Convenant cyberveiligheid mbo (met toelichting)

Versie: 1.3, 14-06-2023

Aangezien het beperken van cyberrisico's, naast de eigen verantwoordelijkheid van de onderwijsinstelling, ook een sectorbrede verantwoordelijkheid is, willen de leden van de MBO Raad in dit Convenant Cyberveiligheid afspraken maken op dit gebied.

Overwegende dat:

- een betrouwbare IT-omgeving een randvoorwaarde is voor goed onderwijs;
- de dreigingen op het gebied van cybercriminaliteit toenemen;
- de weerbaarheid tegen deze aanvallen voor individuele instellingen een steeds grotere opgave wordt;
- we op dit gebied als mbo-sector willen samenwerken;

maken de leden de volgende afspraken met elkaar met betrekking tot cyberveiligheid in het mbo.

Uitgangspunten

1. We geven niet toe aan afpersing en betalen niet aan criminelen.
2. Om invulling te kunnen geven aan dit uitgangspunt werken we samen op het gebied van cyberveiligheid om:
   A. de cyberrisico's te beheersen;
   B. de impact van eventuele cyberincidenten te beperken.
3. We verbinden ons aan de uitgangspunten en afspraken in dit convenant en spreken elkaar aan op naleving. We hanteren daarbij het principe van 'pas toe of leg uit'.

A. Samenwerken aan het beheersen van cyberrisico's

4. We standaardiseren als basis voor samenwerken: we hanteren een modelaanpak op het gebied van IBP (Informatiebeveiliging en Privacy).
5. We maken gebruik van een sectorbrede applicatie voor het bijhouden van risico's, maatregelen en volwassenheid op het gebied van IBP.
6. Voor onze normen/toetsingskaders op het gebied van IBP sluiten wij aan bij de standaarden die in samenwerking met universiteiten en hogescholen in SURF-verband worden gehanteerd.
7. We stellen mbo-breed het gemiddelde streefniveau vast voor onze volwassenheid op het gebied van IBP. Dit gemiddelde niveau van volwassenheid is de norm voor alle mbo-instellingen.
8. We nemen deel aan de sectorbrede benchmarks op het gebied van IBP en werken mee aan de validatie en vaststelling van onze volwassenheidsscores.
9. We hanteren standaard formats voor onze verantwoording op het gebied van IBP.
10. We werken samen aan sectorbrede mitigerende maatregelen op het gebied van cyberveiligheid.
11. We werken samen op het gebied van leveranciersmanagement voor mbo-breed gebruikte cloud-toepassingen.

B. Beperken van de impact van cyberincidenten

12. We delen relevante informatie tijdens een cybercrisis met SURFcert.
13. We bieden elkaar uitwijkopties in tijden van crisis.
14. We delen de geleerde lessen na een cybercrisis.
15. We nemen deel aan een collectieve voorziening om de eventuele schade te herstellen.

C. Implementatie en evaluatie

16. De uitvoering van deze afspraken op het gebied van cyberveiligheid wordt afgestemd binnen de netwerken van MBO Digitaal. Wanneer over dergelijke uitvoeringsafspraken geen consensus kan worden bereikt, worden deze ter besluitvorming voorgelegd aan de leden.
17. De looptijd van dit convenant komt overeen met de looptijd van het Programma Cyberveiligheid mbo: tot 01-10-2027. Ruim voor het verstrijken van deze einddatum wordt bij voldoende draagvlak een nieuwe versie of een verlenging van dit convenant aan de leden voorgelegd.
18. De Kerngroep MBO Digitaal evalueert de werking van het convenant ten minste jaarlijks en geeft opdracht om eventuele verbeterpunten die uit deze evaluatie voortvloeien te implementeren.
19. Nadere afspraken die worden gemaakt naar aanleiding van de in het vorige artikel bedoelde evaluatie worden geacht deel uit te maken van het convenant.

Door ons te committeren aan deze mbo-brede uitgangspunten kunnen we efficiënt samenwerken, samen investeren in maatregelen en gezamenlijk rekenschap afleggen aan de maatschappij.

Toelichting Convenant cyberveiligheid mbo

Versie: 1.3, 14-06-2023

1. Door dit uitgangspunt actief uit te dragen geven wij een duidelijk signaal af naar criminelen. Om dit waar te kunnen maken zetten we samen in op maatregelen waarmee we zoveel mogelijk voorkomen dat we in een situatie terechtkomen waarbij we gedwongen zijn om te betalen.
2. De samenwerking ziet op diverse aspecten van cybersecurity:
   - Identificeren van risico's
   - Beschermen tegen aanvallen
   - Detectie van aanvallen
   - Reageren op incidenten
   - Herstellen van de schade
   - Leveranciersmanagement
3. De afspraken in dit convenant zijn bindend en we zien met elkaar op toe op naleving. Tegelijkertijd heeft elk lid een eigen verantwoordelijkheid op het gebied van cyberveiligheid. Waar uitgangspunten botsen, maken de leden een eigen onderbouwde afweging op basis van het principe 'pas toe of leg uit'.
4. Onze gemeenschappelijke aanpak is gebaseerd op het *NBA-volwassenheidsmodel voor informatiebeveiliging*. Binnen dat model werken we modeldocumenten en good-practices uit. Door op deze manier te standaardiseren kunnen we beter samenwerken, informatie delen en van elkaar leren.
5. De GRC-applicatie (governance-risk-compliance) is beschikbaar vanaf 2024 en wordt gebruikt om in een beveiligde omgeving de risico's, de maatregelen en de volwassenheid op het gebied van IBP binnen de organisatie te beheren en eenvoudig gegevens te kunnen aanleveren ten behoeve van benchmarks. Het gaat daarbij om:
   a. Het registreren en documenteren van de actuele- en de streefvolwassenheid binnen de instelling, als stuurinstrument voor de instellings-roadmap IBP;
   b. Het regelmatig aanleveren van (geanonimiseerde) volwassenheidscores via een export/systeemkoppeling, ten behoeve van voortgangsmetingen in het kader van van het Programma Cyberveiligheid mbo;
   c. Jaarlijkse sectorbrede benchmarks op het gebied van IB en P;
   d. Het kunnen verlenen van externe toegang voor (peer)reviews en externe audits.

