saMBO-ICT

SURF

Kennisnet

Hoe? Zo!

Informatiebeveiligingsbeleid in het mbo

Inhoudsopgave

1	Inleiding	3
2	Waarom informatiebeveiliging?	4
3	Om welke risico's gaat het en hoe ga ik daarmee om?	8
4	Hoe kom ik 'in control'?	11
5	Hoe kan ik het informatiebeveiligingsbeleid oppakken?	19
6	Hoe wordt informatiebeveiligingsbeleid toegepast in de praktijk?	23
7	Wat kunnen we sectorbreed doen?	32
	Samenvatting	36
	Bronnen	37

1. Inleiding

Aanleiding

Het is niet bekend hoe goed of slecht het beleid rond informatiebeveiliging momenteel in het mbo geregeld is. Gezien de mogelijke risico's die instellingen lopen en die in de toekomst door aangescherpte wet- en regelgeving nog groter zullen worden is het van groot belang dat de sector zijn verantwoordelijkheid in deze neemt. Deze publicatie steekt in op de risico's. Zonder overdrijving of bangmakerij wordt een aantal risico's op een rij gezet en wordt de conclusie getrokken dat een gedegen en gestructureerde aanpak van de informatiebeveiliging in het mbo van belang is. Tegelijk zitten bestuurders en managers met veel vragen over hoe je dat dan aanpakt. Reden om informatie en de achterliggende vragen rondom informatiebeveiliging maar eens op een rij te zetten.

Voor wie?

Deze uitgave van Hoe? Zo! is met name gericht op bestuurders en onderwijsmanagers in het onderwijs. In eerste instantie is het toegespitst op het mbo, maar de hoofdlijnen zijn zeker ook toepasbaar buiten het mbo.

Hoe? Zo!

Kennisnet en saMBO-ICT hebben een aantal publicaties uitgegeven in de zogeheten Hoe? Zo!-reeks. Deze reeks geeft overzicht en inzicht over wat er speelt aangaande actuele ict-onderwerpen in het onderwijs (zoals Leermiddelenbeleid, Bring Your Own Device of ICT en recht). U kunt de reeks gebruiken om uw visie te vormen, ter ondersteuning van een implementatietraject of om als instelling een richting te bepalen met betrekking tot ict-gebruik. Iedere publicatie in de Hoe? Zo!-reeks is opgebouwd uit vragen. Aan de hand daarvan worden antwoorden gegeven, keuzemogelijkheden geschetst en tips gegeven. Deze publicatie beschrijft soms hoe het moet, soms hoe het kan. Er is meestal niet één pasklaar antwoord: instellingen hebben keuzevrijheid en moeten hier zo veel mogelijk gebruik van maken.

Leeswijzer

Na het lezen van deze Hoe? Zo!-publicatie is duidelijk wat er komt kijken bij informatiebeveiligingsbeleid, waarom het belangrijk is, en hoe u er als bestuurder of onderwijsmanager mee aan de slag kunt.

De hoofdstukken 2 en 3 leggen daarvoor de basis. Daarin wordt de vraag naar het waarom besproken alsmede de risico's die aanleiding geven tot een brede aanpak. Het belangrijkste onderdeel volgt in hoofdstuk 4; hoe krijg ik als bestuurder nu grip op deze materie? In hoofdstuk 5 wordt ingegaan op de mogelijke aanpak van informatiebeveiligingsbeleid. Hoofdstuk 6 gaat de diepte in, de complexiteit wordt duidelijk en er wordt aangegeven wat er in de praktijk allemaal nodig is. Tot slot schetst hoofdstuk 7 dat instellingen het zeker niet allemaal zelf moeten uitvinden maar dat er veel mogelijkheden zijn voor samenwerking om zo tot een effectieve en efficiënte aanpak te komen van informatiebeveiliging in het mbo-onderwijs.

Hoe?

2. Waarom informatiebeveiliging?

Welke risico's lopen we?

Wat betekent de veranderende wetgeving voor het onderwijs?

Hoe goed hebben we de risico's in beeld?

Zo!

Informatiebeveiliging staat intussen bij elke instelling wel ergens op de agenda. Incidenten in het onderwijsveld hebben ervoor gezorgd dat op veel plekken de wenkbrauwen gefronst werden en dat steeds meer mensen zich gingen afvragen wie wat waar aan moest doen. Dat is zeker het geval bij veel ict-afdelingen. Maar informatiebeveiliging is niet alleen de verantwoordelijkheid van de afdeling ict, het is een verantwoordelijkheid van de gehele mbo-instelling met als kartrekker het College van Bestuur. Het gaat in eerste instantie niet om ict maar om gedrag, cultuur en bewustwording, met als basis een vastgesteld en breed gedragen beleid, duidelijke procedures en heldere protocollen. Als dit beleid, deze procedures en protocollen instellingsbreed geïmplementeerd zijn, dan pas is ict aan zet bij de uitvoer en monitoring. Informatiebeveiligingsbeleid is geen techniek feestje, het is een constant bewustzijn van de risico's die een school loopt, risico's waardoor haar continuïteit in zowel het onderwijs als de bedrijfsvoering in gevaar kan komen.

Welke risico's lopen we?

De afgelopen jaren hebben diverse examenfraudes in Nederland de pers gehaald. Iedereen kent de voorbeelden van scholen die in het nieuws gekomen zijn omdat examens op het internet beland zijn voordat dit de bedoeling was. Hierdoor heeft het onderwijs flinke imago-schade opgelopen en hebben studenten, docenten en medewerkers er veel last van ondervonden. En in hoeveel gevallen hebben we er geen weet van en is de fraude geslaagd (net als de studenten wellicht)? Voor onderwijsinstellingen die als kernwaarde het uitgeven van diploma's, als gevalideerde waardepapieren hebben, is dit toch een precaire zaak.

Daarnaast zijn er ontwikkelingen op het gebied van de wetgeving waar onderwijsinstellingen mee te maken hebben en waar zij in de toekomst zeker nog meer mee te maken krijgen. De risico's op vervolging, claims en/of boetes bij overtreding van bijvoorbeeld de privacy wetgeving dreigen ernstig toe te nemen en verdienen gepaste aandacht.

En wat te denken van het risico van discontinuïteiten in de bedrijfsvoering en het onderwijs zelf als de ict-functie stagneert of zelfs uitvalt, als onze informatieomgevingen worden gehackt of gesaboteerd? Het aantal DDOS aanvallen waarbij computercriminelen het netwerk van een school platleggen is in het mbo flink gestegen. Onderzoek van SURFnet toont aan dat iedere (bij SURF aangesloten) onderwijsinstelling in Nederland het afgelopen jaar te maken heeft gehad met een aanval. Met een sterk toegenomen afhankelijkheid van die ict-functie in alle processen is het van belang dat dit risico dan ook zoveel mogelijk wordt ingeperkt.

Kortom, diverse risico's van verschillende aard die het onderwijs ertoe dwingen om naast technische ook beleidsmatig gepaste maatregelen te treffen.

Wat betekent de veranderende wetgeving voor het onderwijs?

Een goed informatiebeveiligingsbeleid en bijpassende procedures en beheersmaatregelen zijn van groot belang. En dat geldt niet alleen voor een onderwijsinstelling. De gezondheidzorg in Nederland is, bijvoorbeeld, ook volop in beweging als het gaat om de bescherming van patiëntengegevens. Deze sector heeft zelf het heft in eigen hand genomen (scholing, elkaar controleren, collegiale ondersteuning, etc.). Dit wordt door het onderwijs dan ook gezien als een voorbeeld van een aanpak die in de toekomst ook voor de gehele onderwijssector kan worden gehanteerd.

Kijken we naar het bedrijfsleven dan zien we dat daar bescherming van privacy tot enkele jaren terug gezien werd als bijzaak, één van de vele administratieve lasten die op bedrijven drukt. Omgang met persoonsgegevens deed men op basis van 'gezond verstand', niet zozeer omdat de wet dit opdroeg. Het ontbreken van concreet toepasbare regels en zware sancties maakte dat aan schendingen van privacy niet zwaar werd getild. Alleen op grove overtredingen, die van invloed waren op grotere groepen betrokkenen, werd

Zo!

sanctionering toegepast. Na de komst van de code-Tabaksblat, de corporate governance-code en de code goed openbaar bestuur[1], is nakoming van bescherming van gegevens en privacywetgeving, een steeds belangrijker onderdeel geworden van de bedrijfsvoering.

In januari 2012 is door de Europese Commissie een voorstel gelanceerd voor een Europese Privacy Verordening (EPV). Deze verordening vervangt nationale wetgeving in alle landen van de Europese Unie. Op 12 maart 2014 heeft het Europees Parlement de EPV, officieel de 'Algemene Verordening Gegevensbescherming' (AVG) genoemd, aangenomen. Bij overtreding van de wet kan dit grote gevolgen hebben voor de organisatie. Niet alleen is er kans op imagoschade maar ook kan de organisatie aansprakelijk worden gesteld voor de geleden schade, met een maximale boete van € 100.000.000 (of 5% van de jaaromzet).

De EPV gaat uit van 'privacy by default'. Bij de aanschaf of het laten ontwikkelen van software, de inrichting van databases en inrichting van een ict-systeem staat privacy centraal. Privacy is geen sluitpost (meer). Iedere organisatie moet zorgen dat de gebruikte en verzamelde persoonsgegevens en de bewaartermijn daarvan zijn afgestemd op het doel waarvoor zij worden verzameld.

De verwachting is dat door de EPV, op termijn, gegevens van iedere Europese burger beter zullen worden beschermd. Onderwijsinstellingen zullen verplicht worden datalekken binnen 72 uur te melden. Tevens rust een uitgebreide documentatieplicht op hen en een zwaardere verplichting tot heldere uitleg over het gebruik van persoonsgegevens, alsmede het recht op wissen van gegevens (het recht op vergeten). Organisaties die persoonsgegevens verwerken van meer dan 5.000 betrokkenen, worden daarbij ook verplicht om een privacy officer aan te stellen.

Daarbij moeten de beveiligingsmaatregelen voldoen aan de recente stand van de techniek. Sinds 2013 geeft de Code voor Informatiebeveiliging[2] een goede indicatie welke beveiligingsmaatregelen van een instelling mogen worden verwacht.[3]

SURF heeft in april 2014 een brief gestuurd aan alle Colleges van Bestuur (universiteiten en HBO-instellingen) om aan te geven wat de gevolgen van deze maatregel zijn voor de informatievoorziening. Kort samengevat komt het er op neer dat, indien persoonlijke gegevens van medewerkers of studenten ten onrechte gebruikt worden, dit kan leiden tot een forse boete. In het hoger onderwijs zijn vorig jaar door het CBP (College Bescherming Persoonsgegevens) twee onderwijsinstellingen gecontroleerd op de naleving van de privacywetgeving. Het is aannemelijk dat dit in de toekomst ook bij mbo-instellingen gaat plaatsvinden.

Hoe goed hebben we de risico's in beeld?

Het is wel duidelijk dat het onderwerp informatiebeveiliging steeds belangrijker is geworden. Veel instellingen zijn op de een of andere manier bezig met het onderwerp. Maar de vraag of mbo-instellingen hun beveiliging "op orde" hebben kan niemand beantwoorden.
De behoefte om te kunnen aantonen dat de mbo-sector de informatiebeveiliging goed op orde heeft, wordt door zowel de overheid als saMBO-ICT, middels een taskforce, als de instellingen zelf gevoeld.
In de eerste plaats moeten er dan afspraken komen over wat het betekent om "de zaak op orde" te hebben.

De eerste taak is om de risico's te benoemen, zoals examenfraude, door derden inbreken op het netwerk, onjuiste financiële transacties, lekken van persoonlijke gegevens, continuïteit van de ict-functie, etc. Vervolgens is de vraag hoe de instelling omgaat met deze risico's.
En om te weten of je iets goed doet of niet moet er sprake zijn van een norm of een normenkader waaraan je het gevoerde informatiebeveiligingsbeleid kunt toetsen. Er zal dus een normenkader met elkaar moeten worden afgesproken aan de hand waarvan mbo-instellingen de

Zo!

risico's inzichtelijk maken en de resultaten van het beleid kunnen kwantificeren. Dit normenkader is een gezamenlijke afspraak voor het gehele mbo, die ook met de overheid is afgestemd. Zij kunnen immers ook wensen of eisen op dit gebied hebben. Het is van belang dat de onderwijsinstellingen die norm dan ook gaan hanteren en gaan meten wat de stand van zaken is op het gebied van informatiebeveiliging. Alleen zo krijg je inzicht in de situatie van de specifieke instelling en die van de sector als geheel en kun je je als instelling gaan vergelijken met andere instellingen. Zo komt er een benchmark op het gebied van informatiebeveiliging.

