Programma Informatie-beveiliging 2015

saMBO-ICT Kennisnet

TASKFORCE MBO INFORMATIEBEVEILIGING

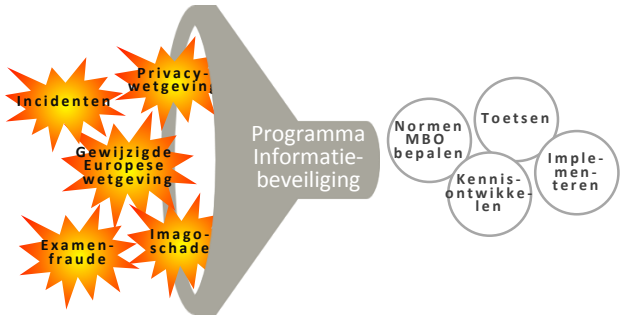
Programma Informatie-beveiliging?

Waarom een programma informatiebeveiliging?

Het doel van het programma informatiebeveiliging is het stimuleren en ondersteunen van instellingen bij het ontwikkelen en uitvoeren van informatiebeveiligingsbeleid. Informatiebeveiliging is voor het mbo een belangrijk thema geworden. Het belang ervan wordt door Europese regelgeving onderstreept en ook door een serie incidenten aangetoond. Niet alleen maatschappelijk, maar ook vanuit de overheid wordt er richting de instellingen druk uitgeoefend om maatregelen te nemen. Er wordt bij veel instellingen ingezien dat er onverantwoorde risico's worden gelopen wanneer de informatiebeveiliging niet op orde is.

Vooropgesteld moet worden dat elke instelling afzonderlijk maatregelen moet nemen. We kunnen gezamenlijk echter veel doen om dit te ondersteunen en doen dit door in te zetten op kennisontwikkeling, bewustwording, ondersteuningsproducten en –activiteiten, zoals:

- het vaststellen van normen (wanneer is het op orde?)
- het toetsen van die normen (hebben we het op orde?)
- het nemen van maatregelen (hoe pak je het aan?)
- het opdoen van kennis (wat moet je weten?)



In het actieplan Informatiebeveiligingsbeleid zijn de activiteiten benoemd die al gerealiseerd zijn of in de komende periode worden gerealiseerd. Het actieplan wordt komend cursusjaar uitgevoerd onder leiding van de Taskforce Informatiebeveiligingsbeleid. Deze taskforce werkt daarbij intensief samen met zowel Kennisnet als Surf.
Een korte impressie van het actieplan en de daarbij behorende activiteiten staan per werkgroep in deze folder beschreven. Zie voor het volledige plan de programmapagina op de saMBO-ICT-website of de themapagina van Kennisnet.

Werkgroep 1 Normenkader mbo

Aan welke normen moet het informatiebeveiligingsbeleid in het mbo voldoen?

Naast het hebben van een informatiebeveiligingsbeleid is het belangrijk om te weten wanneer het beleid afdoende is, dus aan welke normen het beleid moet voldoen. Hiertoe ontwikkelt de werkgroep een normenkader informatiebeveiligingsbeleid voor het mbo. Dit normenkader wordt gebaseerd op het normenkader vanuit het ho (hoger onderwijs) dat naar het mbo wordt vertaald. In de uitwerking van het normenkader worden de maatregelen aangegeven om alle risico's rond informatiebeveiliging het hoofd te kunnen bieden en bovendien wordt aangegeven hoe dit kan worden getoetst. Het bevat normen met betrekking tot:

- Beleid en organisatie
- Personeel en studenten
- Ruimten en apparatuur
- Continuïteit
- Toegangsbeveiliging en integriteit
- Controle en logging

Naast de normen wordt –in een vijfpuntsschaal– ook per niveau beschreven hoe hieraan kan worden voldaan . Er wordt zowel een minimum als een streefniveau aangegeven.
Het normenkader wordt door de sector en het ministerie van OCW gezamenlijk vastgesteld.

Speciale aandacht voor informatiebeveiliging Examinering

Naast het normenkader mbo wordt speciale aandacht besteed aan de informatiebeveiliging van de examinering. Hiervoor wordt een toetsingskader opgeleverd die op de Triple A-architecturen en de procesarchitectuur examinering is gebaseerd.

Producten Werkgroep 1 Normenkader MBO

1. Normenkader MBO (januari 2015)
2. Toetsingskader Informatiebeveiliging Examinering (maart 2015)

Werkgroep 2 Assessment & Benchmark

Voldoet ons informatiebeveiligingsbeleid aan de normen?

Meten is weten. In werkgroep 2 wordt gewerkt aan methodieken om ook daadwerkelijk te kunnen meten of aan het toetsingskader IBB MBO wordt voldaan.

Hoe stel je dit vast?

Een instelling bepaalt zelf met welke methode wordt vastgesteld of -en in welke mate- de informatiebeveiliging voldoet aan het normenkader**.** Het programma Informatiebeveiliging faciliteert hiertoe verschillende mogelijkheden, namelijk:

- **Zelf-assessment**
- **Peer-to-peer audit**
- **Externe IT-Audit**

Ten behoeve van een **zelf-assessment** wordt een tool (QuickScan) ontwikkeld waarmee instellingen hun eigen maatregelen kunnen toetsen en vervolgens de resultaten kunnen vergelijken met andere mbo-instellingen (benchmark).

