PLATFORM
INTEGRALE VEILIGHEID
HOGER ONDERWIJS

Een initiatief van de Vereniging Hogescholen en VSNU

KPMG

Aan de Vereniging Hogescholen & VSNU
Van de Stuurgroep Integrale Veiligheid Hoger Onderwijs (IV-HO)
15 juni 2020

Aanbieding sectoradvies:

‘Governance van Cybersecurity, Privacy & Kennisveiligheid HO – Pas toe of leg uit!’

Als Stuurgroep van het Platform Integrale Veiligheid Hoger Onderwijs geven wij richting aan de ontwikkeling van integrale veiligheid in het hoger onderwijs. In het platform werken onze mensen gezamenlijk aan dit actuele onderwerp. Zo hebben zij langs de bestuurlijke lijn geadviseerd aan de Minister OCW op het onderbreken en weer op gang brengen van het fysieke onderwijs n.a.v. de coronacrisis. Het hoger onderwijs heeft zich gelukkig weerbaar getoond en binnen korte tijd een historische omslag gemaakt naar online onderwijs en onderzoek.

Dat betekent ook dat we onze weerbaarheid op het gebied van cybersecurity en kennisveiligheid moeten vergroten. De ransomware-aanval op de Universiteit Maastricht ligt hierbij nog vers in het geheugen. Ook op het gebied van kennisveiligheid moeten we stappen zetten. Kennisdeling is van groot belang voor onze maatschappelijke en economische ontwikkeling, maar is ook interessant voor criminele organisaties en sommige buitenlandse mogendheden.

In de brief aan de Tweede Kamer van het ministerie van OCW van februari is een aantal maatregelen aangekondigd. Deze maatregelen liggen op technisch niveau: betere monitoring en detectie (SOC’s), daarnaast intensievere samenwerking, het vergroten van veiligheidsbewustzijn en audits.

Om ook invulling te geven aan het aspect van organisatieontwikkeling is in Platformverband onderzocht hoe de governance van Cybersecurity en Kennisveiligheid in de instellingen zelf ingericht zou kunnenworden om de bestuurbaarheid ervan te verbeteren. Vervolgens is met KPMG, de CISO’s en enkele ‘cyberprofessoren’ een expertopinie tot stand gekomen.

Deze Positon Paper bevat dus een expertopinie over de inrichting van de cybersecurityfunctie. in samenhang met de andere integrale veiligheidsgebieden. Het is een service-document en er gaat geen normerende werking vanuit. Het bevat een ideaalbeeld dat ter inspiratie wordt aangeboden. Uiteraard speelt schaalgrootte een rol en is de praktijk weerbarstig, maar wij hopen dat het paper zal bijdragen aan kennisontwikkeling en het goede gesprek in onze sector hoger onderwijs, met een duidelijk ideaalbeeld voor ogen...

Verzoek

Als Stuurgroep IV-HO willen wij onze collega-bestuurders van hoger onderwijsinstellingen uitnodigen om in koepelverband deze Position Paper te agenderen.

Bijlage(n):

Position Paper

PLATFORM
INTEGRALE VEILIGHEID
HOGER ONDERWIJS

Een initiatief van de Vereniging Hogescholen en VSNU

KPMG

POSITION PAPER

Definitieve versie, 20 april 2020

Inrichting governance van cybersecurity in het hoger onderwijs

Pas toe of leg uit!

Deze Position Paper is opgesteld vanuit het Platform Integrale Veiligheid Hoger Onderwijs (IV-HO)[1] en gaat in op de twee veiligheidsgebieden 'Cybersecurity & Privacy' en 'Kennisveiligheid', zoals beschreven in het 'Dreigingsbeeld Hoger Onderwijs'[2]. In deze paper hanteren wij voor de eenvoud de term 'cybersecurity' om de governance van deze veiligheidsgebieden te belichten. Integrale veiligheid[3] en zeker ook cybersecurity gaan als een saté-prikker dwars door andere beleidsterreinen heen en hebben raakvlakken met een veelvoud van hen, zoals HR, wet- en regelgeving, financiën en kwaliteit.

Voor de duidelijkheid: cybersecurity beslaat niet enkel de digitale bescherming van informatie, maar behelst ook de informatiebeveiligingsaspecten van kennis, privacy, fysieke beveiliging en continue beschikbaarheid van informatie en IT.

Waarom is een inhaalslag hard nodig?