Instellingen kunnen zelf bepalen en/of door derden laten controleren waar de norm wordt behaald en welke onderdelen nog voor verbetering in aanmerking komen. Assessments en audits zijn daar de aangewezen middelen voor, naast het delen van best practices. Kennisontwikkeling binnen de mbo-instelling is een voorwaarde om informatiebeveiligingsbeleid goed op de kaart te zetten en adequaat en daadkrachtig aan te pakken. Naast het bepalen van een norm en het meten daarvan, zullen mbo-scholen zich ook tactisch en operationeel moeten bezig houden met informatiebeveiliging. Het registreren en delen van incidenten bijvoorbeeld moet ingebed zijn in het beleid van de organisatie. De aanpak bestaat daarbij niet alleen uit technologische maatregelen of het afspreken van processen en protocollen, het menselijke aspect is zeker zo belangrijk. Cultuur en gedrag zijn een voorwaarde voor een succesvolle uitvoer. Bewustwording is essentieel op alle niveaus, van het college van bestuur tot de examenmedewerker. En het is van belang dat het bewustzijn altijd aanwezig is, waarbij de mbo-scholen informatiebeveiliging als consequente en constante factor in alle processen aandacht geven.

Door het beter structureren van het informatiebeveiligingsbeleid bij een mbo-instelling wordt aantoonbaar dat dit beleid bijdraagt aan de realisering van de overall doelstellingen die de onderwijsinstelling voor zichzelf heeft geformuleerd ('alignment'). De uiteindelijke doelstelling is altijd het bieden van een kwalitatief hoogwaardige onderwijsomgeving, die bijdraagt aan de verbetering van de kwaliteit van de samenleving als geheel. Deze omgeving behoort veilig te zijn en te voldoen aan alle relevante wet- en regelgeving.

Een voorbeeld van een succesvol geïmplementeerd onderdeel van het informatiebeveiligingsbeleid is het digitaal examinerings-proces, dat gebaseerd is op:

- een vastgesteld beleid,
- geschoolde en betrokken medewerkers op alle niveaus en in alle geledingen,
- een goed werkende ict-omgeving waarbij ook de continuïteit gewaarborgd is,
- een sluitende toegangsbeveiliging (alleen geautoriseerde medewerkers en studenten hebben toegang tot de examens) en tot slot,
- een voortdurende controle en logging om ervoor te zorgen dat het proces volgens afspraak wordt uitgevoerd waardoor een mbo-instellingen met recht kan stellen dat zij op het gebied van examineren in control is.

Hoe?

3. Om welke risico's gaat het en hoe ga ik daarmee om?

Hoe ga ik om met de risico's?

Om welke risico's gaat het?

Van welke risico's moet ik mij als bestuurder bewust zijn?

Hoe krijg ik zicht op de concrete risico's binnen mijn instelling?

Zo!

"Het Regio College biedt een veilige Digitale Leer en Werkomgeving (DLWo) voor deelnemers en medewerkers. Informatiebeveiliging is een noodzakelijke voorwaarde om op ieder gewenst moment over betrouwbare gegevens te kunnen beschikken en de continuïteit van de bedrijfsprocessen te waarborgen."

Wim van Amersfoort, voorzitter van het College van Bestuur van het Regio College

Van welke risico's moet ik mij als bestuurder bewust zijn?

Informatiebeveiliging is een aangelegenheid van het College van Bestuur en niet van de afdeling ict of van de mensen van het functioneel beheer. Dit heeft alles te maken met de ontwikkeling van ict. Een korte terugblik:

- In fase I (tot ongeveer 2005) stond de hardware centraal en was de ict-afdeling leidend;
- In fase 2 (tot ongeveer 2012) stond de software (de applicaties) centraal en waren de ict-afdeling en functioneel beheer leidend;
- In fase 3 (heden) staan de data centraal en zijn de proces- en systeemeigenaren leidend. Data zijn bijvoorbeeld gegevens van deelnemers, examens, jaarstukken etc.

Als data niet goed beschermd worden dan brengt dat risico's met zich mee. En dit kan leiden tot diverse vormen van schade of beschadiging van de organisatie:

1. **Reputatieschade:** door incidenten die gemeld worden in de media. Bijvoorbeeld examenfraude, wachtwoorden op straat, examens gestolen. Dit is slecht voor het imago van een school. Een mbo-instelling geeft belangrijke waardepapieren, namelijk diploma's, uit en die uitgifte moet goed beschermd worden.
2. **Financiële schade:** doordat data niet juist zijn kunnen deelnemers niet voor bekostiging in aanmerking komen; ook claims of boetes hebben financiële consequenties.
3. **Continuïteit mbo-instelling of opleiding:** nadat de examenfraude bij een school geëvalueerd was door het ministerie van OC&W heeft dit uiteindelijk geleid tot het sluiten van de onderwijsinstelling. Ook bij mbo-instellingen geldt dat het verlies van accreditaties mogelijk is doordat niet aan de eisen van toezichthouders wordt voldaan.
4. **Wet en regelgeving:** er moet voldaan worden aan bepaalde wet- en regelgeving. Privacywetgeving is een sprekend voorbeeld, op basis van nieuwe Europese wetgeving, strakkere normen, hogere boetes en serieuze aanpak betekent dit dat een mbo-instelling deze wetgeving onderdeel van hun informatiebeveiligingsproces moet maken.
5. **Risico's in de cloud:** meer en meer komen data en toepassingen in de cloud terecht. Dit levert specifieke aandachtspunten op zoals eigenaarschap, toegang en privacy, continuïteit van de dienstverlening van externe partijen, etc.[4]
6. **Te beperkt kennisniveau in de instelling, binnen het mbo:** ontwikkelingen gaan snel, het onderwerp wordt steeds belangrijker, de gevolgen groter. Het kennisniveau moet vandaag en in de toekomst continue op peil worden gehouden d.m.v. scholing, congressen, werkgroepen, etc. Het risico van onvoldoende kennis is dat er onjuiste beslissingen worden genomen, met alle gevolgen van dien, ten aanzien van informatiebeveiliging.

Hoe krijg ik zicht op de concrete risico's binnen mijn instelling?

Hieronder wordt één van de meest gebruikte methodieken omschreven. De bekendste is de methodiek van Risk assessment:

Risico is de kans dat een gebeurtenis plaatsvindt, "vermenigvuldigd" met het gevolg van die gebeurtenis. Als het gevolg kwantificeerbaar is kan dit daadwerkelijk een vermenigvuldiging zijn. Het gevolg kan positief dan wel negatief zijn. Meestal wordt het woord echter in de negatieve zin gebruikt.

Voorbeeld 1: Het risico van brand in huis door blikseminslag met als gevolg totale verwoesting.

Met de methodiek van de Risk Assessment gaat het om het benoemen van de risico's, met oorzaak en gevolg en vervolgens het beoordelen van de risico's aan de hand van kans en impact.

Kans = 1 (laag) Impact = totale verwoesting = 3 (hoog)

Vervolgens worden de bovengenoemde risico's beoordeeld op basis van kans en impact in relatie tot een gekozen schaalverdeling (3-punts schaal).

Zo!

Voorbeeld 2: risico 1 uit de lijst op de volgende pagina (Privacy) het risico van onjuiste gegevens door onvoldoende bescherming van persoonsgegevens met als gevolg een onterechte weergave.

Kans is klein (1), maar de impact groot (3). In dit voorbeeld betekent dit een hoog risico (3 rood). Op deze manier kunnen dan alle risico's worden beoordeeld.[5,6]

Met welke concrete risico's kan een mbo-instelling worden geconfronteerd?

Onderdeel	Risico omschrijving	Oorzaak	Gevolg
1. Privacy	Het risico dat data onrechtmatig wordt opgeslagen en onvoldoende bescherming van persoonsgegevens.	Onvoldoende scheiding van rechten over groepen van personen.	Niet nakomen van de privacy wetgeving.
2. Kernregistratie-systeem	Het risico op fraude of onrechtmatige invoer in kernregistratiesysteem.	Onvoldoende controles en functiescheiding in het systeem.	Frauduleuze handelingen kunnen plaatsvinden, reputatieschade.
3. Cijferregistratie-systeem	Het risico op fraude bij invoer/mutatie van cijfers in cijferregistratiesysteem.	Onvoldoende ingebouwde controles (functiescheiding, 4-ogen principe).	Een onjuiste beoordeling van deelnemers, reputatieschade.
4. Beschikbaarheid netwerk	Het risico op uitval van IT-Infrastructuur.	Gebrek aan redundante (dubbele) uitvoer (stroom, servers, netwerk apparatuur etc.).	Geen beschikbaarheid.
5. Ongeoorloofd gebruik/toegang	Het risico op ongeoorloofd gebruik/toegang (bij-voorbeeld door hackers) tot de IT-infrastructuur.	Onvoldoende technische beveiligingen.	Niet beschikbaar zijn, onbetrouwbaarheid en diefstal van gegevens, reputatieschade.
6. Studentenvolg-systeem	Het studentenvolgsysteem is niet beschikbaar.	Het niet redundant uitvoeren van de database server (mogelijk in de cloud).	Studenten/medewerkers/docenten die niet bij hun gegevens kunnen.
7. Elektronische leeromgeving	Het risico op ongeautoriseerd gebruik van de elektronische leeromgeving.	Een gebrek aan procedures en/of het opvolgen daarvan.	Fraude, diefstal, reputatieschade etc.
8. Onvolledige dienstverlening door leveranciers	Het risico op onvolledige dienstverlening door leveranciers.	Een gebrek aan vastleggen van afspraken (SLA) of een te veel aan vertrouwen (geen monitoring).	Niet beschikbaar zijn voor de klant, reputatieschade.
9. Ongeautoriseer-de toegang	Het risico op ongeautoriseerde toegang.	Onvoldoende volwassenheid/bewustzijn over IT-beveiliging bij medewerkers door bv. deling van wachtwoorden.	Fraude, diefstal, reputatieschade.
10. Dataverlies	Het risico op dataverlies.	Een gebrek aan back ups (procedures) of calami-teitenplan.	Gebrek aan beschikbaarheid, reputatieschade.

Tabel 1. Risico's op het gebied van gegevens waar een mbo-instelling mee te maken kan krijgen.

Pas als de risico's zijn geanalyseerd kan de volgende stap genomen worden; het beheersbaar maken van de risico's.

Hoe?

4. Hoe kom ik ‘in control’?

Waar wil of moet ik aan voldoen?

Wat moet ik monitoren in het kader van beveiliging?

Wat is de rol van de audit?

Wie heeft welke verantwoordelijkheid?

Hoe hebben ze dat in het HO geregeld?

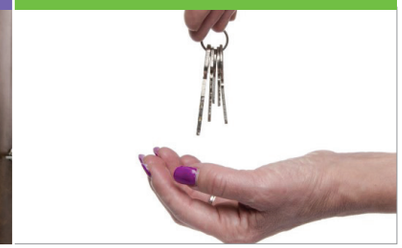
Hoe voldoe ik aan de kaders?

Zo!

Wat is de verhouding tussen de normen, kaders, toetsing, bewijzen en ondersteuning?

Doel van het informatiebeveiligingsbeleid is om de benoemde risico's beheersbaar te maken. Dit wordt gerealiseerd door het probleem, het minimaliseren van de risico's, beleidsmatig te benaderen.

