Inspectie van het Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

Contactpersoon
Ellen Jagtman en Bert Jaap van Oel

Onze referentie
Datum
21 mei 2021

Kopie aan

memo

presentatie Cyberveiligheid

We gaan graag met U in gesprek over het thema cyberveiligheid. Dat doen we aan de hand van de ervaring en kennis die we hebben opgedaan gedurende het instellingsonderzoek Universiteit Maastricht (eerste helft 2020) en het huidige stelselonderzoek in het HO. Als onderdeel van het stelselonderzoek zijn we met veel partijen in gesprek: uiteraard met bestuurders en It-ers binnen instellingen, met de koepels en met OCW maar ook met partijen als het NCSC, Surf, de inspectieraad en bijvoorbeeld het agentschap telecom. Met ons stelselonderzoek willen een bijdrage leveren aan de cyberweerbaarheid van het hoger onderwijs. Alle gesprekken en analyses tezamen vormen de input voor een inspectiepublicatie over cyberveiligheid in het HO (publicatie volgt in de loop van 2021).

In de die publicatie en in de presentatie staan de BIO-standaarden (zie bijlage) centraal. We tonen voor elk van die standaarden voorbeelden en dilemma's uit het lopende onderzoek op drie niveaus: de onderwijsinstelling, het stelsel (in bijzonder HO) en het (interne en externe) toezicht.

De volgende onderwerpen passeren daarbij de revue:

- Kaders en aanleiding voor ons onderzoek;
- Netwerkanalyse: partijen die zich bezig houden met (toezicht op) cyberveiligheid;
- Het risicoprofiel voor het (hoger) onderwijs als geheel en van de afzonderlijke instellingen;
- De aandacht voor cyberdreigingen als onderdeel van de interne kwaliteitszorg en van het interne en externe toezicht;
- De kennis en kunde die nodig is om risico's te identificeren en op waarde te kunnen schatten.

Bijlage: BIO-standaarden

De volgende onderwerpen zijn afgeleid van de BIO – Baseline Informatiebeveiliging Overheid – richtlijnen. Het gaat om standaarden ten behoeve van de bestuurstafel (https://bio-overheid.nl/media/1355/bio-leaflet-voor-bestuurders.pdf).

Vergroten bewustzijn (standaard 1): Bestuurders agenderen tijdens overleggen met regelmaat het belang van informatiebeveiliging. Er bestaan bewustwordingsmaatregelen onder studenten, onderzoekers, docenten en medewerkers die met regelmaat worden ingezet.

Veilige en open cultuur (standaard 2): Informatiebeveiliging is in essentie risicomanagement wat begint bij identificatie. Het bestuur bevordert een open en veilige cultuur waarin medewerkers zich vrij voelen om (potentiële) risico's te melden bij de juiste persoon.

Inrichten risicoteam (standaard 3): Maak gebruik van de kennis en verantwoordelijkheden van proces- en systeemeigenaren. Er is samenwerking tussen een risicoteam door de Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Controller. Deze systeemeigenaren functioneren tevens als onafhankelijk adviseur voor het bestuur.

Borging risicomanagement (standaard 4): Risicomanagement is een cyclisch, iteratief en terugkerend proces: dreigingen, omgeving en wetgeving veranderen. Er wordt rekening gehouden met deze veranderingen zodat maatregelen doeltreffend en doelmatig zijn.

Ketensamenwerking (standaard 5): Partners en leveranciers kunnen op afhankelijke wijze aantonen dat deze partijen aan de geldende eisen voldoen.

Controleren en evalueren (standaard 6): Regelmatige controle en evaluatie zijn belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie (e.g., regelmaat, rapportages).

Investeren in informatiebeveiliging (standaard 7): Er worden voldoende middelen beschikbaar gesteld om de onderkende risico's op een adequate manier te behandelen.