Inspectie van het Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

Binnen zonder kloppen

Cyberveiligheid in het onderwijs

Inleiding

Steeds vaker vinden cybergerelateerde incidenten plaats, zo ook in het onderwijs. Eind 2019 was er veel media-aandacht voor de Universiteit Maastricht die door een ransomware-aanval werd getroffen.[1] Deze aanval bracht de voortgang van het onderwijs en onderzoek bij de Universiteit Maastricht tijdelijk in gevaar. Maar ook (kleinere) instellingen in het primair onderwijs (po), voortgezet onderwijs (vo), speciaal onderwijs (so) en middelbaar beroepsonderwijs (mbo) zijn reeds slachtoffer geworden van een cyberaanval.
Bij de Universiteit Maastricht waren de gevolgen destijds zo groot, dat de Inspectie van het Onderwijs (inspectie) besloot om de cyberweerbaarheid van het hoger onderwijs in het algemeen te onderzoeken. Uitgebreide informatie over dit stelselonderzoek vindt u in het volledige rapport: Binnen zonder kloppen - Digitale weerbaarheid in het hoger onderwijs.

Dit document is een samenvatting van de belangrijkste bevindingen van het rapport 'Binnen zonder kloppen' inclusief enkele aanvullingen. Deze samenvatting is gericht op bestuurders uit alle onderwijssectoren, immers alle onderwijsinstellingen ongeacht sector en schaalgrootte lopen risico. Met deze samenvatting willen wij bestuurders van alle onderwijsinstellingen en uit alle onderwijssectoren op een laagdrempelige manier informeren en hen daarmee prikkelen om tot actie over te gaan.

Als bestuurder bent u allereerst zelf verantwoordelijk voor uw (cyber)incidentmanagement.[2] Bestuurders moeten zorgen voor de continuïteit van het onderwijs tijdens digitale verstoringen en voor de adequate beveiliging van de persoonsgegevens van onderwijsdeelnemers, ouders, medewerkers en andere betrokkenen. Onderwijsinstellingen moeten echter wel in staat zijn om dit ook daadwerkelijk zelf te regelen. Toenemende digitalisering brengt nieuwe uitdagingen met zich mee die het noodzakelijk maken om bepaalde onderdelen centraal, dus op stelselniveau, te faciliteren of in te regelen.[3] Het verschil tussen instellingsniveau en stelselniveau komt ook structureel terug in deze samenvatting.

Inhoud

Inleiding	1
Standaard 1: vergroten bewustzijn	3
Standaard 2: veilige en open cultuur	5
Standaard 3: inrichten risicoteam	6
Standaard 4: borgen risicomanagement	8
Standaard 5: aandacht ketensamenwerking	10
Standaard 6: controleren en evalueren	12
Standaard 7: geld investeren in informatiebeveiliging	14
Aanbevelingen voor bestuurders op basis van de standaarden	15

[1] Zie: https://nos.nl/artikel/2316120-universiteit-maastricht-kampt-met-ransomware-aanval (geraadpleegd op 22 juli 2022).

[2] Zie; TK, 2021-2022, 35925-VIII-190, p 2.

[3] Ter illustratie: de overheid zal waar nodig het uitvoeren van Data Protection Impact Assessments (DPIA's) op digitale producten die in het onderwijs veel gebruikt worden faciliteren, zie hiervoor: TK, 2021-2022, 35925-VIII-190, p 2.

Op dit moment ontbreekt een wettelijk kader met specifieke handhavingsinstrumenten voor cyberveiligheid, daarom is terughoudendheid van de inspectie gepast.[4] Desondanks is het in bepaalde gevallen mogelijk dat bij cyberincidenten een rol is weggelegd voor de inspectie. Een belangrijke indicatie hiervoor is de (mogelijke) impact die een cyberincident heeft op het stelsel[5]. De minister is namelijk uiteindelijk verantwoordelijk voor het onderwijsstelsel en zal hierover de regie moeten nemen. Voorbeelden van die regie zijn: het agenderen van cyberveiligheid in het onderwijsveld, de realisatie van een gedeeld normenkader voor het onderwijs en het toegankelijk maken van informatie over actuele dreigingen voor onderwijsinstellingen. Zo is recent in de Kamer de toezegging gedaan om een gemeenschappelijk kader voor informatiebeveiliging in het onderwijs te ontwikkelen.[6] Daarnaast werkt Kennisnet met de PO-Raad en de VO-raad samen aan een normenkader voor het primair- en voortgezet onderwijs.[7] Als basis hiervoor gebruiken zij het normenkader hoger onderwijs van SURF.[8]

In dit document vindt u een samenvatting van de volgende standaarden uit het rapport 'Binnen zonder kloppen':[9]

1. Vergroten bewustzijn
2. Veilige en open cultuur
3. Inrichten risicoteam
4. Borgen risicomanagement
5. Aandacht ketensamenwerking
6. Controleren en evalueren
7. Geld investeren in informatiebeveiliging

Per standaard wordt er onderscheid gemaakt tussen instellingsniveau en stelselniveau.

Aan het eind van dit document vindt u een lijst met aanbevelingen. U als bestuurder wordt uitgenodigd om de aanbevelingen uit deze samenvatting mee te nemen en in te zetten voor uw eigen onderwijsinstelling én het stelsel.

Het is goed om te weten dat het Nationaal Cyber Security Centrum (NCSC)[10] 8 basismaatregelen opgesteld heeft voor cybersecurity, namelijk:

8. Zorg dat elke applicatie en elk systeem voldoende loginformatie genereert.
9. Pas multifactorauthenticatie toe waar nodig.
10. Bepaal wie toegang heeft tot uw data en diensten.
11. Segmenteer netwerken.
12. Versleutel opslagmedia met gevoelige bedrijfsinformatie.
13. Controleer welke apparaten en diensten bereikbaar zijn vanaf het internet en bescherm deze.
14. Maak regelmatig back-ups van uw systemen en test deze.
15. Installeer software-updates.

Wilt u meer weten? Bekijk een uitgebreide beschrijving per basismaatregel op de website van NCSC.

[4] De komende tijd verkent OCW hoe verantwoording en handhaving op digitale veiligheid in het onderwijsstelsel verder kunnen worden ingericht, zie: TK, 2021-2022, 35925-VIII-190, p 2.

[5] De inspectie kan binnen het huidige wettelijke kader wel in gesprek gaan met onderwijsinstellingen in geval van ernstige verstoringen van de continuïteit van het onderwijs. Maar de inspectie heeft momenteel geen aparte (handhavende) bevoegdheden op gebied van cyberveiligheid. Ook kan de inspectie een stimulerende rol vervullen richting het onderwijsveld. Dit doet de inspectie al met de oprichting van de werkgroep cyberveiligheid in het onderwijs. Zie: TK, 2021-2022, 35925-VIII-190, p. 3.

[6] Zie TK, 2021-2022, 35925-VIII-190, p 2-3.

[7] Zie: TK, 2021-2022, 35925-VIII-190, p 4. Zie ook het commissiedebat Digitalisering in het Onderwijs 1 december 2021 https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2021A07231(geraadpleegd op 12 juli 2022).

[8] SURF is een coöperatieve vereniging van zowel onderwijs- als onderzoeksinstellingen, waar de focus ligt op informatie- en communicatietechnologie. Voor meer informatie zie: https://www.surf.nl/over-surf (geraadpleegd op 26 april 2022). Voor het normenkader zie: https://www.surf.nl/normenkader-surfaudit-audit-je-informatiebeveiliging (geraadpleegd op 11 mei 2022).

[9] Deze standaarden zijn afkomstig uit het rapport Binnen zonder Kloppen – Digitale weerbaarheid in het Hoger Onderwijs. Zie Inspectie van het Onderwijs (2021) *Binnen zonder Kloppen, Digitale Cyberweerbaarheid in het Hoger Onderwijs* https://www.onderwijsinspectie.nl/documenten/themarapporten/2021/09/15/digitale-weerbaarheid-in-het-hoger-onderwijs (geraadpleegd 28 april 2022).