Bij informatiebeveiliging, kunnen er op verschillende niveaus vragen worden gesteld over de inrichting van dit beleid. Het gaat hierbij om de volgende vragen en deelgebieden:

1 Waar wil of moet ik aan voldoen?	2 Hoe voldoe ik hieraan?	3 Voldoe ik aan de normen?	4 Wat verwacht ik van anderen?
Kaders en normen	**Normen en toetsingskaders**	**Toetsen en bewijzen**	**Ondersteuning**
Omschrijving ▪ Wet- en regelgeving ▪ Strategische agenda ▪ Informatie-beveiligingsbeleid *Normen* ▪ ROSA Katern Privacy en beveiliging (voor het onderwijs) ▪ ISO 27001/27002 (Code voor Informatiebeveiliging)	*Omschrijving* ▪ Te nemen maatregelen vanuit basisniveau voor beveiliging informatie en privacy ▪ Extra maatregelen op basis van classificatie *Toetsingskaders* ▪ Cloud Control Matrix (voor leveranciers) ▪ NORA katern Informatiebeveiliging (voor OCW/DUO) ▪ Baseline Informatiebeveiliging Rijksoverheid (voor DUO) ▪ SURF normenkader instellingen hoger onderwijs (voor instellingen) ▪ Mbo toetsingskader Taskforce IBB	*Omschrijving* ▪ Aanpak (wijze van vaststelling conformiteit, frequentie, etc) ▪ Uitvoeren self assessments en/of externe audits (peer auditing en externe audit) *Bewijzen* ▪ ISAE 3402 (door leveranciers) ▪ SURFaudit, MBOaudit (door instellingen) ▪ Kwalificatie OSO (door instellingen en leveranciers)	*Omschrijving* ▪ Aanwijzingen voor gebruik ▪ Gedragsrichtlijnen, checklist ▪ Onderlinge afspraken (SLA) ▪ Bewerkersovereenkomsten ▪ Aansluitcriteria *Producten (o.a.)* ▪ Checklist Cloud security (voor instellingen en leveranciers) ▪ Toetsingskaders gegevens-overdracht VO en MBO (voor instellingen en leveranciers) ▪ Toetsingskaders IBB SURF en Taskforce MBO
			

Figuur 1. Samenhang tussen normen bepalen, normen toetsen en normen bewijzen

Zo!

Waar wil of moet ik aan voldoen?

Binnen het onderwijs bestaat er een Referentie Onderwijs Sector Architectuur (ROSA). Daarin zijn uitgangspunten beschreven voor het digitaal uitwisselen van gegevens en het inrichten van de informatiehuishouding van het gehele Nederlandse onderwijs. Zo ontstaat een gemeenschappelijke informatiehuishouding die door de onderwijsinstellingen, het ministerie van OC&W, DUO en andere partijen (zoals leveranciers) in het onderwijsveld gedragen wordt. De ROSA bevat principes, standaarden en bouwstenen en zoekt daarmee aansluiting bij bestaande (internationale) principes en andere (sectorspecifieke) onderwijsarchitecturen. Iedereen die zich in het onderwijs op de een of andere manier bezighoudt met informatie-uitwisseling (zoals projectleiders, beleidsontwikkelaars, bestuurders, onderwijsmanagers en technici) krijgt met de referentiearchitectuur een krachtig hulpmiddel in handen voor de inrichting van de gemeenschappelijke informatie-huishouding.

Binnen het Samenwerkingsplatform Informatie Onderwijs (SION), wordt gewerkt aan een nieuwe bijlage bij de ROSA: de 'katern privacy en security' (katern P&B). Deze katern bevat generieke (juridische) kaders, principes en normen op het gebied van beveiliging en privacy. Vanuit de beschreven principes, kunnen bestaande normen worden gehanteerd. Specifiek voor cloud computing is voor het hoger onderwijs door SURFnet een soortgelijk kader ontwikkeld: het 'Juridisch Normenkader cloudservices'. Dit normenkader is een afgeleide van de wettelijke verplichtingen, die onderwijsinstellingen hebben als zij beheerder zijn van vertrouwelijke gegevens. Verder geeft het een overzicht van de best-practice-clausules voor overeenkomsten met leveranciers van clouddiensten.

Daarnaast worden in het onderwijsveld nog enkele andere initiatieven ontwikkeld in het kader van de ROSA. Voorbeelden van concrete maatregelen en normen die hieruit afgeleid zijn, is het Certificeringsschema Edukoppeling[7]; een duurzame standaardoplossing voor gegevensuitwisseling met cloud leveranciers binnen het onderwijs die voldoet aan de benodigde beveiligingsnormen. Deze Edukoppeling-standaard leidt er toe dat alle ketenpartijen in het onderwijs erop moeten kunnen vertrouwen dat gegevens die aan de leverancier worden verstrekt, op de juiste manier worden verwerkt.

Tot slot zijn er aanvullende initiatieven zoals de Cloud Control Matrix, waarin beschreven staat waaraan clouddiensten moeten voldoen en de Baseline Informatiebeveiliging Rijksoverheid (BIR), die door DUO voor haar gegevensuitwisseling wordt gebruikt.

Alle bovengenoemde (voorbeeld) documenten hanteren het internationaal erkende ISO 27001/27002 normenkader, de zogenaamde Code voor Informatiebeveiliging. Het is dan ook logisch dat iedere onderwijsinstelling kiest voor dit normenkader.[8]

Hoe voldoe ik aan de kaders?

Voor het informatiebeveiligingsbeleid in het mbo zijn het SURF normenkader en het daarvan afgeleide mbo-toetsingskader leidend. Om het assessment te kunnen invullen moeten allereerst de bewijzen (evidence) gecontroleerd worden. Deze bewijzen worden aantoonbaar gemaakt door het verzamelen van documenten (beleidsstukken, vergaderverslagen, e-mails, etc), het houden van interviews op alle niveaus binnen de instelling en waarnemingen ter plaatse (bijvoorbeeld: Is de toegang tot de serverruimte beveiligd d.m.v. een pasje?). Deze bewijzen zijn de input voor het assessment.

Voldoe ik als instelling aan de normen?

Van de principes en kaders, worden dus concrete normen afgeleid. Of en hoe deze normen door de onderwijsinstelling worden toegepast, wordt getoetst door middel van een assessment of audit. Dit kan op drie manieren:

1) Self assessment: de instelling controleert aan de hand van bijvoorbeeld een toetsingsschema of voldaan wordt aan de normen en legt daartoe zelf een verklaring af.

Zo!

2) Peer-auditing: een collega instelling controleert op onafhankelijke wijze of de instelling voldoet aan het normenkader.
3) Externe audit: hierbij voert een professioneel extern auditor een audit uit in de onderwijsinstelling en geeft een officiële verklaring af.

Wat verwacht ik van anderen?

SaMBO-ICT, Kennisnet en SURF zorgen voor de benodigde checklists, handleidingen, sjablonen en toetsingskaders. Hierbij gaat het om aanwijzingen voor gebruik, gedragsrichtlijnen, en voorbeelddocumenten (sjablonen). In het hoger onderwijs is de Checklist Cloud-security daarvan een voorbeeld[9]. Voor het mbo wordt er gewerkt aan een toetsingskader gegevensoverdracht vo-mbo. Hierin zijn richtlijnen opgenomen waarmee getoetst wordt welke eisen gesteld kunnen worden aan de leverancier die de uitwisseling van gegevens tussen vo- en mbo-instellingen faciliteert.

Wie heeft welke verantwoordelijkheid?

Hoe zit het met de verantwoordelijkheden in de mbo-instelling nu, wie is waarvoor verantwoordelijk, in relatie tot de eerder benoemde risico's? Kan het College van Bestuur aangeven of ze 'in control' zijn? Hoe groot is het bewustzijn in de organisatie, zijn er incidenten, wie weet daarvan?

De verantwoordelijkheid voor informatiebeveiligingsbeleid kan op drie gebieden worden toegekend:

1. Beleid en personeel; dit is een gedeelde verantwoordelijkheid van het College van Bestuur en de afdeling HRM.
2. Techniek en continuïteit; dit is een gedeelde verantwoordelijkheid van het College van Bestuur en de ict-afdeling.
3. Toegangsbeveiliging / integriteit en logging / monitoring; dit is een gedeelde verantwoordelijkheid van het College van Bestuur, functioneel beheer en als het even kan een specifiek aangewezen functionaris voor beveiligingszaken, de zogenaamde Security Officer.

Uiteraard is deze indeling voor discussie vatbaar. Het geeft wel een richting aan waarmee gewerkt kan worden. De hoofdgedachte is dat het College van Bestuur op alle niveaus een actieve rol speelt en altijd opdrachtgever is.

Een voorbeeld van samenhang tussen kaders, normen, toetsing, bewijzen en ondersteuning

Het gaat om een woonhuis, waarbij inbrekers buiten moeten worden gehouden. Het huis mag niet toegankelijk zijn voor onbevoegden. Het kader waaraan voldaan moet worden (deelgebied 1) is bijvoorbeeld 'inbreken is bij wet verboden', of 'verboden toegang voor onbevoegden' (wet of kader). De manier om hier aan te voldoen (deelgebied 2), is door het huis degelijk te beveiligen en af te sluiten (het 'hoe'). Om te controleren of aan die norm wordt voldaan (deelgebied 3), kan worden nagegaan of de sloten deugdelijk zijn (bijvoorbeeld alleen gebruik van BORG-geclassificeerde sloten), of dat er een certificering kan plaatsvinden van Politiekeurmerk Veilig Wonen. Bij het voldoen aan de eisen van het keurmerk wordt een certificaat verleend (en meestal stickers voor op de ramen en deuren om potentiele inbrekers af te schrikken). Iedereen kan nu zien dat er maatregelen zijn genomen die aan de norm voldoen (het huis is deugdelijk afgesloten, zodat de verwachting is dat inbrekers buiten gehouden kunnen worden).

Tijdens vakanties zorgt de buurvrouw voor de planten en legt zij de post op tafel. De verwachting en afspraak is wel dat de buurvrouw de sleutel die zij daarvoor nodig heeft, netjes opbergt. Hier is een afhankelijkheid: ook al is het huis beveiligd en is die beveiliging gecertificeerd, als de buurvrouw de deur vergeet af te sluiten, is het huis alsnog kwetsbaar voor inbrekers. Er moet een afspraak (deelgebied 4) komen met de buurvrouw over zorgvuldig gebruik van de sleutel en het afsluiten van het huis.

Zo!

Hoe hebben ze dat in het HO geregeld?

De Nederlandse universiteiten, hogescholen en onderzoeksinstellingen werken samen aan ict-innovaties binnen het SURF samenwerkingsverband. Op bestuurlijk (strategisch), beleidsmatig (tactisch) en uitvoerend (operationeel) niveau werken vertegenwoordigers vanuit hoger onderwijs en onderzoek samen in de SURF-holding. De deelnemende instellingen voor hoger onderwijs en onderzoek zetten beleid uit en ontwikkelen, toetsen en bewaken de kwaliteit ervan.

Het thema 'Security en privacy' is een aantal jaren geleden prominent op de agenda gezet (SURF meerjarenplan 2011-2014 "Samen excelleren"). De aanpak is niet alleen vernieuwend maar ook verfrissend. Vanuit een generieke risicoanalyse waarbij de risico's voor de gemiddelde onderwijsinstelling voor 80 – 90% zijn opgenomen, zijn er modellen en starterkits ontwikkeld, zodat iedere onderwijsinstelling, zonder al te grote investeringen, een informatiebeveiligingsbeleid kan opzetten. Een landelijk netwerk van informatiebeveiligers, werkzaam in het hoger onderwijs is opgezet onder de naam SURFibo. Het doel is de informatiebeveiliging bij hogescholen en universiteiten te verbeteren. Dit doet SURFibo o.a. door het uitwisselen van ervaringen, het gemeenschappelijk verdiepen van kennis, het ontwikkelen van informatiebeleid, beveiligingsprocedures en leidraden.[10,11,12]

Bestaat er zoiets als een (terugkerend) proces van informatiebeveiliging?

Beheersing en ontwikkeling van informatiebeveiliging is binnen het hoger onderwijs opgezet als een iteratief proces.

Daarbij wordt gebruik gemaakt van de 4 fasen van de Deming cirkel (plan-do-check-act).

Op de volgende pagina wordt getoond welke fasen worden onderscheiden.

Aanpak Saxion Hogeschool

Saxion is gestart met een classificatie systeem, waarbij men gestart is met de 15 meest kritische systemen. Vervolgens zijn de overige systemen aangepakt. In totaal worden er ongeveer 600 systemen geclassificeerd.

Concreet zijn de volgende stappen genomen:
1. Classificatie van systemen
2. Opstellen maatregelen matrix bij classificatie niveau
3. Opstellen risico analyse
4. Vastleggen actieplan door management

Voorjaar 2014 is men druk bezig met een bewustwordingsprogramma voor alle medewerkers. Dit om ervoor te zorgen dat ook in de toekomst beveiliging op een afgesproken niveau blijft binnen de organisatie. Dit awareness programma begint laagdrempelig en wordt maandelijks ingezet. Hierbij gaat het in eerste instantie puur om de bewustwording bij de medewerkers (awareness-campagne), maar men wil dit ook gaan borgen via HRM. Het bewustwordingsniveau moet geborgd en vastgesteld worden in een gesprekscyclus.