Er kan ook worden gekozen voor een zogenaamde **peer-to-peer-audit** waarbij het programma instellingen die hiervoor kiezen bij elkaar brengt, de assessoren traint en de audits organiseert. De voorbereiding hiervan start in 2015. De audits vinden in 2016 plaats.

Daarnaast of daarbovenop kan worden gekozen voor een **externe IT-Audit**. Het programma zorg voor een gezamenlijke aanbesteding hiervan middels een programma van eisen, aanbestedingsdocumenten en een aanbod aan de instellingen. Instellingen maken zelf de keuze of men hier gebruik van wil maken.

Producten Werkgroep 2 Assessment & Benchmark

1. Zelf-assessment tool (maart 2015)
2. Benchmark MBO (eind 2015)
3. Peer-to-Peer Audit (2016)
4. Aanbesteding externe IT-Audit (eind 2015)

Werkgroep 3 Beleid & Organisatie

Hoe ga ik binnen mijn instelling aan de slag met informatiebeveiliging?

Om scholen behulpzaam te zijn bij het opstellen van een informatiebeveiligingsbeleid en dit ook daadwerkelijk te implementeren, wordt door de werkgroep Beleid & Organisatie een aantal producten opgeleverd. Het eerste product, een Hoe?Zo!-uitgave over informatiebeveilgingsbeleid, is al verschenen. Dit boekje kan behulpzaam zijn bij het creëren van bewustwording en geeft antwoord op allerhande vragen die een onderwijsmanager rondom dit thema kan (zou moeten!) hebben. Daarnaast wordt een format voor informatiebeveiligingsbeleid opgeleverd en een generiek stappenplan/roadmap ten behoeve van implementatie binnen een school.

Producten Werkgroep 3 Beleid en Organisatie

1. Informatiebeveilgingsbeleid in het MBO, Hoe?Zo!
2. Format Informatiebeveiligingsbeleid (maart 2015)
3. Stappenplan Implementatie (januari 2015)
4. Roadmap MBO (verbeterd stappenplan) (juni 2015)

Werkgroep 4 Kennis-ontwikkeling

Hoe krijg en houd ik de kennis binnen mijn school op peil?

De werkgroep kennisontwikkeling heeft voor 2015 'actieve masterclasses' opgezet. Deze masterclasses bestaan uit een training van 5 dagen waarin alle aspecten van Informatiebeveiligingsbeleid binnen het mbo aan de orde komen. Tijdens de training wordt er direct gewerkt aan een concrete invulling van dit beleid voor de eigen instelling. Om de kennis vervolgens op peil te houden wordt een platform voor kennisdeling opgericht. Ook wordt aangehaakt bij de in het Hoger Onderwijs bestaande structuren zoals SURFibo, SURFaudit en SURFcert.

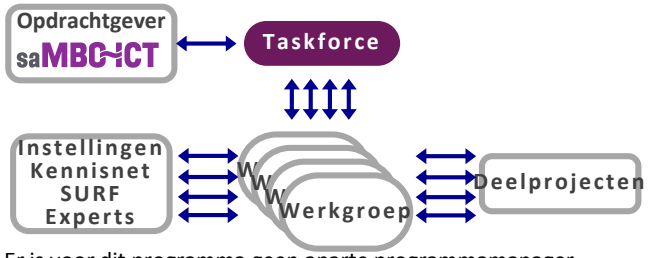
Programma Masterclass IBB	
Dag 1	Inleiding in de IBB documenten van SURF
Dag 2	Risicomanagement
Dag 3	Theorie IBB en IT-auditing
Dag 4	Toelichting en toepassing SURF-audit
Dag 5	Onderlinge presentaties IBB eigen instelling

Producten Werkgroep 4 Kennisontwikkeling

1. Masterclasses IBB-1/IBB-2 (maart 2015/juni 2015, vol)
2. Masterclass IBB-3 (in voorbereiding)
3. Platform IBB (maart 2015)

Aansturing, Afstemming en samenwerking

Het programma Informatiebeveiliging wordt als volgt aangestuurd:



Er is voor dit programma geen aparte programmamanager aangesteld; de coördinatoren van de werkgroepen stemmen onderling af en leggen verantwoording af aan de Taskforce.

Samenwerking?

Zoals eerder al gesteld, zijn instellingen zelf verantwoordelijk voor het informatiebeveiligingsbeleid**.** Door echter gezamenlijk in te zetten op kennisontwikkeling, bewustwording, ondersteuningsproducten en –activiteiten kunnen we elkaar hierbij enorm helpen. **Kortom: Samen *slim* & Slim *samen*.**

...daar wil ik meer van weten!

Verder lezen en nadere informatie

Op de website van saMBO-ICT maar vooral op die van Kennisnet is meer informatie beschikbaar over het programma Informatiebeveiliging.
Scan de QR-code of ga naar:
www.kennisnet.nl/themas/informatiemanagement/informatiebeveiliging/

Download ook het Hoe?Zo!-boekje over Informatiebeveiligingsbeleid in het mbo.

contactgegevens
saMBO-ICT
Houttuinlaan 6
3447 GM Woerden
Telefoon +31 (0) 348-753500
Email: info@sambo-ict.nl
www.sambo-ict.nl