[10] Publiek-private samenwerking, onderdeel van het Ministerie van Justitie en Veiligheid dat zich richt op het creëren van een veilige, open en stabiele informatiesamenleving en het vergroten van de digitale weerbaarheid.

Standaard 1: vergroten bewustzijn

Wat betekent dit voor bestuurders?
Bestuurders agenderen tijdens overleggen met regelmaat het belang van informatiebeveiliging. Er bestaan bewustwordingsmaatregelen onder studenten, onderzoekers, docenten en medewerkers die met regelmaat worden ingezet.

Cyberveiligheid heeft een technische, maar ook een menselijke kant. Daardoor is cyberveiligheid niet alleen de verantwoordelijkheid van de ICT-afdeling, maar juist van iedereen in de organisatie. Instellingen zoeken daarom naar een balans tussen technische beveiliging (security by design) en het vergroten van het bewustzijn. U als bestuurder heeft een rol bij het stimuleren van veilig handelen van medewerkers, studenten en leerlingen. Deze standaard richt zich op de menselijke kant, bijvoorbeeld een sterk wachtwoord gebruiken en een phishing mail op tijd herkennen.

Onderwijsinstellingen zijn allereerst zelf verantwoordelijk voor hun cybersecuritybeleid en u als bestuurder speelt een grote rol bij het bewustwordingsproces van iedereen in de organisatie. U kunt de risico's verkleinen of incidenten voorkomen door het belang van informatiebeveiliging regelmatig te agenderen. Juist als het onderwerp cyberveiligheid nog onwennig is binnen uw organisatie, is dit extra belangrijk. Agendering draagt namelijk bij aan de bewustwording bij de gebruikers en dit kan leiden tot veiliger digitaal handelen. Daarbij is het belangrijk dat u als bestuurder zich realiseert dat u verantwoordelijk bent voor het stimuleren van goed gedrag van medewerkers. Ook is het belangrijk dat u beseft dat het kennisniveau van medewerkers sterk kan verschillen.

Niet alleen het risicoprofiel van de specifieke instelling is bepalend voor de keuze van een passende aanpak. Het is ook van belang dat met regelmaat de meest actuele en meest dreigende risico's in kaart worden gebracht, in de loop van de tijd kunnen risico's immers veranderen. Het is daarom belangrijk dat bestuurders proactief nadenken over de vraag: klopt mijn risicoprofiel nog wel? Daarnaast speelt ook de cultuur bij onderwijsinstellingen een rol. Denk bijvoorbeeld aan het belang van academische vrijheid. Pas op voor de suggestie dat academische vrijheid en vrijheid van onderwijs niet samen gaan met een veilig ICT-landschap. Dit hoeft niet met elkaar te conflicteren. Heeft een docent bijvoorbeeld behoefte aan afwijkende softwarepakketten of extra gebruikersrechten, dan is er ook een gesprek nodig over of dit daadwerkelijk noodzakelijk is en of er aanvullende cybersecuritymaatregelen gewenst zijn. Deze gesprekken kunnen een positieve bijdrage leveren aan de bewustwording.

Bestuurders kunnen het bewustzijn vergroten door aandacht te besteden aan[11]:

1. Basisinformatie en voorlichting
2. Awareness
3. Security by design
4. Laagdrempeligheid en veiligheid van meldingsprocedures[12]

Wees alert op activiteiten die stelselpartijen organiseren

Koepels en andere partijen uit het onderwijsveld organiseren regelmatig interessante activiteiten op het gebied van cyberveiligheid of digitalisering. Dit zijn bijeenkomsten voor bestuurders maar bijvoorbeeld ook voor informatiebeveiliging- of privacy specialisten binnen onderwijsinstellingen. Houd daarom bijvoorbeeld de agenda's van PO-Raad, VO-raad, MBO Digitaal, sectorraad GO en SURF in de gaten.

[11] Inspectie van het Onderwijs (2021) *Binnen zonder Kloppen, Digitale Cyberweerbaarheid in het Hoger Onderwijs*. Zie: https://www.onderwijsinspectie.nl/documenten/themarapporten/2021/09/15/digitale-weerbaarheid-in-het-hoger-onderwijs, p. 25-26 (geraadpleegd op 28 april 2022).

[12] In de toekomst zal gekeken worden of aan de in oprichting zijnde CERT voor het funderend onderwijs een meldplicht voor cyberincidenten kan worden gekoppeld. Zie: TK, 2021-2022, 35925-VIII-190, p 4.

Wat moet er op stelselniveau gebeuren?
Instellingen en alle belanghebbenden houden elkaar onderling scherp; men bespreekt interne en externe dreigingen. Er zijn landelijke bewustwordingscampagnes rondom veilig werken en cyberdreigingen.

Instellingen kunnen meedoen aan initiatieven die op stelselniveau worden georganiseerd, zoals de (sinds 2016) tweejaarlijkse gezamenlijke cyberoefening (OZON).[13]
De focus ligt niet enkel op deelname van ICT-ers, ook bestuurders kunnen deelnemen. Tijdens de oefening worden diverse aspecten van een cyberaanval gesimuleerd, waaronder: infecties in het instellingsnetwerk, (social) media-aandacht, contact met hackers, vragen van studenten en medewerkers en berichten van dienstenaanbieders.
Als deelnemer aan deze oefening is het doel voor instellingen om de toegebrachte schade te herstellen of de impact hiervan te beperken. SURF coördineert het opzetten, uitvoeren en evalueren van deze cyberoefening.

Ook worden er door stelselpartijen activiteiten georganiseerd specifiek voor bestuurders. Ondanks het toegenomen bewustzijn rond cyberweerbaarheid, is er nog geen structurele samenwerking op stelselniveau.[14]
Het oprichten van kenniscentra en het bevorderen van regionale samenwerking is wenselijk.

Stappenplan en campagne: maak er gebruik van!

Er zijn al allerlei initiatieven uit het onderwijsveld om het bewustzijn van onderwijsinstellingen rond cyberveiligheid te vergroten. Kennisnet heeft een stappenplan opgesteld om informatiebeveiliging en privacy goed te organiseren en SURF heeft de campagne Cybersave Yourself ontwikkeld, bestaande uit een website en een toolkit met kant en klaar materiaal. Schoolbesturen, maak hier gebruik van!

[13] Voor universiteiten, hogescholen, ziekenhuizen en onderzoeksinstellingen, zie ook standaard 3.

[14] OCW, SURF, het platform Integrale Veiligheid Hoger Onderwijs (IV-HO), Kennisnet, SIVON, MBO-digitaal etc. kunnen een aanjagende of ondersteunende rol vervullen. Waar partijen als de PO-Raad, VO-raad, MBO-Raad, Vereniging Hogescholen (VH) en de Universiteiten van Nederland (UNL) een verbindende rol kunnen vervullen.

Standaard 2: veilige en open cultuur

Wat betekent dit voor bestuurders?

Informatiebeveiliging is in essentie risicomanagement dat begint bij identificatie van risico's en incidenten. Het bestuur bevordert een open en veilige cultuur waarin medewerkers zich vrij voelen om (potentiële) risico's proactief te melden bij de juiste persoon.

Uit het onderzoekt blijkt dat de volgende zaken belangrijk zijn voor het stimuleren en borgen van een veilige en open cultuur:

a. Het gedrag van het bestuur is een voorbeeld voor anderen door bijvoorbeeld te laten zien dat fouten maken mag, maar ook door het gesprek aan te gaan over oplossingen.
b. Er is een zorgvuldige handelswijze richting melders vastgelegd en geborgd.
c. Het bestuur laat zien dat zij achter de procedure en mensen die de regels uitvoeren en naleven, staan.