Zo!

Figuur 2. Informatiebeveiliging als onderdeel van de budgetcyclus

Zo!

Wat moet ik monitoren in het kader van beveiliging?

Het informatiebeveiligingsbeleid van een organisatie kan worden ingericht in verschillende onderdelen of clusters. In de internationaal gebruikte Code voor Informatiebeveiliging, worden 11 thema's (hoofdstukken) beschreven. Binnen het hoger onderwijs wordt hierbij gebruik gemaakt van de SURFaudit. Het SURFaudit toetsingskader biedt onderwijsinstellingen een getrouw beeld waar de instelling staat op het gebied van informatiebeveiliging door een volwassenheidscore toe te kennen, daarbij gebruikmakend van een self-assessment. Hierbij worden voor het onderwijs de volgende clusters onderscheiden:

1. Beleid en Organisatie (informatiebeveiligingsbeleid, classificatie, inrichten beheer)
2. Personeel, studenten en gasten (informatiebeveiligingsbeleid, aanvullingen arbeidsovereenkomst, scholing en bewustwording)
3. Ruimte en Apparatuur (beveiligen van hardware, devices en bekabeling)
4. Continuïteit (antivirussen, back-up, bedrijfscontinuïteit, planning)
5. Toegangsbeveiliging en Integriteit (gebruikersbeheer, wachtwoorden, online transacties, sleutelbeheer, validatie)
6. Controle en logging (systeemacceptatie, loggen van gegevens, registreren van storingen, toetsen beleid)

Aan ieder cluster wordt een volwassenheidsgraad toegekend op basis van bewijs (evidence). Met andere woorden de instelling moet objectief kunnen aantonen op basis van documenten, interviews of waarneming ter plaatse dat de volwassenheidsgraad correct is.

De Autorisatiematrix, voorbeeld van controle op de "werking"

De kernregistratie van deelnemers is een cruciaal onderdeel van het applicatielandschap van een mbo-instelling. Het is het bronbestand voor verschillende andere applicaties (doorgeven van persoonsgegevens van deelnemers aan andere applicaties) en de basis voor de financiering van de onderwijsinstelling (DUO-Bron). Het is dan ook vanzelfsprekend dat alleen de juiste personen de juiste rechten krijgen toebedeeld binnen de applicatie. Doorgaans is dit vastgelegd in de autorisatiematrix.

Deze matrix is vastgelegd in geaccordeerd beleid, is gecommuniceerd met het (betrokken) personeel en wordt door de applicatie afgedwongen. Binnen de auditclusters wordt dus aan alle voorwaarden voldaan.

De accountant zal dan ook vooral kijken naar de wisselingen in het personeelsbestand. Zijn nieuwe collega's toegevoegd (joiners) en zijn vertrokken collega's verwijderd (leavers)? Dit zal doorgaans wel plaatsgevonden hebben. Tot slot zal hij ook onderzoeken of de personen die een andere functie of rol (changers) gekregen hebben ook de daarbij horende rechten hebben gekregen of verloren. Dit is niet altijd het geval. In feite controleert de accountant op deze manier de "werking" van de autorisatiematrix.

Zo!

Welke diepgang wil ik als instelling bereiken?

Een vaak gemaakte kanttekening bij het informatiebeveiligingsbeleid is: het staat nu wel op papier maar wordt het ook toegepast?
De diepgang van het informatiebeveiligingsbeleid kent drie volgtijdelijke niveaus, te weten:

Opzet: Vaststellen dat er beheersmaatregelen aanwezig zijn die waarborgen dat er een continue, integere en exclusieve IT-dienstverlening omtrent de in scope zijnde diensten is. Tevens vaststellen in hoeverre deze beheersmaatregelen schriftelijk zijn vastgelegd.

Bestaan: Vaststellen dat de in beschreven beheersmaatregelen op het moment van onderzoek ook in de praktijk zijn geïmplementeerd.

Werking: Dagelijks toepassen van het informatiebeveiligingsbeleid door zowel de beheerders als door de overige medewerkers.

Het doel is uiteraard om te komen tot het niveau “werking”.

Wat is de rol van de audit?

Het uiteindelijke doel van het informatiebeveiligingsbeleid is om aantoonbaar controle te hebben over de informatiebeveiliging. Een goedkeurende verklaring (zie kader “In Control Statement”) op de jaarrekening gaat dan gepaard met een goedkeurende verklaring op de ict-omgeving.

“In Control Statement” (goedkeurende verklaring)

- **Doel:** verantwoording door het College van Bestuur over de kwaliteit van de interne beheersing van een bepaald onderwerp als onderdeel van de jaarrekening.
- **Verstrekker:** College van Bestuur verstrekt het In Control Statement, beoordeling door accountant (RA of RE).
- **Scope:** Tekst van het In control statement voor een onderwerp, als onderdeel van de jaarrekening maar kan ook zelfstandig.
- **Aanpak:** De auditor onderzoekt als onderdeel van zijn controle of het ‘in control statement’ voldoende basis heeft in de vorm van een “werkend systeem voor interne beheersing en risicomanagement voor het realiseren van de doelstellingen”.
- **Rapportage:** Goedkeuring bij het In Control Statement, zelfstandig of als onderdeel van de jaarrekening.

Jan Visser, PWC

Hoe?

5. Hoe kan ik het informatiebeveiligingsbeleid oppakken?

Hoe breng je informatie-beleid binnen de organisatie onder de aandacht?

Hoe start ik als mbo-instelling?

Hoe pak je dit gestructureerd aan?

Zo!

"Onze studenten en hun ouders/ verzorgers, leerbedrijven en medewerkers mogen erop vertrouwen dat hun privégegevens maar ook studieresultaten bij ons in goede handen zijn. Daarom is informatieveiligheid voor het ROC van Twente een belangrijk onderwerp. In ons beleid omtrent informatieveiligheid zijn afspraken gemaakt hoe wij allemaal bewuster om dienen te gaan met (vertrouwelijke) informatie en hoe we dit vanuit de techniek optimaal ondersteunen. Eigenlijk gewone hygiëne en dus heel erg voor de hand liggend."

Dennis van Zijl,
directeur Financiën,
Studentenadministratie &
Control, ROC van Twente

Hoe start ik als mbo-instelling?

Het is wenselijk om informatiebeveiligingsbeleid eerst maar eens op te laten pakken door iemand die optreedt als kwartiermaker en die een rol heeft waarbij in eerste instantie alleen verantwoording aan het College van Bestuur wordt afgelegd. Op termijn kan de kwartiermaker opgeleid of vervangen worden door de rol/functie van security officer. De kwartiermaker heeft significant capaciteit (tijd en kennis) ter beschikking om een start te maken. Deelname aan of kennis nemen van de netwerken van Kennisnet en saMBO-ICT plus het informatiebeveiligingsprogramma voor het mbo is zeer wenselijk zodat het wiel niet telkens hoeft te worden uitgevonden. Eventueel kan tijdelijke inhuur van expertise overwogen worden.

De kwartiermaker (of de security officer) is een medewerker op een HBO of academisch denkniveau en in het bezit van een ruime ervaring binnen ict. Hij moet de staande ict-organisatie maar ook de mbo-instelling beoordelen op basis van een objectief normenstelsel.

Niet alleen de loonkosten van de security officer zijn een aanslag op het budget van de instelling maar ook de externe ondersteuning (zeker in de beginfase) en de investeringen en exploitatie van audit en monitoring tools. Het is moeilijk aan te geven om welke bedragen het dan gaat.

De kwartiermaker moet voldoende middelen en duidelijke kaders hebben om zijn taak te kunnen vervullen. Het lijkt logisch dat hij start met een nulmeting en vervolgens een baseline (minimaal te behalen waarde) voorstelt aan het College van Bestuur.

Hoe breng je informatiebeleid binnen de organisatie onder de aandacht?

De kwartiermaker moet in de beginfase vooral communiceren met zijn belanghebbenden. Deze zijn in vier groepen onder te verdelen:

1. Opdrachtgever (College van Bestuur)
   Doel: formele goedkeuring van het informatiebeveiligingsbeleid;
2. Gebruikers (personeel)
   Doel: daadwerkelijke toepassing van het goedgekeurde beleid. Postercampagnes, trainingen, maar ook aanvullingen op de arbeidsovereenkomst zijn hier wenselijk;
3. Ict-beheerders
   Doel: ict-beheerders zijn ervan doordrongen dat zij een cruciale rol spelen in het informatiebeveiligingsbeleid. Voor beheerders ligt de weg naar data vaak open, monitoring en logging is dan ook noodzakelijk;
4. Externen
   Doel: afdwingen van het informatiebeveiligingsbeleid met formele overeenkomsten. De realiteit leert dat dit moeilijk is bij overeenkomsten met grote leveranciers (bijvoorbeeld Microsoft).

Het College van Bestuur moet deze communicatie ondersteunen door de kwartiermaker te mandateren. Uiteindelijk moet dit ook leiden tot brede communicatie in de instelling om draagvlak te creëren, cultuuraspecten te adresseren, procedures en protocollen te verspreiden en uiteindelijk dus informatiebeveiliging adequaat in te bedden in de hele organisatie.

Hoe pak je dit gestructureerd aan?

SURFibo heeft een stappenplan ontwikkeld, de zogenaamde Starterkit[13], dat voor de (nieuwe) security officer (kwartiermaker) bruikbaar is. Dit stappenplan kent aan aantal fasen en het kan er voor de mbo-sector als volgt uit zien:

Fase 1: Inventarisatie huidige situatie

Het is belangrijk dat een informatiebeveiliger weet hoe de organisatie in elkaar zit, wat de primaire en ondersteunende bedrijfsprocessen zijn, welke informatiesystemen gebruikt worden om die bedrijfsprocessen te ondersteunen, wie verantwoordelijk is voor het beheer daarvan, etcetera.

Zo!

Fase 1 bestaat dan ook uit het voeren van kennismakingsgesprekken met eigenaren en beheerders van bedrijfsprocessen, informatiesystemen, applicaties, e.d. Als dat inzicht is verkregen (en gedocumenteerd), wordt in overleg met die eigenaren bekeken hoe kwetsbaar de bedrijfsprocessen zijn voor verstoringen in de ict-voorziening: voor de belangrijkste applicaties wordt voor beschikbaarheid, integriteit en vertrouwelijkheid gescoord op een schaal van 1 (nog niets aan beveiliging gedaan) tot 3 (voldoende gedaan). Dit is bekend als de zogenaamde BIV-classificatie.

Daarnaast wordt geïdentificeerd voor welke onderdelen van informatiebeveiliging beleid en procedures bestaan. Denk hierbij onder meer aan de aanwezigheid van een goedgekeurd beleidsdocument, het hebben van een beveiligingsorganisatie waarin iedereen zijn of haar verantwoordelijkheden kent, een gebruiksreglement, een incident registratiesysteem, viruscontrole, etc. Meestal zijn er al technische voorzieningen op beveiligingsgebied getroffen zoals bijvoorbeeld het gebruik van viruscheckers, maar is de informatiebeveiligingsorganisatie nog niet gerealiseerd en het beleid niet vastgesteld.

Onderdeel van fase 1 kan zijn de Social Hack – Integrale securitytest waarin Social Engineering en Ethical hacking worden gecombineerd

Een onderwijsinstelling kan door haar open en gastvrije karakter kwetsbaar zijn voor onbekende (en bekende) gasten met verkeerde intenties. Denk hierbij aan ongeautoriseerde toegang tot cijfers, examens, privacygevoelige studentinformatie of vertrouwelijke stukken van het College van Bestuur. Met een Social Hack kan de onderwijsinstelling op een gecontroleerde manier in een relatief kort tijdsbestek testen hoeveel risico zij loopt om slachtoffer te worden van cyber crime. Daarnaast is een Social Hack bij uitstek een goed middel om het bewustzijn van informatiebeveiliging binnen de onderwijsinstelling te vergroten.

Een Social Hack is bedoeld om een onderwijsinstelling inzicht te geven in kwetsbaarheden en risico's rondom ongeautoriseerde toegang tot afgesloten ruimten, het computer netwerk en applicaties. Tijdens een Social Hack worden zogeheten social engineering technieken en technisch hacken gecombineerd in een integrale securitytest.