Instellingen voor hoger onderwijs zijn van nature open, kennis moet kunnen stromen. Er was hierdoor in het verleden dan ook weinig noodzaak tot een 'Fort Knox'-beveiliging en een volwassen cybersecurityfunctie. Het bewustzijn wat betreft informatie- en IT-gerelateerde risico's was traditioneel ook laag. Die tijden zijn veranderd; specifieke informatie heeft bij instellingen een hoge waarde en een uiterst vertrouwelijk karakter (de 'kroonjuwelen' zoals gevoelige persoonsgegevens), de beschikbaarheid van de informatie- en IT-voorzieningen is onmisbaar en de integriteit van onderzoeks- en studieresultaten is cruciaal.

Recente incidenten en een toenemend dreigingsniveau laten zien dat een flinke inhaalslag van de digitale weerbaarheid moet plaatsvinden. Cybersecurity gaat niet enkel over het voorkomen van incidenten, maar ook over het snel detecteren en herstellen van incidenten, en het organiseren hiervan.

De minister van OCW heeft in haar recente Kamerbrief aangegeven dat wordt geïnvesteerd in beveiligingsbewustzijn, monitoring (SURFcert, Security Operations Centers) en periodieke toetsing. Reeds in 2018 is het belang van cybersecurity en in de bredere zin integrale veiligheid binnen het hoger onderwijs onderkend door de vorming van het platform IV-HO.

---

1 Opgesteld door KPMG is samenwerking met de werkgroep IV-HO-governance. Wij bedanken de hoogleraren Cybersecurity Bibi van den Berg (UL) en Michel van Eeten (TU Delft) voor hun input en feedback. Deze Position Paper is niet bedoeld als weergave van hun standpunten. Tevens hebben de SCIPR-bestuursleden en CSC-voorzitters een conceptversie van feedback kunnen voorzien.

2 Het hoger onderwijs heeft zich in 2018 gecommitteerd aan het sectorbreed en in iedere instelling integraal organiseren en professionaliseren van het veiligheidsbeleid.

3 De andere integrale veiligheidsgebieden, te weten Sociale Veiligheid, Zorgwekkend gedrag & Radicalisering, Internationalisering, Integriteit, Gebouwveiligheid en Arbo & Milieu komen hier niet expliciet aan bod; wel zijn dezelfde principes van toepassing.

Deze Position Paper vormt de vervolgstap door een standpunt in te nemen over de organisatorische inrichting van cybersecurity en met name over de 'aanvoerder' om de inhaalslag invulling te geven.

Deze paper gaat derhalve in op de governance van cybersecurity[4]. Voor nadere detaillering verwijzen wij graag naar het 'Model Informatiebeveiligingsbeleid' van SCIPR. De organisatorische inrichting op de andere veiligheidsgebieden kan eenzelfde route volgen als beschreven in deze paper. Hieronder lichten wij de inrichting van cybersecurity als voorbeeld toe.

Waaraan dient de inrichting van effectieve governance te voldoen?

De juiste inrichting van de cybersecurityfuncties is van belang om risico's te analyseren, beleid en prioriteiten te bepalen, medewerkers voor te lichten, de juiste maatregelen te laten treffen en deze na periodieke evaluatie zo nodig bij te stellen. Cybersecurity is niet met een technische exercitie of compliance-checklist op een hoog niveau te krijgen, wel met risicomanagement, prioriteitstelling en een multidisciplinaire aanpak.

Een gedegen governance en strategische positionering van cybersecurity waarborgen aanvullend dat de geschikte technische en organisatorische maatregelen getroffen worden om de relevante risico's af te dekken, en dat deze gehandhaafd worden én blijven. Daarbij mag het geen onnodige bureaucratie introduceren of een negatieve kosten-batenverhouding opleveren. Instellingsbrede besluitvorming en rapportering over cybersecurity dient efficiënt te kunnen verlopen en nevengeschikt – en dus niet ondergeschikt – te zijn aan andere beleidsterreinen. Dit zorgt ervoor dat nieuwe onderzoeksprojecten, samenwerkingen, e.d. het minimum cybersecurityniveau niet kunnen ondermijnen.

Dit voorstel betreft niet louter een structuurkwestie (het 'harkje'); natuurlijk zijn ook de bijbehorende processen, bewustwording, cultuur en wijze van persoonlijk opereren en communiceren onontbeerlijk om een hoger cybersecurityniveau te bereiken. Belangrijke uitgangspunten zijn dat het bredere veiligheidsbeleid integraal is georganiseerd en dat de governance aansluit bij het besturingsmodel van onderwijsinstellingen.