Het is van belang dat informatie over ICT en cyberveiligheid en de contactgegevens van de helpdesk goed vindbaar zijn. Daarnaast moet op alle niveaus binnen de organisatie gewerkt worden aan het realiseren van een open en veilige cultuur. Er is een transparante, veilige meldprocedure nodig die bovenal laagdrempelig is. De mogelijke schaamte die mensen ervaren bij het doen van meldingen moet weggenomen of zo veel mogelijk ingeperkt worden. Door een meldprocedure zo in te richten, worden mensen gestimuleerd om incidenten en risico's uit eigen beweging te melden. Daarvoor is het cruciaal dat iedereen weet waar ze meldingen kunnen doen, ook moeten deze meldingen vervolgens op de juiste plek belanden. Meldingen moeten niet alleen gaan over datalekken, maar ook over veiligheid in de brede zin van het woord. Kortom, er moet een transparante en laagdrempelige meldprocedure zijn én medewerkers moeten geprikkeld worden om ook daadwerkelijk meldingen te doen.

Wat moet er op stelselniveau gebeuren?

Alle belanghebbenden stimuleren dat er een veilige en open cultuur is: meldingen kunnen in vertrouwen worden gedaan. Melders worden niet afgerekend op hun openheid. Het lerend vermogen van het stelsel staat voorop.

Net als op instellingsniveau, begint melden ook op stelselniveau bij gemakkelijk vindbare centrale contactgegevens. Er moet ruimte zijn om de risico's, de kwetsbaarheden en de incidenten onderling te delen en om van elkaar te leren. Zo heeft de open manier van communiceren bij de Universiteit Maastricht na de hack in 2019, het hele stelsel verder geholpen.[15] Niet-bekostigde hoger onderwijsinstellingen, ofwel rechtspersonen voor het onderwijs (rpho's), voelen zich vaak weinig tot niet verbonden met bekostigde instellingen en andere actoren in het onderwijsveld en missen toegang tot ondersteuning en informatie, wat een blinde vlek veroorzaakt. ICT'ers van bekostigde instellingen houden elkaar binnen SURF op de hoogte. Maar niet alle bekostigde instellingen zijn lid van SURF en geen enkele niet-bekostigde onderwijsinstelling is lid. Dit zorgt voor kwetsbaarheden op stelselniveau. Er is ook nauwelijks contact tussen de bekostigde en de niet-bekostigde instellingen. Momenteel is er nog geen eenduidig aanspreekpunt of stelselbreed meldpunt voor onveilige situaties. De verwachting is dat het bovenstaande niet enkel geldt voor hoger onderwijsinstellingen, maar dat deze problematiek speelt binnen alle onderwijssectoren, dus ook binnen het po, (v)so, vo en mbo. Funderend onderwijsinstellingen die bijvoorbeeld niet aangesloten zijn bij Kennisnet of Sivon, zullen naar waarschijnlijkheid niet op de hoogte zijn van de vraagstukken die spelen binnen het ministerie van Onderwijs, Cultuur en Wetenschap (OCW). Ook zullen zij mogelijkerwijs niet vertegenwoordigd zijn in gesprekken.

[15] Zie: https://www.surf.nl/wat-universiteit-maastricht-leerde-van-de-ransomwareaanval-deel-1 (geraadpleegd op 29 april 2022).

Er zijn veel verschillende besturen die verantwoordelijk zijn voor heel diverse onderwijsinstellingen. Als bestuurder is het belangrijk je bewust te zijn van het feit dat iedereen kwetsbaar is en slachtoffer kan worden van een cyberincident. Daarom is het cruciaal dat meldingen (over kwetsbaarheid) ook bestuurders bereiken die minder vertegenwoordigd zijn.

Snellere melding door vindbaarheid en veiligheid

Bij elke school en ieder bestuur staat een privacy statement op de website. Toch helpt bij het voorkomen van cyberincidenten een veilige en open cultuur veel meer dan een statement. Het is daarom des te belangrijker dat medewerkers gemakkelijk kunnen vinden hoe zij in het algemeen moeten handelen en wat zij moeten doen als er een cyberprobleem is. Zorg bijvoorbeeld dat de informatie van een helpdesk en veelgestelde vragen gemakkelijk vindbaar zijn. En werk uit hoe je met elkaar in contact komt als een website uit de lucht is. Het is vooral belangrijk dat mensen zich meteen melden als een probleem zich voordoet, om te voorkomen dat het groter wordt dan nodig is.

Bekijk mooie voorbeelden van overzichtelijke pagina's over informatiebeveiliging en privacy van de Radboud Universiteit en Universiteit Twente.

Standaard 3: inrichten risicoteam

Wat betekent dit voor bestuurders?
Maak gebruik van de kennis en verantwoordelijkheden van de proces- en systeemeigenaren. Er is een samenwerking tussen een risicoteam door de chief information security officer (CISO), functionaris gegevensbescherming (FG) en controller. Deze systeemeigenaren functioneren ook als onafhankelijk adviseur voor het bestuur.

Deze standaard richt zich op het organiseren van acties naar aanleiding van (mogelijke) cyberdreigingen en -incidenten. Het risicoteam brengt dreigingsinformatie uit verschillende bronnen continu en tijdig samen, zodat het wanneer nodig kan reageren op de dreigingsinformatie en bij een cyberincident direct kan bepalen wanneer er opgeschaald moet worden binnen en buiten de organisatie.[16] Het is van belang dat er sprake is van een dekkend meldsysteem, dit is cruciaal voor een goed functionerend crisisteam.

Bij de afhandeling van cyberincidenten en voor risico-inschattingen gebruiken onderwijsinstellingen veel verschillende structuren (onder meer door schaalgrootte). U als bestuurder kunt zich afvragen of er binnen de instelling security officers werkzaam, of dat er specialistische teams zijn. Uit de jaarverslagen van instellingen blijkt dat de coronapandemie een grote impact gehad heeft op het inschatten van risico's en daarmee op het inrichten van crisisteams. Kleine instellingen beschikken meestal niet over alle expertise, maar zijn net zozeer kwetsbaar. Voor bestuurders van kleinere instellingen geldt het advies om krachten te bundelen, bijvoorbeeld door aansluiting bij stelselpartijen zoals Kennisnet, SIVON en MBO-digitaal. Verschillende hoger onderwijsinstellingen hebben de afgelopen jaren het crisismanagementplan of businesscontinuïteitsplan vernieuwd, een crisismanager aangesteld of integraal veiligheidsmanagement opgezet. Soms zijn de cyber gerelateerde risico's opgenomen in de algemene crisisaanpak. Dit zijn acties die u als bestuurder ook kunt overwegen. Het is belangrijk dat bestuurders zich bewust zijn van het feit dat de aanpak van een cyberincident verschilt van andere risico's omdat een cyberincident direct de hele instelling kan treffen.

Bij de instellingen met een computer emergency response team (CERT), heeft de CERT een rol op operationeel niveau als er een cyberincident plaatsvindt.[17] Grotere instellingen hebben soms ook decentrale CERT-teams die kunnen opschalen naar een centrale CERT. Sinds de cyberaanval op de Universiteit Maastricht wordt nadrukkelijker over de inzet van security operations centers (soc) gedacht. Daarbij ligt de focus op het actiever detecteren van cyberdreigingen om incidenten eerder op te sporen en eventuele aanvallen af te wenden of de impact daarvan te beperken.[18] Het oefenen van een cyber-crisissituatie helpt instellingen, vooral om de communicatielijnen te verbeteren tijdens crisisbestrijding. Door een cyberoefening uit te voeren blijft de structuur van de crisisaanpak bekend bij medewerkers.