Met een Social Hack wordt een aanval gesimuleerd van een kwaadwillende bezoeker die zich via publieke ruimtes van de onderwijsinstelling toegang probeert te krijgen en gevoelige (digitale) informatie weet te benaderen. De nadruk bij deze gesimuleerde aanval zal liggen op het doorbreken van maatregelen om toegang te verkrijgen tot het interne netwerk van buitenaf.

Wanneer deze zogeheten "mystery guest" eenmaal toegang heeft tot het computernetwerk van de onderwijsinstelling, worden technische ethical hacking methoden toegepast om te onderzoeken of ongeautoriseerd toegang kan worden verkregen tot gevoelige informatie. In een duidelijke rapportage worden de gehanteerde scenario's, eventuele bevindingen, geconstateerde risico's en aanbevelingen voor verbetering vastgelegd.

Een onderwijsinstelling kan een Social Hack in opdracht laten uitvoeren door professionele, tot ethical hacker gecertificeerde security specialisten.

Zo!

Fase 2: Korte termijn verbeteringen en opstellen plan van aanpak
Om aan het bestuur aan te kunnen tonen dat het loont om structureel aandacht aan informatiebeveiliging te geven worden de meest lonende maatregelen doorgevoerd (laaghangend fruit). Deze zijn afgeleid uit de inventarisatie van kwetsbaarheden en de stand van zaken m.b.t. te nemen maatregelen. In deze fase wordt ook een plan van aanpak voor de lange termijn opgesteld, waarin alle aspecten van informatiebeveiliging aan de orde komen. In dat plan komen projectvoorstellen te staan die de komende jaren uitgevoerd moeten worden. Denk hierbij aan het opstellen van een baseline informatiebeveiliging, het inrichten van de informatiebeveiligingsorganisatie en maatregelen op het gebied van bedrijfscontinuïteit.

Fase 3: De dialoog met bestuurders
In deze fase is het belangrijk om commitment van het bestuur te krijgen. Kan de informatiebeveiliger het bestuur overtuigen van het belang van structurele aandacht voor informatiebeveiliging?
In principe kan dit op basis van de al eerder genomen maatregelen (laaghangend fruit) en de risicoverlaging die daarmee gerealiseerd is.

Verschillende gesprekken en presentaties zijn nodig om duidelijk te maken dat informatiebeveiliging helpt om de overall doelstellingen van de onderwijsinstelling te realiseren. Aandacht voor de Wet Bescherming Persoonsgegevens, aansprakelijkheidsclaims van opdrachtgevers, reputatieschade, het niet 'in control' zijn, zijn doorgaans zaken die tot inzicht kunnen leiden. Het is wenselijk om te wijzen op de ontwikkelingen die in gang zijn gezet door Kennisnet en saMBO-ICT. Deze organisaties vergroten door conferenties en presentaties de bewustwording van de bestuurders. Uiteindelijk ontstaat er betrokkenheid en worden middelen (menskracht en euro's) ter beschikking gesteld voor de uitvoering van het gepresenteerde plan van aanpak.

Fase 4: Projectmatige uitvoering plan van aanpak
Informatiebeveiliging moet beheersbaar gemaakt worden. Daarvoor is aansluiting op de budgetcyclus noodzakelijk. Dus zal er naast het opstellen van beleid en het inrichten van een informatiebeveiligingsorganisatie waarin rollen en verantwoordelijkheden zijn beschreven, ook gewerkt moeten worden aan het inrichten van de Plan-Do-Check-Act-cyclus voor informatiebeveiliging. Dat geeft ook mogelijkheden om delen van het plan van aanpak in de jaarbegroting op te nemen. Verder moet er gewerkt worden aan de inrichting van een risico-methodiek, het incident managementproces, het inrichten van een communicatie- en rapportagestructuur en de uitvoering van diverse deelprojecten uit het plan van aanpak. Het is uiteraard noodzakelijk dat iedere medewerker doordrongen is van de noodzaak van informatiebeveiliging en daar dan ook vanzelfsprekend zijn steentje aan bijdraagt.

Fase 5: Beheer
Het is cruciaal de status van informatiebeveiliging in de instelling te monitoren en, bij geconstateerde tekortkomingen, maatregelen te treffen. Dit kan door het uitvoeren van nieuwe risicoanalyses, door het (laten) uitvoeren van audits, door het inhuren van een 'mystery-guest' die de vinger op de zere plekken legt, etc. Onderdeel van beheer is ook de bevordering van bewustwording. Dat kan middels trainingen via een intranetsite, posters en/of e-learning. Waar het om gaat is dat het beleid bekend wordt gemaakt en wordt gehandhaafd. Dit vergt de nodige aandacht. Mensen kennen de risico's onvoldoende en doen, soms uit behulpzaamheid, dingen die beter achterwege gelaten kunnen worden (social engineering) en daar moet op getraind worden. Controle, naleving en sancties vormen het onvermijdelijke sluitstuk van een serieus informatiebeveiligingstraject. Interne en externe accountants kunnen daarbij behulpzaam zijn.

Hoe?

6. Hoe wordt informatiebeveiligingsbeleid toegepast in de praktijk?

Hoe werkt een IT Audit?

Hoe wordt het normenkader toegepast?

Welke kwaliteitsaspecten worden toegepast?

Hoe ziet de governance er uit bij een mbo-instelling?

Om welke documenten, procedures en protocollen gaat het?

Wet- en regelgeving, waar heb ik mee te maken?

Zo!

Hoe werkt een IT-Audit?[14]

IT-auditing is het vakgebied dat zich bezighoudt met het beoordelen van de automatisering van de organisatie en de organisatie van de automatisering. IT-auditing is een specialisme binnen het auditing-vakgebied. Het specialisme wordt meer en meer gevraagd bij uitvoering van accountantscontroles.

Tot enkele jaren geleden heette het vakgebied EDP-Auditing, ofwel beoordeling van Electronic Data Processing. De laatste decennia heeft IT-auditing zich verbreed tot de relatie bedrijfsprocessen en ict en richt de aandacht zich minder op het rekencentrum en systeemontwikkelafdelingen. Aanleiding voor het ontstaan van het vakgebied is de toenemende automatiseringsgraad. Doordat de verwerking van administratieve processen steeds meer binnen geautomatiseerde informatiesystemen plaatsvond, kon een accountant veelal onvoldoende zekerheid meer krijgen omtrent de getrouwheid van de financiële verslaglegging van organisaties. Het doorgronden van geautomatiseerde informatiesystemen vergt andere kennis dan alleen bedrijfseconomie en administratieve organisatie.

Hoe wordt het normenkader toegepast?

Kenmerkend voor het vakgebied auditing is dat een onderzoek plaatsvindt ten opzichte van een eerder opgesteld en afgestemd normenkader. Zonder normenkader is een onderzoek feitelijk geen audit.

SURFaudit hanteert het generieke internationale normenkader voor informatiebeveiliging ISO27001 en de daarvan afgeleide set van best practices ISO 27002. In de literatuur is dit normenkader bekend onder de titel “Code voor Informatiebeveiliging”. Het operationele toetsingskader van de SURFaudit is afgeleid van ISO 27002.

Clustering naar zes thema’s

SURFaudit heeft de 84 onderdelen ingedeeld in zes clusters. De clustering is gebaseerd op een logische indeling die goed bruikbaar is voor het mbo-onderwijs. Per cluster zijn ook de kwaliteitsaspecten toegevoegd.

Cluster	Onderwerpen (o.a.)	Kwaliteitsaspecten	Betrokkenen
1. Beleid en Organisatie	Informatiebeveiligingsbeleid Classificatie Inrichten beheer	Beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid	College van Bestuur Directeuren
2. Personeel, studenten en gasten	Informatiebeveiligingsbeleid Aanvullingen arbeidsovereenkomst Scholing en bewustwording	Beschikbaarheid en integriteit	College van Bestuur Dienst HR Ondernemingsraad
3. Ruimte en Apparatuur	Beveiligen van hardware, devices en bekabeling	Integriteit en beschikbaarheid	College van Bestuur Ict dienst of afdeling
4. Continuïteit	Anti virussen, back up, bedrijfscontinuïteit planning	Beschikbaarheid	College van Bestuur ict dienst of afdeling Functioneel beheer
5. Toegangs-beveiliging en Integriteit	Gebruikersbeheer, wachtwoorden, online transacties, sleutelbeheer, validatie	Integriteit en vertrouwelijkheid	College van Bestuur Functioneel beheer Ict dienst of afdeling
6. Controle en logging	Systeemacceptatie, loggen van gegevens, registreren van storingen, toetsen beleid	Controleerbaarheid	College van Bestuur Stafmedewerker informatie-beveiliging

Tabel 2. Clustering naar thema’s

Zo!

Welke kwaliteitsaspecten worden toegepast op informatiebeveiliging?

Het toetsingskader gaat uit van de kwaliteitsaspecten Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid.

Beschikbaarheid: de mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is;
- Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is;
- Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

Integriteit: de mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;
- Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
- Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Vertrouwelijkheid: de mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.
Deelaspecten hiervan zijn:

- Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is;
- Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is;
- Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn;
- Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

Controleerbaarheid: de mogelijkheid om kennis te verkrijgen over de structurering (documentatie) en werking van de IT-dienstverlening.
Deelaspecten hiervan zijn:

- Testbaarheid: De mate waarin de integere werking van de IT-dienstverlening te testen is;
- Meetbaarheid: Zijn er voldoende meet- en controlepunten aanwezig;
- Verifieerbaarheid: De mate waarin de integere werking van een IT-dienstverlening te verifiëren is.

De kwaliteitsaspecten effectiviteit en efficiëntie worden verder niet besproken. In een financiële ict-benchmark worden deze onderzocht, maar niet in de SURFaudit.

Hoe kan ik de processen in mijn instelling indelen naar risiconiveau?

Onderdeel van het toetsingskader is de zogenaamde BIV-classificatie. In de toekomst zullen alle gegevens waarop dit informatiebeveiligingsbeleid van toepassing is, geclassificeerd moeten zijn. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse.

De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risico analyses.

Zo!

De BIV-classificatie is afgeleid van de bovenstaande kwaliteitsaspecten. Daarvan worden er drie toegepast:

- **B**eschikbaarheid
- **I**ntegriteit
- **V**ertrouwelijkheid

Ten aanzien van de **beschikbaarheid**seisen worden de volgende klassen onderscheiden:

Klasse	Basisprincipes	Beveiligingsniveau
Niet vitaal	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar klanten.	Basisbescherming
Vitaal	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar klanten.	Basisbescherming +
Zeer vitaal	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 etmaal brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar klanten.	Basisbescherming ++

Tabel 3. Klassen i.r.t. beschikbaarheid

Welk beveiligingsniveau geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt. De classificatie dient door of namens de eigenaar van het betreffende informatiesysteem te worden bepaald.

Voor **integriteit** en **vertrouwelijkheid** worden de volgende indeling gevolgd.

Klasse	Basisprincipes	Beveiligingsniveau
Openbaar	▪ Iedereen mag de gegevens inzien, bijvoorbeeld de website van een mbo-instelling ▪ Een geselecteerde groep mag deze gegevens wijzigen	Basisbescherming
Intern	▪ Iedereen die aan de instelling is verbonden als medewerker of student mag deze gegevens inzien; toegang kan zowel binnen als buiten de instelling (remote) worden verleend, bijvoorbeeld voor de lesroosters of de Elektronische leeromgeving ▪ Een geselecteerde groep mag deze gegevens wijzigen.	Basisbescherming
Vertrouwelijk	▪ Er is expliciet aangegeven wie welke rechten heeft t.a.v. de raadpleging en de verwerking van deze gegevens, bijvoorbeeld Kernregistratie systeem.	Basisbescherming +

Tabel 4. Klassen i.r.t. integriteit en vertrouwelijkheid

Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen. Met basisbescherming + wordt dus een hoger beveiligingsniveau bedoeld dan bij basisbescherming. Basisbescherming ++ is het hoogste beschermingsniveau bij een mbo-instelling.

Zo!