Hoe past de CISO-functie in de organisatiestructuur? ('verticale ophanging')

Het CvB draagt de eindverantwoordelijkheid voor risico's van de gehele instelling, inclusief die van cybersecurity. Ondersteunend hieraan is het proces van *Enterprise Risicomanagement* (ERM) dat risico's identificeert en inzichtelijk maakt, voorstellen doet voor risicobeperking en (rest)risico's monitort.

Het CvB belegt het informatie- en risico-eigenaarschap in de (1e) lijn en mandateert beleidsmakers en functionele experts in de beleidsstaf (2e lijn) om hen te helpen die risico's tot een acceptabel niveau te reduceren – dus niet om verantwoordelijkheid voor risico's of cybersecurity te nemen! Die 1e lijn bestaat uit het management in de faculteiten of instituten, maar ook in de ondersteunende diensten. Daar hoort ook het eigenaarschap voor cybersecurity te liggen.

4 NB: Voor privacy bestaat de wettelijke functie van Functionaris Gegevensbescherming (FG), die onafhankelijk toezicht houdt op en adviseert over privacy (vanuit de 3e lijn). Hierdoor is naast de formele FG-functie ook een rol weggelegd voor een Privacy Officer (vanuit de 2e lijn), die vergelijkbaar is met die van de CISO (m.a.w. voor privacybeleid, inrichten privacyrisicomanagementsysteem, inbrengen expertise, ondersteunen DPIA's, e.d.).

De aanvoerder voor cybersecurity is de CISO of Chief Information Security Officer. De CISO is de 2e lijn: de gemandateerde beleidsmaker, cyberrisicomanager en expertmatig adviseur van de 1e lijn. Dus niet de IT-specialist die beveiligingsmaatregelen treft. De CISO is op instellingsniveau beleidsvoorbereidend, ondersteunt de organisatie met hun lijnverantwoordelijkheid voor risicoanalyses van processen, projecten en inkopen, geeft expertadvies aan de 1e lijn en is één van crisismanagers bij incidenten. Een CISO rapporteert periodiek aan het CvB en de RvT over de voortgang op het jaarplan, risico's en een aantal kritieke indicatoren, zoals incidenten en veiligheidsbewustzijn. Het bestuur kan alleen met een goed overzicht de risico's overzien en op onderbouwde wijze de juiste keuzes maken. Ook vormt de CISO het interne én externe aanspreekpunt voor cybersecuritykwesties.

Grote instellingen beschikken daarnaast ook over een onafhankelijke interne auditfunctie (3e lijn) die de relatie tussen informatie/risico-eigenaren in de 1e lijn en beleidsmakers (2e lijn) monitort op effectiviteit. De meeste onderwijsinstellingen missen veelal een onafhankelijk orgaan dat de naleving van beleid en effectiviteit van het samenspel tussen 1e en 2e lijn toetst en vaststelt of de 2e lijn relevante risico's voor de organisatie ophaalt en monitort. Zij kunnen deze toetsende rol dan extern laten invullen, of die verwachten vanuit Raad van Toezicht, inspectie, Autoriteit Persoonsgegevens of accountant. De drie verdedigingslijnen zijn geadopteerd uit de private sector, waar dit zg. '*three lines of defence*'-model de de-facto standaard is voor organisatorische inrichting van risicobeheersing.

HO-instellingen zijn bijzondere instituten, waar het adopteren van dergelijke corporate governanceprincipes uit het bedrijfsleven naast een organisatorische aanpassing ook een cultuurverandering vraagt. Met het CvB als beleidsbepaler varen de faculteiten, instituten en hun decanen/directies deels een eigenstandige koers. Ze beschikken over beleidsvrijheid en eigen budget, beheren gebouwen en laboratoria, bepalen hun aanname-beleid, e.d. Om de gehele instelling op het minimaal vereiste cybersecurityniveau te laten opereren is het noodzakelijk dat de governance van cybersecurity alle organisatieonderdelen bereikt en betrekt. De decentrale mindset waarin deze faculteiten en instituten leven geldt niet voor IT en cybersecurity; zij zijn technisch te zeer met elkaar verweven. Een lokaal aangeschafte cloudtoepassing of een zelfstandig met internet verbonden lab kan niet alleen de kroonjuwelen van eigen onderzoek aantasten, maar maakt de gehele instelling kwetsbaar en kan ernstige verstoringen en datalekken veroorzaken.