Kennisdeling in het onderwijsveld is cruciaal

In december 2021 deed zich een groot probleem met Log4J voor. Dit was een kwetsbaarheid in veel verschillende softwareprogramma's waar toen nog geen oplossing voor was. Eerst was onbekend in welke programma's het was toegepast. Om het onderwijs te helpen heeft Kennisnet alle in het primair en voortgezet onderwijs gangbare digitale onderwijsproducten geanalyseerd en een openbare lijst gemaakt van softwareprogramma's die kwetsbaar waren voor Log4J. Ook als de leverancier hiervoor een oplossing had stond dit erbij. Het was mooi om te zien dat er geen lidmaatschap van Kennisnet nodig was om deze informatie te kunnen zien; die was voor iedereen toegankelijk. Kennisnet volgde hiermee de werkwijze van de Nationaal Coördinator Terrorismebestrijding en Veiligheid. SURF heeft vervolgens een vergelijkbare lijst voor het middelbaar beroepsonderwijs en hoger onderwijs gemaakt.

[16] Een risicoteam is een team dat gericht is op het detecteren en mitigeren van risico's om te voorkomen dat een cyberincident zich daadwerkelijk voordoet (preventie). Een crisisteam komt in beeld als zich een cyberincident heeft voorgedaan en het heeft een prominente rol bij de afhandeling van een cyberincident.

[17] Een CERT is een team van ICT-professionals dat zich richt op het voorkomen en verhelpen van computer of netwerk gerelateerde veiligheidsincidenten.

[18] Een soc richt zich op het voorkomen van, opsporen van, beoordelen van en reageren op beveiligingsproblemen in IT-infrastructuren en -systemen. Een soc kan zowel een eigen afdeling binnen een bedrijf zijn of worden afgenomen bij een leverancier.

Wat moet er op stelselniveau gebeuren?

Op stelselniveau is er een risicoteam dat zicht heeft op (stelsel) risico's in het (hoger) onderwijs. In dat risicoteam zijn diverse disciplines vertegenwoordigd: privacy, onderwijslogistiek, cyber, onderwijskwaliteit, beleid en naleving. Bij incidenten binnen een ho-instelling is dit risicoteam eerste aanspreekpunt voor instellingen. Bij grotere incidenten fungeert het risicoteam ook als het crisismanagementteam. Indien relevant worden (interne/externe) toezichthouders op de hoogte gebracht door (het bestuur van) de instelling.

Een aanval op één instelling kan gevolgen hebben voor het hele onderwijsstelsel. In al die gevallen kunnen een gezamenlijk risicoteam en een crisismanagementteam een belangrijke rol spelen. Op diverse plekken in het onderwijs is er sprake van kennis(deling) of respons op de afhandeling van cyberincidenten. SURF wordt gezien als een belangrijke bron van informatie voor het hoger onderwijs stelsel. SURF heeft een eigen CERT, namelijk SURF-CERT. Het NCSC deelt informatie via SURF-CERT met hoger onderwijsinstellingen. Maar helaas zijn niet alle instellingen, zoals kleine instellingen en niet bekostigde instellingen, daarbij aangesloten. Dit heeft een informatieachterstand tot gevolg en kan leiden tot kwetsbaarheden in het stelsel. Naar aanleiding van de aanval op de Universiteit Maastricht (2019) ontstond bij verschillende instellingen de behoefte aan versterking van de detectie en de monitoring van risico's om zo (mogelijke) incidenten eerder in beeld te krijgen.[19] Op het moment dat een incident gerelateerd is aan persoonsgegevens komt de Autoriteit Persoonsgegevens (AP) in beeld, omdat er een meldplicht is.[20] De AP geeft aan bijna een verdubbeling in het aantal datalekmeldingen te zien in 2021 ten opzichte van 2022.[21] De AP heeft een stappenplan opgesteld voor het ondernemen van actie bij een datalek.[22] Voor andere incidenten zijn er geen voorschriften voor het toezicht in het onderwijsdomein. Bestuurders maken zelf de afweging over het wel of niet melden. Dit is anders bij vitale infrastructuren, daar geldt wel een meldplicht. Toch blijkt dat er weinig gebruik gemaakt wordt van elkaars expertise tijdens een incident. Betrokkenen in het stelsel hebben dan helaas ook vaak maar beperkt zicht op en informatie over cyberincidenten bij individuele instellingen.[23]

Wanneer een cyberincident mogelijk de kwaliteit van het onderwijs of de continuïteit van de organisatie in gevaar brengt, kan de inspectie besluiten om een onderzoek in te stellen. Met cyberincidenten kunnen verzoeken tot losgeldbetaling gepaard gaan. Het uitgangspunt van de Nederlandse overheid is dat er geen losgeld wordt betaald aan cybercriminelen als een instelling gehackt wordt. Rechtmatigheids- en doelmatigheidseisen ten aanzien van de besteding van overheidsgelden spelen hier een rol.[24] Losgeld is onrechtmatig als het uit publieke middelen komt.

[19] Zo is er via SURF een gezamenlijk soc opgericht voor het hoger onderwijs. SURF-SOC is continu beschikbaar om op basis van signalen van een (mogelijk) incident in actie te komen. Een soc detecteert cyberdreigingen pro-actiever om zo incidenten eerder op te kunnen sporen en eventuele aanvallen af te wenden of de impact ervan te beperken. Zie: https://www.surf.nl/surfsoc-samen-informatiebeveiliging-versterken (geraadpleegd op 29 juli 2022).

[20] Onafhankelijke toezichthouder die toezicht houdt op de verwerking van persoonsgegevens.

[21] Zie: https://autoriteitpersoonsgegevens.nl/nl/nieuws/datalekken-door-cyberaanvallen-bijna-verdubbeld (geraadpleegd op 15 juni 2022).

[22] Zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/acties-bij-een-datalek (geraadpleegd op 15 juni 2022).

[23] Bij actoren in het onderwijsstelsel valt bijvoorbeeld te denken aan SURF, Kennisnet, SIVON, Digital Trust Center (DTC), Autoriteit Persoonsgegevens (AP), koepels et cetera.

[24] Rechtmatigheid ziet op de vraag of de onderwijsmiddelen wel besteed zijn in lijn met de geldende wet- en regelgeving. Doelmatigheid ziet op de vraag of de onderwijsmiddelen kosten- en doelbewust zijn aangewend. Zie: https://www.onderwijsinspectie.nl/onderwerpen/toezicht-op-financieel-beheer/toezicht-op-financiele-rechtmatigheid-en-doelmatigheid (geraadpleegd op 9 mei 2022).

Standaard 4: borgen risicomanagement

Wat betekent dit voor bestuurders?

Risicomanagement is een cyclisch, iteratief en terugkerend proces, omdat dreigingen, omgeving en wetgeving veranderen. Er wordt rekening gehouden met deze veranderingen zodat de maatregelen doeltreffend en doelmatig zijn.

Het borgen van het risicomanagement omvat alle systematische acties die nodig zijn om ervoor te zorgen dat het risicomanagement voldoet aan de kwaliteitseisen. U als bestuurder moet zorgen dat de maatregelen die voortvloeien uit het risicomanagement doeltreffend en doelmatig zijn.

Voorwaarden voor het borgen van risicomanagement zijn onder meer:

- Benoem functionarissen die verantwoordelijk zijn voor het identificeren en beoordelen van cyberrisico's.
- Stel maatregelen op basis van risico-inschattingen en -afwegingen op die helpen de mogelijke impact van cyberrisico's te verkleinen.[25]
- Zorg ervoor dat historische en actuele informatie over cyberrisico's duidelijk en beschikbaar is, en periodiek (tijdig) uitgewisseld wordt.
- Zorg ervoor dat het risicomanagement geïntegreerd is in alle werkprocessen van de organisatie en regelmatig geagendeerd wordt.

Grote instellingen stellen vaak een specifieke persoon of aparte eenheid in de organisatie aan die verantwoordelijk is voor cyberrisicomanagement (centraal of decentraal). Vaak zijn er ook structurele gesprekken tussen het bestuur en de ICT-afdeling. Kleine instellingen hebben mogelijk de verantwoordelijkheid voor het risicomanagement rond cybersecurity apart binnen – of buiten – de organisatie belegd.

[25] Denk bijvoorbeeld aan overlegstructuren ten behoeve van structurele informatie-uitwisseling.