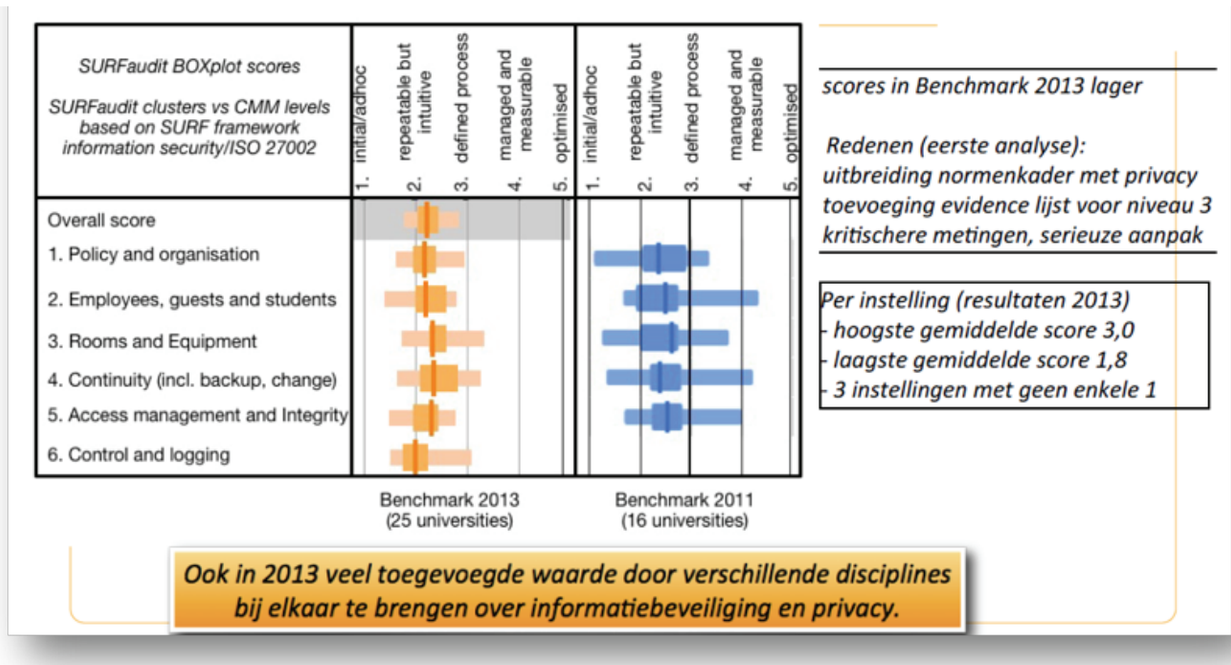
Waar sta ik? Wat zijn maturity levels?

Het **Capability Maturity Model** is een model dat aangeeft op welk niveau de informatiebeveiliging van een organisatie zit. Door ervaring in het gebruik is gebleken dat dit model op diverse processen in de organisatie toepasbaar is, ook op informatiebeveiligingsbeleid.

Het model onderscheidt vijf niveaus:

1. Initial: op dit niveau is de aanpak chaotisch en ad hoc. Problemen worden pas opgelost als ze zich voordoen. Dit is het niveau waarop iedere organisatie start.
2. Repeatable: is het niveau waarbij de organisatie zover geprofessionaliseerd is (bijvoorbeeld door het invoeren van projectmanagement) dat bij het ontwikkelproces gebruik wordt gemaakt van de kennis die eerder is opgedaan. Beslissingen worden dus genomen op basis van ervaring. De kennis is aanwezig in de hoofden van de medewerkers.
3. Defined: is het niveau waarbij de belangrijkste processen zijn gestandaardiseerd. De kennis is onafhankelijk van personen en is volledig beschreven in documenten (procedures, werkinstructies, etc.).
4. Managed: is het niveau waarbij de kwaliteit van het ontwikkelproces wordt gemeten zodat het kan worden bijgestuurd.
5. Optimised: is het niveau waarbij het ontwikkelproces als een geoliede machine loopt en er alleen maar sprake is van fijn afstemming (de puntjes op de i).

De SURFaudit benchmark (zie figuur 4)[19] geeft aan dat van de 25 deelnemende universiteiten en Hbo-instellingen slechts drie onderwijsinstellingen op alle beheersmaatregelen tenminste op het volwassenheidsniveau 2 scoorden. Bij de rest van de onderwijsinstellingen zat er in de scores altijd wel een 1 bij. En ook hier geldt dat de zwakste schakel de sterkte van de ketting bepaalt.



Figuur 3. SURFaudit – resultaten Bechmark 2013

Zo!

Hoe ziet de governance er uit bij een mbo-instelling?

Governance geeft aan hoe de verantwoording georganiseerd is en wie waarvoor verantwoordelijk is. Van belang daarbij is om onderscheid te maken naar richtinggevend of strategisch, sturend of tactisch en operationeel niveau. Bij de benaming van rollen wordt zoveel mogelijk aangesloten bij het PvIB.4 (Functies in de informatiebeveiliging. Platform voor Informatiebeveiliging (PvIB), 2006)

De Information Security Officer is een nieuwe rol op strategische (en tactisch) niveau die rechtstreeks aan het College van Bestuur verantwoording aflegt, net als de controller en de kwaliteitsmanager. Hij toetst het ict-beleid en adviseert in nauw overleg met de directeur ict en/of de Informatiemanager het College van Bestuur. De Information Security Officer bewaakt ook de uniformiteit binnen de instelling. De rol van Information Security Manager is vormgegeven op het ondersteunend niveau van elke sector, portaal of dienst. Deze vervult een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit doen ze samen met de Information Security Officer (vanwege de uniformiteit) en met de eigenaren van de technische platforms. De rol van Information Security Manager kan worden ingevuld door een functionele beheerder van een applicatie. Op operationeel niveau wordt overlegd met de functionele (functioneel beheer Financiën en functionele beheerders van bijvoorbeeld educatieve applicaties) en technische beheerders. Er wordt aandacht besteed aan de implementatie van de informatiebeveiligingsmaatregelen.

Ten aanzien van de financiering van informatiebeveiliging kunnen binnen een mbo-instelling de volgende richtlijnen worden gevolgd:

- Algemene zaken, zoals het opstellen van een informatiebeveiligingsplan voor de gehele instelling of een externe audit, worden uit het centrale ict-budget betaald.
- De beveiliging van informatiesystemen komt ten laste van het informatiesysteem zelf.
- Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten.
- Hetzelfde geldt voor bewustwording en training: er kunnen instellingsbrede bewustwordingscampagnes zijn (centraal gefinancierd) en lokale voorlichting en training voor specifieke toepassingen of doelgroepen (decentraal gefinancierd).

Niveau	Wat?	Wie?	Overleg	Documenten
Richtinggevend	▪ Bepalen IB strategie ▪ Organisatie t.b.v. IB inrichten ▪ IB-planning en control vaststellen ▪ Business continuity management	▪ CvB, i.c. Portefeuillehouder IB, o.b.v. advies Information Security Officer (kwartiermaker) ▪ Directeur Bedrijfsdienst of ict	CvB stelt vast Strategisch ict-overleg adviseert	▪ IB beleidsplan ▪ IB baseline (basis maatregelen) ▪ Business continuity plan
Sturend	▪ Planning & Control IB: ▪ Voorbereiden ▪ Normen en wijze van toetsen bepalen ▪ Evalueren beleid en maatregelen ▪ Begeleiden van externe audits	▪ Proceseigenaar ▪ Information Security Officer (kwartiermaker) ▪ Information Security Manager (functioneel beheerder)	Tactisch IB overleg	▪ Risicoanalyses en audits ▪ Jaarplan en verslag
Uitvoerend	▪ Implementeren IB-maatregelen ▪ registreren en evalueren incidenten ▪ communicatie eindgebruikers	▪ Information Security Manager (functioneel beheerder) ▪ Overige Functioneel Beheerders ▪ Ict-medewerkers	Operationeel IB overleg	▪ SLA's (security paragraaf) ▪ Incidentregistratie, incl. evaluatie

Tabel 5. Inrichting van governance op verschillende niveaus

Zo!

Om welke documenten, procedures en protocollen gaat het?

Een mbo-instelling die haar informatiebeveiliging op orde heeft zou de volgende documenten moeten kunnen overleggen (opzet), die overigens ook goedgekeurd zijn (bestaan) en daadwerkelijk worden toegepast (werking);

1. Het informatiebeveiligingsbeleid
2. Baseline van maatregelen (basisniveau maatregelen)
   Deze baseline beschrijft de maatregelen die minimaal nodig zijn om instelling breed een minimaal niveau van informatiebeveiliging te kunnen waarborgen. Bijvoorbeeld volwassenheidsniveau 2.
3. Jaarplan/verslag
   Elk jaar leveren de Security Managers een jaarverslag en een jaarplan voor het volgende jaar in bij de Security Officer. Het jaarplan is mede gebaseerd op de resultaten van de periodieke controles / audits. Er wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (incl. genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Dergelijke verslagen kunnen geconsolideerd worden in de bestuurlijke Planning & Control-cyclus. Waar nodig wordt apart aandacht besteed aan decentrale systemen.
4. Business Continuity Plan
   Business Continuity Management (BCM) is de benaming van het proces dat potentiële bedreigingen voor een organisatie identificeert en bepaalt wat de impact op de “operatie” van de organisatie is als deze bedreigingen daadwerkelijk manifest worden.
5. Dienstenniveau overeenkomsten (SLA’s)
   Een service level agreement (SLA) is een overeenkomst tussen een leverancier en een afnemer. Bijvoorbeeld de ict-afdeling sluit met externe leveranciers een SLA af t.b.v. de ondersteuning van concernsystemen. Dat zijn contracten met afspraken en randvoorwaarden over geleverde diensten. In deze contracten zit standaard een informatiebeveiligingsparagraaf, waarin de verantwoordelijkheden van de leverancier zijn opgenomen. Bij leveranciers die de beschikking krijgen over persoonsgegevens van en over leerlingen en personeel, wordt naast de SLA ook een (wettelijk vereiste) bewerkersovereenkomst gesloten.
6. Inhuur- en uitbestedingscontracten
   Bij de inhuur van diensten en personeel van derde partijen zal ook aandacht aan informatiebeveiliging besteed moeten worden, bijvoorbeeld door te stellen dat het instellingsbeleid ook van toepassing is voor hen. Hetzelfde is van belang bij uitbestedingen. Ook hier moeten zo nodig bewerkersovereenkomsten worden gesloten als deze derde partijen toegang krijgen tot persoonsgegevens.
7. Procedures en protocollen
   Gedragscodes en richtlijnen voor medewerkers, studenten en derden, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging zoals bijvoorbeeld:
   - Acceptable use policy, voor het veilig gebruik van ict-voorzieningen (bijvoorbeeld: Bruikleenovereenkomst notebooks);
   - Wachtwoordenbeleid;
   - Toepassing van cryptografische hulpmiddelen (bijvoorbeeld in het kader van examineren);
   - Classificatierichtlijnen;
   - Beleid voor het afsluiten van servers en werkstations;
   - Integriteit en gedragscode voor ict-functionarissen;
   - Gedragscode voor veilig e-mail en internetgebruik;
   - Privacyreglement of -protocol;
   - Protocol social media.

Zo!

Wet- en regelgeving, waar heb ik mee te maken?

Bij het inrichten van beleid rond informatiebeveiliging is het belangrijk rekening te houden met onderstaande wetten en regelgeving.

Wet Educatie en Beroepsvorming (WEB)

De wetgever geeft nadrukkelijk aan hoe en in welke gevallen het bevoegd gezag gebruik mag maken van het persoonsgebonden nummer.

In de WEB is tevens de medezeggenschap voor leerlingen en hun ouders geregeld. Deelnemers- en ouderraden moeten instemmen met alle besluiten van een instelling als het de privacy van leerlingen en hun ouders betreft. Dus bij het vaststellen van een privacyreglement is instemming nodig, maar ook voor het recht op inzage door de instelling in computerbestanden of devices waar leerlingen tijdens de lessen mee werken.

Wet op de Ondernemingsraden (WOR)

De instelling heeft de instemming nodig van de ondernemingsraad voor elk (voorgenomen) besluit tot vaststelling, wijziging of intrekking van een regeling omtrent het gebruik en de bescherming van de persoonsgegevens van de in de onderneming werkzame personen.

Dit instemmingsrecht ligt voor de hand bij het vaststellen van bijvoorbeeld een privacyreglement. Logging en monitoring zijn eveneens een zaak van de OR. Ondernemingsraden spelen bij de privacybescherming van medewerkers op de werkplek een cruciale rol. De WOR bepaalt dat een ondernemer de instemming van de OR nodig heeft als hij regelingen voor persoonsgegevens van medewerkers wil verwerken.