   Voor deze compliance-gebaseerde werkwijze wordt door de leverancier een scenario ingericht dat laagdrempelig bruikbaar is voor (kleine) instellingen die geen behoefte hebben geavanceerde mogelijkheden. Doorgroeien naar meer risico-gebaseerd werken is als vervolgstap eenvoudig mogelijk.
6. In het mbo wordt, evenals in het hoger onderwijs, gebruikgemaakt van het *NBA-volwassenheidsmodel voor informatiebeveiliging* als toetsingskader (door SURF genoemd het *SURFaudit toetsingskader informatiebeveiliging*). Voor het onderdeel privacy wordt in SURF-verband een toetsingskader geselecteerd en voor de onderwijscontext aangepast, gebaseerd op het AVG-borgingsproduct van de VNG.
7. Uit de nulmeting die eind 2022 is uitgevoerd, komt naar voren dat de mbo-instellingen verwachten dat ze eind 2023 een gemiddeld volwassenheidsniveau van 2,8 hebben bereikt. Het ministerie van OCW hanteert als streefwaarde een gemiddeld volwassenheidsniveau van 3,0 voor elke mbo-instelling. We stellen eind 2023 mbo-breed het tijdpad voor onze volwassenheid op het gebied van IB en P vast.

8. Alle mbo-instellingen nemen deel aan de jaarlijkse benchmarks op het gebied van Informatiebeveiliging en Privacy en leveren hun gegevens tijdig aan voor de centrale verwerking. Daarnaast leggen de instellingen verantwoording af over de kwaliteit van deze zelfassessments via de binnen de mbo-sector gehanteerde methodiek: via peerreview, externe vaststelling of externe audit. Een en ander conform het auditplan dat we mbo-breed met elkaar afspreken.
9. We hanteren standaard formats voor onze (externe) verantwoording op het gebied van IBP, waarbij een afweging wordt gemaakt tussen openheid en veiligheid. We stemmen dit overkoepelend af met de VH en de UNL. Het gaat hierbij om een format per instelling (ten behoeve van het jaarverslag bijvoorbeeld) en een sectorbreed format, ten behoeve van het sectorbeeld naar externe stakeholders zoals het ministerie van OCW.
10. We werken samen bij het onderzoeken en beschikbaar maken van mitigerende maatregelen, bijvoorbeeld op het gebied van awareness, organisatorische maatregelen en technische weerbaarheid. Projectactiviteiten op het gebied van technische weerbaarheid voeren we uit in nauwe samenwerking met SURF, via de Innovatiezone Cyberveiligheid. De meer structurele technische ondersteuning organiseren we samen met SURF in het Security Expertise Centrum.
11. We werken samen richting onze cloudleveranciers, onder andere door gezamenlijk de verwerkersovereenkomsten te beoordelen en gezamenlijk DPIA's, pentests en audits op deze applicaties uit te voeren.
12. We delen -zodra dat mogelijk is- relevante informatie tijdens een cybercrisis met SURFcert. Het gaat daarbij niet alleen om de IoC's (indicators of compromise) maar ook de IoA's (indicators of attack). Door via SURFcert te delen kan efficiënt worden uitgewisseld waarbij de vertrouwelijkheid is geborgd via TLP-afspraken (traffic light protocol: red, amber, green).
13. Als bij een instelling door een cyberincident de continuïteit in gevaar komt, helpen we elkaar om te zorgen dat het onderwijsproces zoveel mogelijk kan doorgaan. Dat kan bijvoorbeeld door elkaar faciliteiten te bieden of expertise beschikbaar te stellen.
14. Na afloop van een cybercrisis delen we de geleerde lessen via o.a. de netwerken van MBO Digitaal. Goede voorbeelden zijn de terugkoppeling vanuit de Universiteit van Maastricht en ROC Mondriaan, waarna de sector diverse maatregelen heeft getroffen om herhaling te voorkomen.
15. We onderzoeken de mogelijkheden voor een collectieve cyberverzekering of waarborgfonds, met voor iedere instelling passende en haalbare voorwaarden. Voor de toelating tot een dergelijke voorziening speelt ons NBA-toetsingskader voor informatiebeveiliging een belangrijke rol.
16. De verdere uitwerking en uitvoering van deze afspraken vindt plaats binnen de netwerken van MBO Digitaal, bijvoorbeeld de netwerken IBP, IM en het netwerk van SURF contactpersonen (CSC's). Besluitvorming over onderwerpen waarvoor het mandaat onvoldoende is, of waarover geen overeenstemming kan worden bereikt, worden aan de leden voorgelegd, bijvoorbeeld bij een regiobijeenkomst of via de ALV.
17. Geen toelichting
18. Geen toelichting
19. Geen toelichting