De cyberaanval op de Universiteit Maastricht in 2019 zorgt ervoor dat risicomanagement rondom cybersecurity binnen hoger onderwijsinstellingen vaker als onderwerp op de bestuurstafel komt, soms zelfs met concrete maatregelen tot gevolg. Maar het gevoel van urgentie rond het risicomanagement van cybersecurity is vaak alleen in een deel van de organisatie aanwezig, meestal bij de ICT-afdeling en soms bij het college van bestuur. Ook is cyberrisicomanagement niet altijd onderdeel van beleidsplannen. De meeste hoger onderwijsinstellingen kennen wel al een goed uitgewerkte kwaliteitszorgcyclus, waarin ze risico's meenemen. Het onderwerp cyberveiligheid komt meestal aan bod in de jaarverslagen, maar lang niet alle instellingen noemen voorbeelden van borgingsmaatregelen. Een risico-inschatting wordt sterk beïnvloed door de waargenomen urgentie van de dreiging.[26]

Bewustwording door phishing mails

Er zijn verschillende manieren waarop organisaties kunnen nagaan of hun risicomanagementsysteem effectief is. Door bijvoorbeeld phishing mails te versturen kunnen zij zien in welke mate hun medewerkers zich bewust zijn van de risico's van zo'n bericht en hoe zij hiermee omgaan. Het is duidelijk dat sommige onderwijsinstellingen een dergelijke interventie bewust inzetten, maar dat niet iedereen dit doet. Dit soort acties kan helpen om helder te krijgen of er nog aanvullende maatregelen nodig zijn. Bekijk de voorbeelden van Erasmus Universiteit, Universiteit Utrecht en Vrije Universiteit.

[26] Zo ging er bijvoorbeeld veel meer aandacht uit naar COVID-19 dan naar cyberveiligheid.

Wat moet er op stelselniveau gebeuren?

Ook op stelselniveau is risicomanagement een cyclisch, iteratief en terugkerend proces: de actoren binnen en buiten de hoger onderwijssector wegen en prioriteren de aandacht voor diverse dreigingen. Er is aandacht voor structurele samenwerking en kennisuitwisseling zodat de maatregelen doeltreffend en doelmatig zijn.

Er moet geïdentificeerd worden welke risico's het niveau van een individuele instelling overstijgen, daarna moeten verantwoordelijkheden rond cyberrisicomanagement vastgelegd worden. Dit leidt mogelijk tot een betere borging van het cyberrisicomanagement.[27] Actuele informatie is noodzakelijk om doelmatige en doeltreffende maatregelen in te kunnen zetten. Ook is het aan te raden om de aandacht voor cyberrisico's vast te leggen in werkprocessen.

Risicomanagement is als bedrijfsvoeringsthema in het hoger onderwijs, zowel voor het bekostigde als niet-bekostigde onderwijs, de verantwoordelijkheid van de instelling zelf. Instellingen functioneren zelfstandig en zien bedrijfsvoering als een decentrale aangelegenheid. OCW geeft hiervoor momenteel geen richtlijnen. Verschillende partijen, waaronder toezichthouders, OCW, Platform Integrale Veiligheid Hoger Onderwijs (Platform IV-HO) en SURF hebben instellingsoverstijgende (cyber)risico's op de agenda staan.[28]

[27] Zo komt een vaste lijn van informatie-uitwisseling ten goede aan de borging van risico's die instellingen overstijgen.

[28] Ter illustratie: SURF richt zich specifiek op cyberrisico's. SURF is ook de partij die het cyberdreigingsbeeld voor het onderwijs samenstelt. Dit cyberdreigingsbeeld is gebaseerd op een vragenlijst onder ho en mbo-instellingen. Het platform IV-HO maakt een algemeen dreigingsbeeld, waarin ook cyberrisico's worden meegenomen.

De verantwoordelijkheid voor het structureel analyseren van cyberrisico's voor het hele stelsel is bij niemand belegd. Een gebrek aan sturing en coördinatie hierin, kan leiden tot het te laat detecteren van risico's, met als gevolg dat iedereen het wiel zelf moet uitvinden.

Er zijn verschillende stelselinitiatieven om dreigingsinformatie op een efficiënte manier met de hoger onderwijsinstellingen te delen, bijvoorbeeld via SURF-CERT. Daarnaast besluiten sommige instellingen zelfstandig om zich aan te sluiten bij landelijke taskforces. Platform IV-HO en SURF besteden veel aandacht aan instrumenten en informatie over risicomanagement, maar de vraag is of dit niet te veel uit het zicht van besturen en koepelorganisaties blijft. Meerdere RvT's blijken weinig te weten over cybersecurity, mogelijke instrumenten en de gebruikte normen. Niet veel RvT's besteden in hun verslaglegging aandacht aan cyberdreigingen.

Er moet nagedacht worden over hoe men het cyber-weerbaarheidsniveau van een hoger onderwijsinstelling vaststelt en hiervan uniform verslag legt. OCW kan hierbij via de wetgeving instellingen sturing geven, bijvoorbeeld door het opstellen van richtlijnen voor cyberveiligheid. Vooral betrokkenen die verantwoordelijk zijn voor de cyberveiligheid binnen hun instelling, blijken voorstanders van enige regulering.

Standaard 5: aandacht ketensamenwerking

Wat betekent dit voor bestuurders?
Partners en leveranciers kunnen op afhankelijke wijze aantonen dat deze partijen aan de geldende eisen voldoen.

Deze standaard richt zich op de samenwerking met partners en leveranciers, het maken van afspraken, en het onderling afleggen van verantwoording, waarbij doorlopend gecontroleerd wordt of aan de afspraken is voldaan.[29]

Instellingen opereren autonoom in een netwerk van partijen, ze bepalen hun eigen koers binnen de gegeven kaders. Door haar open karakter is het hoger onderwijs goed voorbereid op samenwerkingen met derden en heeft daarmee een stevig startpunt als het om cyberweerbaarheid gaat. Digitalisering voegt aan die ketensamenwerking binnen alle onderwijssectoren een extra dimensie toe, doordat zowel de grenzen tussen partijen als de toewijzing van verantwoordelijkheden vervagen. Uw eigen onderwijsinstelling is zelf ook een keten met interne leveranciers, waarbinnen afspraken, afstemming en vertrouwen belangrijk zijn.

Ketensamenwerking speelt binnen alle onderwijsinstellingen, maar verschilt onderling sterk en hangt af van de omvang van de instelling en de visie op uitbesteding en bekostiging. Het verschil in volwassenheid tussen de instellingen bemoeilijkt samenwerking. Vooral kleinere hoger onderwijsinstellingen kiezen bijvoorbeeld graag voor de uitbesteding van diensten en ICT door een gebrek aan kennis of capaciteit. Grotere instellingen hebben juist relatief veel interne capaciteit en beheren daardoor dus ook veel intern. Zoals een eigen securityafdeling en soms een eigen security operations center. Bij de inkoop van externe diensten en producten is de kwaliteit meer afhankelijk van externe leveranciers. Wel is het onderwerp security steeds vaker onderdeel van het inkoopproces en de samenwerkingsafspraken. Het belangrijkste hierbij is dat de afspraken duidelijk zijn en dat ze worden nageleefd.

In principe is een onderwijsinstelling zelf verantwoordelijk voor de incidentafhandeling, maar SURF(-CERT) is ook beschikbaar voor ondersteuning hierbij. SURF informeert het NCSC wel over incidenten en kwetsbaarheden, maar de betrokkenheid van het NCSC na een incident is beperkt.