Wet Bescherming Persoonsgegevens (WBP)

Hierin is de bescherming van de privacy van ‘betrokkenen’ (leerlingen, ouders en personeel) geregeld. De wet geeft een aantal algemene kaders (niet specifiek voor het onderwijs). Uit deze wet volgt dat een instelling verplicht is om passende technische en organisatorische maatregelen te nemen om verlies en onrechtmatige verwerking van persoonsgegevens van leerlingen, en personeel te voorkomen.
Hoe gevoeliger de gegevens, des te meer eisen kunnen worden gesteld. Alhoewel de wet geen technische maatregelen voorschrijft, blijkt dat verwacht wordt dat bedrijven en instellingen toch tenminste uitgaan van de normen die volgen uit de Code voor Informatiebeveiliging. Naleving van de beveiligingsmaatregelen leidt in dit geval dus tot voldoen aan de wettelijke kaders. De Europese Privacy Verordening (EPV) zorgt ervoor dat de WBP verder wordt aangescherpt. Zo zijn de boetes, bij een overtreding, fors verhoogd.

Archiefwet

Een mbo-instelling dient zich te houden aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie die is vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d. Hieronder vallen ook bewaar- en vernietigingstermijnen. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

Auteurswet

Een mbo-instelling zorgt ervoor dat er geen originele werken verspreid worden, zonder dat daarvoor toestemming is verkregen van de eigenaar. Dit betekent dus dat er geen illegale software gebruikt wordt; er is beleid op beheer van (geldige) licenties. Het verdient ook aanbeveling om binnen de instelling afspraken te maken over handhaving en controle hierop.

Telecommunicatiewet

Zolang het communicatienetwerk van een mbo-instelling alleen aan studenten, personeel en bezoekers beschikbaar wordt gesteld, is de Telecommunicatiewet niet van toepassing.

Zo!

Wetboek van Strafrecht (WvSr)
De bepalingen uit het Wetboek van Strafrecht die gaan over computercriminaliteit, worden ten onrechte wel de Wet Computercriminaliteit genoemd. Wil er sprake zijn van strafbaar handelen, dan moet de instelling toch ten minste basale beveiligingsmaatregelen hebben genomen. Zo is bijvoorbeeld het forceren met gereedschap van een voordeur strafbaar (inbraak), maar het binnenlopen van een huis met openstaande voordeur is dat niet.

Politie en Justitie kunnen een school altijd vragen om informatie vrijwillig te geven, maar de mbo-school is daar niet toe verplicht. Het advies is dan ook om terughoudend te zijn met het vrijwillig verstrekken van informatie en persoonsgegevens.

De instelling kan pas verplicht worden gegevens te delen als politie of Justitie de informatie opvragen in het kader van de strafrechtelijke opsporing of om een misdrijf te voorkomen. Daarbij moet het wel gaan om concrete en relevante gegevens; het ligt niet voor de hand dat men de behaalde cijfers van een verdachte student nodig heeft om een inbraak op te lossen. Meestal vraagt de (hulp)officier van justitie gegevens op bij een onderwijsinstelling, maar het is ook mogelijk dat een onderzoeksrechter (rechter-commissaris) erom vraagt. In juridische termen worden dan gegevens ‘gevorderd’. Deze vordering moet op de wet zijn gebaseerd. Zo’n vordering staat vaak op papier. Vaak gaat het om het verkrijgen van aanwezigheidsregistratie, inloggegevens of elektronisch berichtenverkeer van een leerling. Hoe uitvoerig de informatie moet zijn die wordt verstrekt, hangt meestal af van de omstandigheden.

Burgerlijk Wetboek (BW)
Met de invoering van de elektronische handtekening in Nederland, kunnen documenten nu ook digitaal worden ongetekend. Elektronische handtekeningen hebben de zelfde rechtsgevolgen als een schriftelijke ‘natte’ handtekening, zolang de authenticatie methode (het controleren van de handtekening) voldoende betrouwbaar is.

In het BW is geregeld welke eisen aan de handtekening mogen worden gesteld. Zelfs in het geval dat de wet een schriftelijke ondertekening van een contract (bijvoorbeeld de onderwijsovereenkomst) eist, hebben de ondertekenaars het recht een digitale handtekening te zetten. Het gebruik kunnen maken van de elektronische handtekening stelt eisen.

Een elektronische handtekening wordt vermoed voldoende betrouwbaar te zijn, als de elektronische handtekening:
a. op unieke wijze aan de ondertekenaar is verbonden,
b. het mogelijk maakt de ondertekenaar te identificeren,
c. tot stand komt met middelen die de onder controle zijn van de ondertekenaar,
d. opsporing van een wijziging in de ondertekende gegevens ook achteraf mogelijk is,
e. gebaseerd is op een ‘gekwalificeerd certificaat’,
f. gegenereerd is door een ‘veilig middel’.

Hoe?

7. Wat kunnen we sectorbreed doen?

Hoe kunnen we sector-breed samenwerken?

Is er scholing voorhanden?

Hoe kunnen we het mbo benchmarken?

Wat kan ik met assessments en audits?

Zo!

Informatiebeveiligingsbeleid is een groot en complex thema. Zelf het wiel uitvinden is moeizaam en kostbaar. Bovendien, de keten is even sterk als de zwakste schakel. Dat geldt ook voor het mbo. Daarom zouden alle instellingen aan een bepaalde norm moeten voldoen. Maar dan moet je wel samen optrekken, kaders ontwikkelen, informatie delen en voortuitgang boeken. Wat kan er allemaal sector breed worden opgepakt?

Hoe kunnen we samenwerken?

Het bereiken van een voldoende volwassenheidsniveau van informatiebeveiliging zal in eerste instantie in de instellingen zelf plaats moeten vinden. Wel kunnen verschillende gezamenlijke acties worden ingezet om instellingen te ondersteunen, in de vorm van tools, voorbeelden, bijeenkomsten, scholing enz. Wat is er op dit gebied allemaal al ingezet en op welke wijze kunnen instellingen daar gebruik van maken en aan bijdragen?

Samenwerken:
Voor de mbo-sector is een Taskforce Informatiebeveiligingsbeleid (IBB) actief. Deze is samengesteld uit informatiebeveiliging verantwoordelijken, deskundigen en vertegenwoordigers van Kennisnet, SURF en saMBO-ICT. De Taskforce IBB werkt aan het realiseren van een set van gezamenlijke activiteiten die voor het hele mbo-veld relevant zijn in het kader van informatiebeveiligingsbeleid. Daarbij wordt vooral uitgegaan van de expertise die bij het hoger onderwijs door SURF is ontwikkeld.

Maar ook bovensectoraal wordt er binnen SION (Samenwerkingsplatform Informatie Onderwijs) samengewerkt aan sector overstijgende vraagstukken over gegevensuitwisseling in het onderwijs.

Draagvlak en bewustwording:
Er wordt in het begin veel aandacht besteed aan het creëren van een breed draagvlak en bewustwording. Niet alle lagen binnen instellingen zijn zich bewust van risico's van het gebruik van digitale middelen. Datzelfde geldt voor landelijke organisaties, zoals de MBO Raad of examenleveranciers.

De activiteiten rondom het realiseren van draagvlak, zijn gericht op twee aspecten:
1. Bewustwording bij landelijke organisaties;
2. Bewustwording bij verantwoordelijken binnen instellingen.

Bij dit tweede aspect richt de aandacht zich vooral op Colleges van Bestuur, op het onderwijsmanagement en op de ondersteunende organisatieonderdelen. Daarbij wordt aangesloten op de activiteiten die instellingen zelf uitvoeren. Om draagvlak binnen de instellingen te stimuleren worden concrete middelen ontwikkeld om die informatiebeveiliging op de agenda zetten, zoals voorlichtingsmateriaal, posters, brochures, een ondersteunende website en uiteraard deze Hoe? Zo! publicatie.

Kennisontwikkeling en kennisdeling:
Om het deskundigheidsniveau van het mbo als sector in het algemeen en van de instellingen specifiek te vergroten, wordt een aantal activiteiten gestart. De sector maakt daarbij volop gebruik van de kennis en ervaring die het hoger onderwijs al eerder hebben opgedaan. In specifieke bijeenkomsten voor kwartiermakers, beveiligingsmedewerkers en security officers, maar ook in bestaande netwerken zoals het informatiemanagersnetwerk zal IBB kennis en ervaring gedeeld worden. Op termijn zou het mbo ook kunnen aansluiten bij de SURF structuur voor IBB, zoals het netwerk SURFibo en de beveiligingsconferentie die zij organiseren.

Ook wordt er aandacht aan training en scholing besteed. Er worden masterclasses georganiseerd. Deze bestaan uit een serie van vijf volle dagen, elk gericht op een specifiek thema. De doelgroep bestaat uit kwartiermakers, beoogde Security Officers, IT verantwoordelijken, Informatiemanagers, enz. Deze masterclasses worden verzorgd door deskundigen op het terrein van Informatiebeveiliging.
De behandelde thema's concentreren zich op:
- Starterskit Informatiebeveiligingsbeleid;
- Training en toepassing risk assessment;
- Scholing theoretisch kader informatiebeveiliging en IT-audit;

Zo!

- Toepassing SURFaudit;
- Actief ontwikkelen door deelnemers van een concept informatiebeveiligingsbeleid voor de eigen mbo-instelling op basis van bovengenoemde onderwerpen.

De masterclasses worden georganiseerd door Kennisnet, SURF en saMBO-ICT onder verantwoordelijkheid van de Taskforce IBB. Daarnaast zullen ook mogelijke andere scholingstrajecten worden geïnventariseerd.

Tot slot zullen Kennisnet, Surf en saMBO-ICT zorgdragen voor de bundeling van inhoudelijke informatie voor de professionals binnen de scholen. Dat gebeurt in de vorm van een website en een publicatie waarin alle deelpublicaties zijn opgenomen. In deze publicaties wordt naast verdieping en theorie ook dieper ingegaan op de inrichting van een aantal IBB-beheerorganisaties binnen de instellingen, waarbij deze best practices een beeld geven van een mogelijke structuur op zowel kwantitatief (kosten) als kwalitatief (functies) gebied.

Top 3 van issues die regelmatig ge-audit moeten worden:

1. Testen van restore en uitwijk (heeft impact op de productie omgeving en is kostbaar, maar wel van belang).
2. Autorisatiebeheersing (deze is vaak in opzet goed, maar beheersing wordt vervolgens minder goed uitgevoerd. Heeft ook te maken met het configuratiemanagement van de hardware).
3. Wordt er gewerkt volgens verwachting, in casu worden instructies ook afgestemd op de protocollen en procedures en worden deze goed opgevolgd.

Ronald Sarelse, IT Auditor Radboud Universiteit Nijmegen

Hoe kunnen we het mbo benchmarken?

Naast deze Hoe?Zo! publicatie is een stappenplan noodzakelijk om informatiebeveiliging daadwerkelijk in de volle breedte te implementeren binnen de instellingen. Op basis van de Starterkit die voor het hoger onderwijs is ontwikkeld, wordt een generiek plan voor de mbo-scholen gemaakt. Dat stappenplan beschrijft wat een instelling kan doen. Onderdeel van dit stappenplan, is een generiek beleidsplan (Informatiebeveiligingsbeleid). Een dergelijk plan is voor de instellingen een referentie (aanzet) om het eigen beleid vorm te geven. Het is geen invuloefening of trucje om snel een document klaar te hebben liggen. Het gaat tenslotte niet alleen om het hebben van documenten of procedures, het belangrijkste is gedrag en cultuur.

Toetsingskader mbo

Naast het hebben van een informatiebeveiligingsbeleid, is het belangrijk te weten wanneer het beleid afdoende is, dus aan welke norm het moet voldoen en hoe dit getoetst kan worden. Een toetsingskader geeft op basis van normen weer aan waar instellingen aan moeten voldoen om op een bepaald volwassenheidsniveau te kunnen scoren. Dit toetsingskader is gebaseerd op de ISO 27002 norm (Code voor Informatiebeveiliging). De mbo-sector sluit hierbij aan.

In het toetsingskader wordt ook de mate, waarin aan een norm moet worden voldaan, beschreven. Dit gebeurt op basis van een 5 puntenschaal. Daarbij wordt onderscheid gemaakt tussen een minimumniveau en het streefniveau. Het toetsingskader is onderdeel van overleg tussen de mbo-sector en het ministerie van OC&W. Doel is om uiteindelijk gezamenlijke normen vast te stellen.