De CISO heeft derhalve behoefte aan ondersteuning en voelsprieten in dergelijke organisatieonderdelen. Die voelsprieten zullen geformaliseerd moeten worden, bijvoorbeeld als een aangestelde '*Integrale Veiligheid liaison*', die adviseert en niet optreedt als politieagent. Deze IV-liaison moet de faculteit goed kennen (en anders-om) en affiniteit hebben met de veiligheidsgebieden. Verantwoordelijkheid, bevoegdheid en taken van deze functie dienen expliciet beschreven te zijn, evenals de functionele relatie met de IV-verantwoordelijken, zoals de CISO. Maar bovenal moeten de IV-liaisons voldoende tijd en aanzien hebben om betrokken te zijn bij projecten en ontwikkelingen die spelen en dienen zij naleving van cybersecuritybeleid te stimuleren. De CISO zal op regelmatige basis moeten overleggen met deze IV-liaisons om in de gehele organisatie geworteld te blijven.

Moet de CISO buiten IT worden gepositioneerd? ('horizontale ophanging')

In veel instellingen voor hoger onderwijs rapporteert de CISO aan de IT-directeur of aan de CIO, zowel functioneel als hiërarchisch. Alhoewel dat vanuit het verleden logisch verklaarbaar is en soms goed gedijt, is dit geen duurzame oplossing. De CISO schrijft beleid en risico- en compliancegebaseerde prioriteiten voor die ten dele door de IT-organisatie vertaald en ten uitvoer moeten worden gebracht. Ook ziet de CISO toe op de afhandeling van cybersecurity-incidenten die onder andere in de IT-organisatie kunnen zijn ontstaan. Dit maakt dat de CISO onafhankelijk van de IT-directeur c.q. de CIO moet kunnen functioneren. Het advies van de CISO aan het CvB moet soms anders kunnen zijn dan of zelfs tegenstrijdig kunnen zijn met dat van de IT-verantwoordelijke. Wanneer de CISO onder IT ressorteert, is er geen sprake van zg. '*countervailing power*' met voldoende checks & balances – er ontbreekt een gezonde tegenstelling van belangen. Kortom, een volwaardige CISO behoort buiten de IT-organisatie en het CIO Office gepositioneerd te zijn.

De CISO heeft natuurlijk een thuishaven en leidinggevende nodig, niet iedere beleids- of integrale veiligheidsfunctie kan tenslotte rechtstreeks onder het bestuur hangen. Een logische positie voor deze functie is bij één van de stafdiensten, bij andere 2e-lijnsfuncties. De CISO geniet daarbij nog steeds de vrijheid om het CvB onafhankelijk en (on)gevraagd te adviseren over beleid, om onderzoek te doen naar incidenten en om prioriteit te vragen voor nieuwe risico's. Bovendien kan de functie zo ook goed worden gesitueerd samen met de andere integrale veiligheidsgebieden; deze dienen samen te komen in een multidisciplinair integraal veiligheidsoverleg of bestuurlijk platform. De positionering van de CISO en de functionele lijn met andere (2e-lijns)staffuncties is essentieel voor het effectief kunnen uitvoeren van deze functie, net als een constructieve werkrelatie met de technische cybersecurityfuncties in de IT-organisatie.

"CISO's moeten CvB duidelijk maken dat cybersecurity veel meer is dan een IT-vraagstuk alleen."

Bibi van den Berg (hoogleraar Cyber Security Governance, Universiteit Leiden)

Hoe invulling te geven aan de eisen aan de CISO-functie?

De invulling van de CISO-functie kent verschillende taakgebieden op strategisch, tactisch en operationeel gebied die uiteenlopende, multidisciplinaire competenties vereisen. Belangrijke competenties betreffen in ieder geval het op bestuurlijk niveau en op managementniveau afstemmen over risicomanagement- en handhavingsvraagstukken en het uitdragen van noodzakelijke vervolgstappen. Natuurlijk moeten er naast een krachtige bestuurlijke en organisatorische focus ook een goede relatie en goede communicatie met de IT-organisatie zijn – zonder de technische oplossing te veel voor te schrijven. Deze combinatie van competenties is schaars en gewild. Duurzame aandacht, passende inbedding én inschaling van deze functie in de organisatie helpt om CISO's vast te houden.

