecentrum Privacy kan landelijke ontwikkelingen op het gebied van data-ondersteund onderwijs monitoren en adviseren.

- Het faciliteren van een Ethische Raad is onderdeel van ons programma en benoemd als activiteit van het Expertisecentrum Privacy. Het is de bedoeling om hierin samen op te trekken met SURF, omdat hierover ook al veel in gang is gezet, onder andere binnen de zone Studiedata van het Versnellingsplan.

AP Advies 3

Verkennen welke digitale middelen veel gebruikt worden door onderwijsinstellingen en het daarop laten uitvoeren van – actueel te houden – DPIA's die kunnen worden gebruikt door onderwijsinstellingen bij hun risicoanalyse.

Advies OCW

8. Zorg voor voldoende budget per jaar voor het gezamenlijk centraal uitvoeren van DPIA's door SURF Procurement & Contracting waarbij MBO-Digitaal, namens de mbo-sector, de SURF capaciteit mag prioriteren binnen dat budget.
9. Aandacht voor ondersteuning bij de specifieke afweging die elke instelling moet maken n.a.v. de centraal uitgevoerde DPIA.

- In ons plan van aanpak is de ontwikkeling van een sectorbrede softwarecatalogus beschreven, waarbij de mbo-instellingen worden gestimuleerd om hierin documenteren welke softwaretoepassingen en leveranciers worden ingezet voor welke processen. Dit geeft inzicht in de meest gebruikte digitale middelen en dient onder andere als basis voor het centraal (laten) uitvoeren van DPIA's.
- De coördinatie van de centrale uitvoering van deze DPIA's voor het mbo gebeurt door het Expertisecentrum Privacy. De uitvoering wordt zo mogelijk belegd bij SURF, waar mogelijk wordt gemeenschappelijk opgetrokken met het hoger onderwijs.
- Bij het opvolgen van de uitkomsten van deze DPIA's worden de instellingen ondersteund door SURF, aangevuld met diensten vanuit het Expertisecentrum Security en -Privacy.

AP Advies 4

In Europees verband aandacht vragen en zonodig gecoördineerde acties te ondernemen met andere lidstaten richting grote leveranciers van digitale middelen om de juiste waarborgen te treffen voor de bescherming van persoonsgegevens van onderwijsdeelnemers.

Advies OCW

10. Werk samen met de OCW-directie internationaal Beleid aan de probleemanalyse die behoort bij de door MOCW bepleitte oplossing Open Source EU Alternatieven.

- Er zijn in de afgelopen twee jaar centraal DPIA's uitgevoerd op producten van Microsoft, Google en Zoom. De hierbij gevonden privacy-risico's zijn voor een deel door de leverancier zelf opgelost en er zijn risico's geïdentificeerd die de onderwijsinstelling zelf kan mitigeren door aanpassingen in het gebruik van de toepassing of door wijzigen van systeeminstellingen binnen de applicatie. Hierbij zijn de scholen ondersteund door SIVON en/of SURF.

- De mbo-instellingen hebben op dit moment niet het gevoel dat ze benadeeld worden door een vendor lock-in. Hoewel het belangrijk is om de grote tech-leveranciers scherp in de gaten te houden is er wat de mbo-sector betreft op dit punt geen urgentie om in Europees verband te zoeken naar open-source alternatieven. Wij denken dat wij onze positie kunnen versterken door deze leveranciers structureel te blijven monitoren en te auditen en ze vervolgens te houden aan afspraken.
- Vanuit dit programma werken we desgewenst samen met de OCW-directie Internationaal Beleid aan de probleemanalyse.