Verder wordt er met alle sectororganisaties, het ministerie van OC&W en DUO samengewerkt aan het ontwikkelen van een katern ‘Privacy en security’, als onderdeel van de Referentie Onderwijs Sector Architectuur (ROSA). Ook is er de standaard Edukoppeling ontwikkeld die beschrijft aan welke eisen de elektronische berichtenuitwisseling van SaaS-leveranciers moet voldoen.

Quick scan en benchmark

Het meten van de situatie binnen een instelling op basis van vastgestelde toetsingskader is belangrijk voor de instelling om te weten

Zo!

naar welke onderwerpen vooral aandacht uit moet gaan. Met behulp van een bestaande tool (quick scan) kan de instelling binnen het toetsingskader worden beoordeeld. De tool die hiervoor binnen het hoger onderwijs wordt gebruikt wordt aangepast voor het mbo toetsingskader en er zal een handleiding specifiek voor het mbo aan worden toegevoegd. De tool maakt het mogelijk om de eigen situatie af te zetten tegen het gemiddelde in de mbo-sector. Het zal een duidelijk beeld geven voor de instelling zelf, maar bij voldoende deelname ook voor de sector als geheel. Daarmee is het een eerste benchmark voor de mbo-sector (nulmeting). Instellingen zullen gestimuleerd worden om de tool zelf in te vullen.

Wat kan ik met self-assessment, peer audit of een externe audit?

Beoordeling van het eigen informatiebeveiligingsbeleid kan op drie niveaus plaatsvinden, allereerst door een self-assessment, vervolgens door een peer audit waarbij collega mbo-instellingen elkaar beoordelen en ten slotte door een externe auditor.

Self-assessment

Voor een instelling is het self assessment een nulmeting met betrekking tot informatiebeveiliging in de eigen instelling. Daarbij is het niet noodzakelijk om ook echt, met procedures en protocollen, aan te tonen dat het niveau behaald is dat wordt beoogd. Bovengenoemde quick scan levert hier een hulpmiddel voor.

Peer audit

In een peer audit beoordelen instellingen elkaar met betrekking tot het niveau. Er worden peer-to-peer-kringen ingericht waarbij instelling A door instelling B wordt beoordeeld, vervolgens zal B weer door C worden beoordeeld, enz. De beoordelingen worden in de tool ingevuld, zodat een meer getrouw beeld van de sector ontstaat. Deze kringen zorgen voor een bewustwording bij de beoordeelde en bij de assessor. Het is dus niet alleen een beoordeling, maar is ook onderdeel van het leerproces binnen de mbo sector.

Externe Audits: de IT-audit als aanvulling op de onderwijsaudit. Wordt dit noodzakelijk voor een goedkeurende verklaring.
Wat is een IT-audit? Doel van de audit om aan te geven of een organisatie haar informatiebeveiliging op orde heeft.
Dit gebeurt aan de hand van acht vragen:

1. Wie is de **opdrachtgever**? Dit zou het College van Bestuur kunnen zijn.
2. Wat is de **scope**? Bijvoorbeeld KRD Eduarte.
3. Wat is de **diepgang**? Opzet, bestaan of werking.
4. Welke **periode** vindt het onderzoek plaats? Bijvoorbeeld september t/m december 2014.
5. Welke **kwaliteitsnormen** worden gehanteerd? Beschikbaarheid, integriteit, vertrouwelijkheid, controleerbaarheid, efficiency en effectiviteit.
6. Welke **audit**-standaard wordt gehanteerd? Verwezen wordt naar de vakvereniging NOREA.
7. Welk internationaal **normenkader** wordt gehanteerd? Bijvoorbeeld ISO 27002.
8. Welke **assurance** wordt afgegeven? Goedkeurend, afkeurend of met een beperking.

Een IT-auditor mag een dergelijke verklaring verstrekken. Net als een advocaat of arts kent NOREA ook een tuchtrecht. Een onterechte verklaring kan leiden tot sanctionering van de IT-auditor.

Externe audit

Het is de bedoeling om, net als in het hoger onderwijs, het peer audit af te wisselen met externe audits. Dat betekent dat aan een externe partij wordt gevraagd om een audit uit te voeren. Om dit te reguleren en te zorgen dat deze audits op vergelijkbare manier plaatsvinden zal een gezamenlijke aanbesteding plaatsvinden voor de instellingen in het mbo. Daarnaast kan het ook een voordeel opleveren in de kosten voor de instellingen zelf.

Zo!

Samenvatting

In deze Hoe? Zo!-uitgave staat het informatiebeveiligingsbeleid in het mbo centraal.

De uitgave steekt eerst in op de risico's, dat is toch de belangrijkste trigger om hiermee aan de slag te gaan. Zonder overdrijving of bangmakerij wordt er een aantal op een rij gezet en wordt de conclusie getrokken dat een gedegen en gestructureerde aanpak van de informatiebeveiliging in het mbo van belang is. Tegelijk zitten bestuurders en managers met veel vragen over hoe je dat dan aanpakt.

Daar gaat de publicatie dan ook uitvoerig op in. En dat gebeurt langs een logische opbouw:

- Allereerst kijken we naar de kaders en normen; met welke wet- en regelgeving we van doen hebben en welke normen er kunnen worden gehanteerd. En welke afspraken maken we hier dan over, welk normen- en toetsingskader gaan we hanteren?

- Vervolgens komt de vraag aan de orde hoe je aan die normen kunt gaan voldoen. Wat moet je allemaal hiervoor organiseren, welke stappen kun je daarbij volgen?

- Als je dat dan hebt gedaan, kun je dat dan ook aantonen, laten zien en zelfs bewijzen dat je organisatie aan die normenkaders voldoet: assessments en audits helpen daartoe.

- Tot slot, wat kun je hierbij van anderen, van de ondersteuningsorganisaties in het mbo zoals saMBO-ICT, Kennisnet en SURF, verwachten en op welke wijze kan het mbo veld optimaal samenwerken om dit complexe onderwerp effectief en efficiënt aan te pakken? Gelukkig hoeven we niet bij nul te beginnen. SURF heeft in het hoger onderwijs al veel expertise opgebouwd en het mbo kan daar op een goede manier haar voordeel mee doen.

Kortom, informatiebeveiliging is een enorme klus die de sector in gezamenlijkheid voortvarend moet en kan oppakken zodat we uiteindelijk kunnen terugkijken op een succesvol geïmplementeerd en werkend beleid.

Bronnenlijst

Volgnummer	Titel	Publicatiegegevens
1	Nederlandse code voor goed openbaar bestuur (beginselen van deugdelijk overheidsbestuur)	December 2009, Rijksoverheid
2	NEN-ISO/IEC 27002 Informatietechnologie – Beveiligingstechnieken – Code voor informatiebeveiliging	November 2007
3	Checklist Privacy-afspraken voor scholen	April 2014, Kennisnet
4	Informatiemap Aan de slag met Cloudcomputing	Januari 2013, SURFnet/Kennisnet innovatieprogramma
5	Nederlandse code voor goed openbaar bestuur (beginselen van deugdelijk overheidsbestuur)	December 2009, Rijksoverheid
6	A practical guide to risk assessment	December 2008, PWC
7	Certificeringsschema Edukoppeling en Cloud	Juni 2014, versie 1.1 (concept), SION/Kennisnet
8	International Standard ISO/IEC 27001	2005
9	Cloud security, checklist en de te stellen vragen	December 2010, SURFnet BV
10	Informatiebeveiliging in het Hoger Onderwijs	April 2010, Gezamenlijk product van het CIO Beraad en SURF-ibo
11	Informatiebeveiliging in het Hoger Onderwijs nog niet Volwassen	Juni 2009, SURFfoundation en SURFnet
12	Eindrapport Stimulering beveiliging	December 2009, versie 1.0, SURFnet BV
13	Starterkit Informatiebeveiliging	December 2010, SURFfoundation
14	Inrichtingsvoorstel SURFaudit	April 2011, versie 1.2, Alf Moens
	Starterkit Identity Management	April 2011, versie 1.0, SURFnet BV
	SURFaudit, getoetst in de praktijk Verslag auditronde 2011	Februari 2012, Alf Moens, SURFfoundation
	Leidraad Classificatie van Informatie en Informatiesystemen	Juli 2010, SURFibo
	Modelvragenlijsten voor de Classificatie van Informatie en Informatiesystemen	Juli 2010, SURFibo

Meer informatie?

Alle publieke bronnen worden verzameld op een IBB site bij Kennisnet. Daar wordt ook de voortgang van het project IBB in het mbo bijgehouden.

www.kennisnet.nl/themas/informatiemanagement/informatiebeveiliging/

Kennisnet

Ict heeft een grote invloed op de maatschappij en daarmee op ons dagelijks leven. Het onderwijs is de voorbereiding op de maatschappij en deze veranderingen raken vanzelfsprekend ook het onderwijs. Kennisnet is de expert en ict-partner voor het onderwijs bij het efficiënt en effectief inzetten van ict. Met onze kennis, diensten en experimenten ondersteunen wij het onderwijs de kwaliteit van het leren te verhogen, de doelmatigheid van het onderwijs te versterken en de transparantie te optimaliseren.

saMBO-ICT

SaMBO-ICT is een zelfstandige organisatie van en voor alle mbo-instellingen en heeft sterke banden met de MBO Raad en met Kennisnet. Belangrijke pijlers zijn belangenbehartiging, kennis-delingen projecten. saMBO-ICT houdt zich bezig met een breed aantal onderwerpen op het gebied van ict en informatievoorziening. Er wordt daarbij gebruik gemaakt van de kennis en energie die binnen de mbo-organisaties aanwezig zijn. Zoveel mogelijk worden instellingen zelf in staat gesteld om gezamenlijke activiteiten vorm te geven en saMBO-ICT zorgt daarbij voor praktische ondersteuning.

SURF

SURF-holding initieert en financiert innovatieactiviteiten. De dienstverlening van SURF is belegd bij de werkmaatschappijen SURFnet bv, SURFmarket bv, SURFsara bv en SURFshare bv. De bestuurlijke organisatie van SURF maakt het mogelijk de diensten van de werkmaatschappijen zonder aanbesteding aan te bieden aan de instellingen die bij SURF zijn aangesloten. In 2014 heeft de mbo-sector zich ook aangesloten bij SURF.

Colofon

Met dank aan: Andre Wessels (ROC van Twente), Caspar Schutte (ROC Midden Nederland), Fung Yee Poon (Aventus), Erik van Gennip, Ismail Emekli, Sharmain Davelaar (ROC Mondriaan), Edward Schilder (Regio College), Jan Bartling (saMBO-ICT), Alf Moens, Sir Bakx (SURF), Job Vos, Mariette Siemons (Kennisnet).
Auteurs: Ludo Cuijpers (Expert Informatiebeveiliging, Leeuwenborgh), Leo Bakker (Kennisnet)
Eindredactie: Kennisnet, Zoetermeer, saMBO-ICT, Woerden
Vormgeving: Tappan Communicatie, Den Haag
Druk: OBT bv, Den Haag

September 2014

Eerder verschenen in deze reeks:
- Laptops in het MBO Hoe? Zo!
- Digiborden in het mbo. Hoe? Zo!
- Open leermateriaal in het mbo. Hoe? Zo!
- Open standaarden en open source software in het mbo. Hoe? Zo!
- Centraal ontwikkelde examens Nederlandse taal en rekenen. Hoe? Zo! 2.0
- Informatiemanagement in het mbo. Hoe? Zo!
- CRM in het MBO. Hoe? Zo!
- Triple A. Hoe? Zo!
- Sociale media in het mbo. Hoe? Zo!
- Sturen op ICT projecten, Hoe? Zo!
- BYOD, Hoe? Zo!
- ICT en recht, Hoe? Zo!
- Leermiddelenbeleid, Hoe?Zo!
- Documentmanagement, Hoe?Zo!

Deze publicaties zijn te bestellen en te downloaden
via **kennisnet.nl/sectoren/mbo/publicaties/hoezo**

Stichting Kennisnet

Paletsingel 32
2718 NT Zoetermeer

Postbus 778
2700 AT Zoetermeer

T 0800 - 32 12 233
E info@kennisnet.nl
I kennisnet.nl