Slim gebruik van voorbeelddocumenten

Bij informatiebeveiliging en privacy is continu sprake van verandering. Het Netwerk Informatiebeveiliging en Privacy po/vo is van schoolbesturen en wisselt ervaringen uit met Kennisnet, SIVON, PO-Raad en VO-raad. Leden van het netwerk kunnen voorbeelddocumenten gebruiken die een schoolbestuur helpen bij het inzetten van een onderwijstool. Bijvoorbeeld om na te gaan of er maatregelen nodig zijn om leerlingen of studenten de tool veilig te laten gebruiken. Of om te checken hoe een leverancier met persoonsgegevens omgaat in alle jaren dat de methode gebruikt wordt. Door met elkaar op te trekken hoeft niet elke onderwijsinstelling een volledige analyse zelf uit te voeren.

Wat moet er op stelselniveau gebeuren?
Op stelselniveau is er overleg over de kwaliteit en betrouwbaarheid van leveranciers van diensten en kan er gecoördineerd actie ondernomen worden om problemen op te lossen. Waar nuttig kan gebruik worden gemaakt van gezamenlijke inkoop. Er is sprake van een duidelijke en eenduidige rol- en verantwoordelijkheidsverdeling. De verschillende partijen in het veld kennen elkaars rol en weten welke maatregelen ze nemen om risico's tot een acceptabel niveau terug te dringen.

SURF is het centrale punt waaruit diverse vormen van ketensamenwerking ontstaan en worden samengebracht. Het takenpakket van SURF en de onderliggende netwerken is omvangrijk, maar niet per se dekkend. Niet alle bekostigde instellingen zijn in dezelfde mate aangesloten op de informatievoorziening vanuit SURF. Geen enkele niet-bekostigde instelling is lid van SURF. Wel heeft SURF naast leden ook klanten, die toegang hebben tot bepaalde diensten en informatie, maar niet tot alles.[30] Wie geen lid is, heeft ook geen beschikking over alle dreigingsinformatie via SURF.

De drie koepelorganisaties in het hoger onderwijs zien voor zichzelf rond cyberveiligheid een relatief bescheiden rol.[31] Informatiebeveiliging is bijvoorbeeld primair een verantwoordelijkheid van het bestuur en SURF heeft een goed functionerend netwerk waar dit zijn plek heeft.

[29] Een voorbeeld van samenwerking op gebied van cyberveiligheid (bestuurlijk, juridisch of ICT-gerelateerd) is de Cyber Security Academy. Dit is een initiatief van de Universiteit Leiden, de Technische Universiteit Delft en De Haagse Hogeschool met steun van de gemeente Den Haag.

[30] Er zijn bijvoorbeeld verschillende niet-bekostigde instellingen die onder andere Microsoft en andersoortige licenties inkopen via SURF.

[31] De drie koepelorganisaties in het hoger onderwijs: Universiteiten van Nederland, Vereniging Hogescholen en Nederlandse Raad voor Training en Opleiding'.

Het NCSC en SURF-CERT kennen een lange samenwerking. Na het incident bij de Universiteit Maastricht is besloten dat het NCSC het hoger onderwijs op de hoogte brengt bij cyberdreigingen of kwetsbaarheden. NCSC is een kennisautoriteit die sectorspecifieke CERT's kan ondersteunen zodat ze zo goed mogelijk hun werk kunnen doen, en heeft tegelijk ook informatie van hen nodig. Sectorspecifieke CERT's hebben namelijk generieke informatie over bijvoorbeeld kwetsbaarheid in de kritieke processen en melden die aan het NCSC. Het NCSC richt zich op organisaties uit de vitale sectoren. Het Digital Trust Center (DTC) speelt ook een rol in geval van cyberdreigingen. Het DTC heeft een samenwerkingsverband met de Nederlandse Raad voor Training en Opleiding (NRTO). De NRTO is de brancheorganisatie voor private onderwijsinstellingen en het informatiepunt voor cybersecurity voorlichting.[32]

Gezamenlijke DPIA op Google Workspace

Bij het gebruik van softwarepakketten en cloud oplossingen blijft het bestuur verantwoordelijk voor de digitale veiligheid van medewerkers, studenten en leerlingen. Dat geldt ook voor de bescherming van de persoonsgegevens die nodig zijn om zo'n pakket te gebruiken. Om die te mogen verwerken moet een Data Protection Impact Assessment (DPIA) zijn uitgevoerd; daaruit blijkt namelijk of aanvullende maatregelen nodig zijn. Als verschillende onderwijsinstellingen dezelfde software gebruiken kunnen zij een gezamenlijke DPIA laten uitvoeren. Bij het gebruik van Google Workspace in het onderwijs is dit bijvoorbeeld zo aangepakt. SURF en SIVON hebben destijds namens de onderwijssector gesprekken met de leverancier gevoerd. Ook hebben zij vastgelegd welke handelingen noodzakelijk zijn als bestuurders Google Workspace willen blijven gebruiken.

[32] Zie: https://www.digitaltrustcenter.nl/samenwerkingsverband/nrto/ (geraadpleegd 30 juni 2022).

Standaard 6: controleren en evalueren

Wat betekent dit voor bestuurders?
Regelmatige controle en evaluatie zijn belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie (zoals regelmaat en rapportages).

Door de cyberaanval bij de Universiteit Maastricht zijn instellingen zich bewuster van de noodzaak van integrale controle en evaluatie, waarbij ICT een vast onderdeel vormt van de plan-do-check-act-cyclus (PDCA).[33] Vooral grote hoger onderwijsinstellingen geven aan evaluaties in verschillende vormen uit te voeren voor risicomanagement rond cybersecurity. Ook nemen meerdere instellingen deel aan de landelijke cybercrisisoefening. Om tot acties te komen helpt het om door de verschillende lagen van de organisatie heen verantwoordelijkheden aan te wijzen voor het identificeren, beoordelen en evalueren van cyberrisico's.

De normenkaders die gehanteerd worden, verschillen tussen de (bekostigde en niet-bekostigde) instellingen, denk aan: het SURF-normenkader[34] en de ISO-normering[35]. Meerdere RvT's geven aan geregeld de evaluatiegegevens te bespreken in hun vergadering of in hun auditcommissie, maar het blijkt lastig om de evaluatiegegevens goed te kunnen interpreteren. Controle en evaluatie leiden daarom niet altijd tot de nodige verbeteringen en instellingen verantwoorden zich niet publiekelijk over informatiebeveiliging (IB). Daarnaast wordt de ICT-evaluatie vaak als losstaand onderdeel gezien van cybersecurity ; de verbinding leggen tussen alle betrokkenen en belangen blijkt lastig in de praktijk.

Vooral de verantwoordelijken voor ICT geven aan dat ze constant afwegingen maken over de ernst van alle actuele dreigingen, zodat aandacht en maatregelen op tijd opgeschaald of afgeschaald worden. Naast een (uitgebreide) audit zijn er verschillende instellingen die op soms beperkte schaal de praktijk van hun Informatiebeveiliging beproeven, met name door een zogeheten pentest.[36]

Bij grotere instellingen is de PDCA-cyclus geformaliseerd en worden er periodiek (in elk geval jaarlijks) gesprekken gevoerd tussen het CvB en de verantwoordelijke directeuren op basis van de managementrapportages. Die rapportages bevatten doorgaans ook een risico-paragraaf met de topvijfrisico's, verbeterpunten en lopende acties. Toch halen cyberrisico's uiteindelijk meestal niet de top vijf van hoogste prioriteiten. Het is aan te raden om cybersecurity een vast onderdeel te maken van een dergelijke management-rapportage. Bij een goed functionerende PDCA-cyclus hoort ook het afleggen van verantwoording over de gesignaleerde risico's en de acties om deze te adresseren. De RvT is verantwoordelijk voor het interne toezicht en legt in een aparte passage in het jaarverslag verantwoording af over de controle en evaluatie, maar vaak bevatten deze weinig informatie over cyberveiligheid.

Kijk hoe uw eigen instelling scoort!

In het mbo wordt jaarlijks een IBP-E benchmark uitgevoerd die aandacht schenkt aan Informatie-beveiliging (IB), Privacy (P) en Examinering (E). De resultaten op sectorniveau vindt u op de website van MBO Digitaal. Het gaat om een zelfassessment door bekostigde mbo onderwijsinstellingen. Een aantal van de mbo instellingen voert een peer review uit waarbij onderwijsinstellingen elkaars zelfinschattingen beoordelen. De IBP-E benchmark sluit aan bij de ontwikkelingen van het normenkader onderwijs. Weet u als bestuurder hoe uw eigen instelling scoort op deze monitor? Heeft u ook een beeld van uw score in relatie tot uw eigen informatiebeveiligingsbeleid? Wat zijn uw uitdagingen voor de komende tijd?

Grootschalige cyberoefening: doe mee!

Elke twee jaar organiseert SURF de OZON-oefening: een grootschalige en sectorbrede cyberoefening voor onderwijs en onderzoek. Leden van SURF, waaronder universiteiten, scholen, ziekenhuizen en onderzoeks-instellingen, kunnen meedoen. Bij zo'n oefening wordt geoefend met verschillende aspecten die je bij een cyberaanval kunt tegenkomen. Denk niet alleen aan technische aspecten, maar ook bijvoorbeeld aan woordvoering bij een ransomware-aanval. Op de website vindt u ook de ervaringen en evaluaties van vorige edities.

[33] Een stapsgewijze methode gericht op het doorvoeren van verbeteringen in een organisatie.

[34] Voor meer informatie over het normenkader voor de SURF-audit en volwassenheidsniveaus, zie: https://www.surf.nl/normenkader-surfaudit-audit-je-informatiebeveiliging (geraadpleegd op 26 april 2022). Een bewerkte versie van het SURF normenkader wordt gebruikt ten behoeve van het middelbaar beroepsonderwijs, zie: https://mbodigitaal.nl/wp-content/uploads/2016/08/IBPDOC2A-Normenkader-Informatie-beveiliging-MBO-versie-2.0.pdf (geraadpleegd op 12 juli 2022). Er wordt tevens gewerkt aan een normenkader voor het funderend onderwijs. Zie: www.vo-raad.nl/system/downloads/attachments/000/001/398/original/Adviesrapport_Regie_op_ICT_opgemaakt.pdf?1648116531 (geraadpleegd 11 juli 2022).

[35] Zie ISO 27001 en 27002. Voor meer informatie zie: https://www.nen.nl/ict/digitale-ehtiek-en-veiligheid/cyber-privacy/informatiebeveiliging#:~:text=De%20norm%20ISO%2027002%20beschrijft,basisstructuur%20met%20kerneisen%20voor%20managementsysteemnormen (geraadpleegd op 25 april 2022).

[36] Een pentest is een test die inzicht geeft of een computersysteem of software kwetsbaarheden bevat. Na een pentest worden veelal specifieke maatregelen genomen om deze kwetsbaarheden te verhelpen.

Wat moet er op stelselniveau gebeuren?

Er is een landelijk dreigingsbeeld voor risico's in het onderwijs. Er is zicht op de mate waarin instellingen en het stelsel als geheel zijn voorbereid op risico's, hoe risico's worden afgehandeld en er wordt geëvalueerd welke aanpassingen op stelselniveau nodig zijn om escalatie en herhaling te voorkomen.

Cybersecurity is een onderwerp dat de grenzen en de verantwoordelijkheid van de individuele instelling overstijgt. Dit geldt ook voor de controle op en evaluatie van dit onderwerp. Landelijke normen zijn nodig, evenals een benchmark en externe expertise. Het uiteindelijke doel van controleren en evalueren op stelselniveau is het lerend vermogen van het stelsel als geheel te bevorderen.

SURF heeft een normenkader voor informatiebeveiliging in het hoger onderwijs ontwikkeld (Baseline Informatiebeveiliging Hoger Onderwijs, BIHO).[37] Het normenkader is verder uitgewerkt in een toetsingskader waarmee instellingen een self-assessment uitvoeren of een audit laten uitvoeren. Het normen- en toetsingskader vormt de basis van de tweejaarlijkse SURF-audit-benchmark waaraan instellingen vrijwillig kunnen deelnemen.[38] Bij niet-bekostigde instellingen is het normenkader vrijwel onbekend. Met de Universiteiten van Nederland en de Vereniging Hogescholen is afgesproken dat alle bekostigde instellingen deelnemen aan de SURF-audit en dat zij minimaal volwassenheidsniveau 3 nastreven. Ook heeft SURF recent een vernieuwde versie van hun cyberdreigingsbeeld gedeeld.[39]

Er is geen specifieke toezichthouder voor cyberweerbaarheid in het onderwijs. In- en externe toezichthouders kunnen wel het bewustzijn vergroten door: monitoring, rapportering en agendering. Ook is er geen wettelijk voorschrift voor de bedrijfsvoering in het algemeen of voor cyberveiligheid in het bijzonder. De bedrijfsvoering valt onder de verantwoordelijkheid van de individuele instelling en haar bestuur; daarom is de overheid terughoudend in het geven van inrichtingsaanwijzingen. Voor bekostigde onderwijsinstellingen geldt wel dat de continuïteit van het onderwijs en het onderzoek gewaarborgd moet zijn en dat de besteding van middelen rechtmatig en doelmatig moet zijn. Ook niet-bekostigde instellingen moeten de continuïteit van het onderwijs waarborgen om de bevoegdheid om graden te verlenen niet te verliezen. Momenteel is het nog onduidelijk wat de precieze verantwoordelijkheid is van externe toezichthouders hierbij. Er is ook weinig samenwerking tussen de inspecties en overheidsdepartementen. Een samenwerking tussen de toezichthouders zou een stimulans kunnen zijn om tot eenzelfde volwassenheidsniveau te komen als de vitale sectoren.

De inspectie heeft geen handhavingsgronden op instellingsniveau, maar kan wel thematisch stelselonderzoek doen naar de kwaliteit van het (hoger) onderwijsstelsel als geheel. De meeste hoger onderwijsinstellingen hebben geen behoefte aan steviger toezicht, ze geloven meer in het oplossen van incidenten via de formele en informele mogelijkheden die SURF biedt. Tegelijkertijd heeft SURF niet de opdracht of het mandaat om in te grijpen bij een ernstig incident.

[37] Scipr (SURFibo) (2015) *Baseline Informatiebeveiliging HO*. Zie https://www.surf.nl/files/2019-03/baseline-informatiebeveiliging-ho-2015.pdf (geraadpleegd op 26 april 2022).

[38] Voor meer informatie over het normenkader voor de SURF-audit en volwassenheidsniveaus, zie: https://www.surf.nl/normenkader-surf-audit-audit-je-informatiebeveiliging (geraadpleegd op 26 april 2022).

[39] http://www.surf.nl/files/2022-06/cyberdreigingsbeeld-onderwijs-en-onderzoek-2021-2022-lr.pdf (geraadpleegd op 11 juli 2022).

Standaard 7: geld investeren in informatiebeveiliging

Wat betekent dit voor bestuurders?
Er worden voldoende middelen beschikbaar gesteld om de onderkende risico's op een adequate manier te behandelen.

Deze standaard richt zich op de beschikbaarheid van voldoende middelen. Bestuurders geven daarbij aan met een dilemma te zitten: moeten zij zich bij elke investeringsvraag afvragen hoeveel geld nodig is en of dat geld ook aan andere zaken besteed kan worden?

ICT is inmiddels onlosmakelijk verbonden geraakt met het primaire onderwijsproces, het onderwijs is daardoor steeds meer afhankelijk van ICT. Om te bepalen of een maatregel adequaat is, is een sluitende PDCA-cyclus cruciaal.

U als bestuurder bent verantwoordelijk voor het geheel aan investeringen, waaronder ICT. Daarnaast is er doorgaans een centrale ICT-dienst of ICT-directie met een eigenstandig budget waarbinnen gehandeld wordt, vaak als resultaat van een meerjarenbegroting. Instellingen hebben veel beleidsvrijheid in het alloceren van hun bekostiging en binnen een begroting heeft informatiebeveiliging vaak een eigen plek.

Grotere instellingen schatten het risico op cyberdreigingen hoger in door de recente incidenten in het hoger onderwijs en zetten dit om in concrete maatregelen. Kleinere instellingen schatten hun risico's vaak juist lager in, waardoor hun investeringen kleiner zijn en ze minder maatregelen uitvoeren voor het risicomanagement. Mogelijk zijn de investeringen hierbij ontoereikend.

Incidenten hebben geleid tot een gevoel van urgentie, met het gevolg dat noodzakelijke investeringen hoger op de lijst komen te staan. Maar investeringen in de preventie van cyberrisico's zijn vaak onzichtbaar en daarmee intern minder goed te verdedigen, een benchmark voor de omvang van investeringen en de maatregelen is wenselijk.

Uit het onderzoek blijkt dat niet alle basismaatregelen van het NCSC volledig ingebed zijn bij onderwijsinstellingen. Dit maakt het stelsel kwetsbaar en roept vragen op rond sturing.

Wat moet er op stelselniveau gebeuren?
Er worden voldoende middelen beschikbaar gesteld om de onderkende risico's op een adequate manier te behandelen. Dat impliceert dat er regelmatig op basis van een risico-inventarisatie wordt bepaald of er op stelselniveau voldoende middelen beschikbaar zijn voor informatiebeveiliging en of er binnen de bekostiging van instellingen voldoende middelen besteed (kunnen) worden aan beveiliging en preventie.

Onderwijsinstellingen en andere organisaties in het onderwijsveld kunnen op basis van een risico-inventarisatie bepalen of er op stelselniveau voldoende middelen beschikbaar zijn voor IB. Bekostigde instellingen ontvangen een bedrag van de overheid en zijn zelf verantwoordelijk voor de doelmatige besteding hiervan. Maar de vraag is of er voldoende middelen besteed worden aan cyberveiligheid en de preventie van cyberdreigingen. De onderwijsbekostiging vindt plaats volgens het lumpsum-principe en kent daarom geen specifieke toedeling voor bedrijfsvoering. Wel wordt door onderwijsinstellingen aangegeven dat cyber gerelateerde investeringen betaalbaarder worden als het gezamenlijk wordt geregeld. Informatiebeveiliging wordt gezien als primaire verantwoordelijkheid van de onderwijsinstelling zelf. Wel komen er uit diverse incidenten systemische knelpunten naar voren die vragen om generieke maatregelen vanuit het gehele stelsel. SURF speelt hierin ook een rol voor het hoger onderwijs.

Initiatieven voor investeringen en maatregelen komen in het hoger onderwijs doorgaans van onderop, er is een sterke vraagsturing. Dit leidt voor een deel ook tot een ad hoc-beleid. Er is geen businesscase gemaakt op stelselniveau: wat zijn de kosten op stelselniveau en wat zijn de risico's van niet investeren? De verschillen in de volwassenheidsniveaus, de omvang, de visie en de budgetten, zorgen voor een ongelijke uitgangspositie tussen verschillende instellingen. Vooral kleine instellingen geven aan de investeringen niet zelf te kunnen dragen.

Losgeldbetaling is onwenselijk omdat het verdienmodel van hackers zo in stand gehouden wordt. Daarnaast is het onrechtmatig omdat het een betaling van gemeenschapsgeld aan criminelen is. Maar echt goede beveiliging is enorm duur, waardoor het voor individuele instellingen toch financieel aantrekkelijker kan zijn om losgeld betalen. Losgeld is onrechtmatig als het uit publieke middelen komt. De stelselkosten daarvan zijn potentieel enorm. Om dit zoveel mogelijk te voorkomen, is er meer solidariteit in het stelsel nodig. De kosten voor de preventie en voor het oplossen van een hack-incident moeten daarom in gezamenlijkheid gedragen kunnen worden.

Denk op tijd aan budget voor concrete acties

Geld investeren in informatiebeveiliging is belangrijk. Het Nationaal Cyber Security Centrum geeft aan welke basismaatregelen elke organisatie zou moeten treffen. Een goed voorbeeld is investeren in het gebruik van twee-factor-authenticatie. Dit houdt in dat je naast je gebruikersnaam en wachtwoord nog op een andere manier moet aantonen dat jij recht hebt op toegang, zoals door een sms controle of gebruik van een authenticator app. De Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), de Hogeschool van Amsterdam en de Universiteit van Amsterdam hebben deze maatregel versneld doorgevoerd, nadat zij getroffen waren door een cyberaanval.

Aanbevelingen voor bestuurders op basis van de standaarden

Het onderwerp cyberveiligheid vraagt uw aandacht.
Op basis van onze onderzoeken en gesprekken zien we dat er nog veel kansen zijn om de cyberveiligheid van het onderwijs te verbeteren. Hieronder een overzicht van onze aanbevelingen:

- Schenk aandacht aan zowel de technische als de menselijke kant van cybersecurity.
- Wees je bewust van het verschil in kennisniveau over cybersecurity tussen medewerkers en zorg dat kennis up-to-date is.
- Agendeer het belang van informatiebeveiliging regelmatig, dit draagt mogelijk bij aan de bewustwording en aan veiliger digitaal handelen.
- Vergroot het bewustzijn met: basisinformatie en voorlichting, awareness, security by design en laagdrempelige, transparante en veilige meldprocedures.
- Stimuleer en borg een veilige en open cultuur door te denken aan:
  - de voorbeeldfunctie van het bestuur voor anderen in de organisatie;
  - het vastleggen en borgen van een zorgvuldige meldprocedure;
  - het als bestuur ondersteunen van de procedure en mensen die de regels uitvoeren en naleven.
- Neem niet alleen privacy op als onderwerp in de beleidsplannen en de jaarverslagen, maar ook brede informatiebeveiliging (inclusief: borgingsmaatregelen, controle en evaluatie).
- Zorg dat de informatie over ICT en cybersecurity goed vindbaar is, evenals de contactgegevens van de helpdesk.
- Meldingen moeten niet enkel gaan over privacy-gerelateerde zaken maar ook over veiligheid in de brede zin van het woord.
- Evalueer het crisismanagementplan of het business-continuïteitsplan en vernieuw deze wanneer gewenst. Overweeg om een crisismanager aan te stellen of een integraal-veiligheidsmanagementteam op te richten. Neem cybergerelateerde risico's op in de algemene crisisaanpak.
- Wijs door verschillende lagen van de organisatie heen verantwoordelijkheden toe voor het identificeren, beoordelen en evalueren van cyberrisico's, of zorg dat dit extern geborgd is.
- Sluit je aan bij stelselinitiatieven die toezien op het delen van dreigingsinformatie, denk bijvoorbeeld aan partijen als Kennisnet, SIVON, MBO-Digitaal, IV-HO en SURF; doe bijvoorbeeld mee met cybercrisisoefeningen en intensiveer de samenwerking met andere onderwijsinstellingen óók met niet-bekostigde onderwijsinstellingen.
- Wees je ervan bewust dat met de inkoop van ICT-diensten een afhankelijkheidspositie wordt gecreëerd. Zorg dat security onderdeel wordt van het inkoopproces en van de samenwerkingsafspraken.
- Maak ICT een vast onderdeel van de PDCA-cyclus en voer evaluaties uit ter bevordering van het risicomanagement rond cybersecurity.
- Bepaal op basis van een risico-inventarisatie of er op stelselniveau voldoende middelen beschikbaar zijn voor informatiebeveiliging. Maak een businesscase voor de specifieke situatie.
- Betaal geen losgeld aan hackers. Dit houdt namelijk het verdienmodel van hackers in stand en is onrechtmatig aangezien het een betaling van gemeenschapsgeld aan criminelen is.

Voor de volledige lijst met aanbevelingen, zie het rapport Binnen zonder Kloppen – Digitale Weerbaarheid in het Hoger Onderwijs.