De CISO-functie behelst meerdere rollen die door verschillende individuen of door één persoon kunnen worden uitgevoerd. Ook zijn enkele rollen heel duidelijk niet onderdeel van de CISO-functie: de Functionaris Gegevensbescherming (FG) gezien diens positionering en onafhankelijkheid; de technische security manager die zich bezighoudt met de inrichting van cybersecuritymaatregelen omdat die rol niet past naast die van beleidsmaker. Het is wel essentieel dat de CISO intensief samenwerkt met deze rollen om de (gepercipieerde)

afstand tussen de lines of defence klein te houden. Rollen die wel in de CISO-functie[5] passen (en momenteel nog niet zijn opgenomen in het functiehuis) zijn onder andere[6]: beleidsmaker cybersecurity, informatierisico-manager, adviseur veiligheidsbewustzijn en eventueel Privacy Officer (afzonderlijk van de FG).

Zoals aangegeven, is een CISO niet eindverantwoordelijk voor cybersecurity; de CISO is ook geen risico-eigenaar. De CISO (of iemand uit diens team) dient betrokken te zijn bij belangrijke projecten, inkopen en samenwerkingsverbanden. Derhalve ligt het budget voor cybersecurityactiviteiten en -projecten in de lijn respectievelijk bij opdrachtgevers, mits de als kritiek geclassificeerde cybersecurityprojecten ook daadwerkelijk worden uitgevoerd. Deze vorm van prioriteren en budgetteren dient verankerd te zijn in de planning- en controlcyclus en in het projectportfoliomanagement. Bovendien moet de CISO toereikend eigen budget hebben voor de strategische en tactische processen, zoals het opstellen van een meerjarenroadmap cybersecurity, het laten uitvoeren van technische (hack)testen en (SURF)audits, het inhuren van advies of het opschroeven van het veiligheidsbewustzijn van medewerkers en studenten. Bovendien dient dit budget ook toereikend te zijn om tijdelijk medewerkers uit andere organisatieonderdelen toe te wijzen om beveiligingsprojecten gerealiseerd te krijgen.

“Voor de CISO geldt: budget hebben is invloed hebben.”

Michel van Eeten (hoogleraar Governance of Cyber Security, TU Delft)

Welke aanbevelingen leiden tot succes?

Wij raden bestuurders van hoger onderwijsinstellingen aan:

- Organiseer cybersecurity integraal met andere veiligheidsgebieden op basis van risicomanagementprincipes.
- Positioneer de CISO-functie passend in de organisatie (als zuivere 2e-lijnsfunctie en in de relevante gremia). Voor sommige instellingen zal een ‘Leg uit’-optie met overbruggingsperiode en groeipad nodig zijn. Dit geldt bijvoorbeeld vanwege de huidige organisatiestructuur of -omvang en een reeds functionerende constellatie, waarin de CISO nog vanuit de 1e lijn opereert. Desondanks kunnen onze overige aanbevelingen onverkort worden opgevolgd.
- Rust de CISO uit met mandaat, budget en capaciteit om de jaarplandoelen te kunnen bereiken.
- Organiseer cybersecurityfuncties in de functiehuizen voor universiteiten en hogescholen en zorg voor adequate inschaling van de CISO-functie in het instellingsfunctiehuis om CISO met de benodigde competenties te kunnen aantrekken en behouden.
- Geef duurzame aandacht aan cybersecurity en investeer in de relatie met de CISO.
- Regel periodieke rapportage van de CISO aan het CvB (minimaal kwartaallijks) en de RvT (minimaal jaarlijks).
- Bewaak de balans in volwassenheid tussen het kwartet organisatie – mensen – processen – techniek in de voortgang van cybersecurity.

5 In kleinere organisaties kunnen verschillende IV-rollen door één persoon of een klein team worden ingevuld.
6 Voor de detailinvulling van de CISO-functie (en overige informatiebeveiligingsfuncties) verwijzen wij naar de hieronder vermelde publicatie over ‘Beroepsprofielen Informatiebeveiliging 2.0’.

- Draag zorg voor een vorm van informatiegovernance; de cybersecurityfunctie kan alleen goed functioneren als er zicht is op (minimaal) de kroonjuwelen, alsmede het eigenaarschap en informatiemanagement daarvan zijn ingericht.
- Stel een meerjarenplan op om het gewenste niveau voor de verschillende integrale veiligheidsgebieden te behalen én te borgen.
- Start gezamenlijk sectorbrede initiatieven op het gebied van cybersecurity, zoals het inkopen van producten of diensten (b.v. managed Security Operations Centers), het uitwisselen van kennis en personeel, e.d.

Referenties:

- Model voor Informatiebeveiligingsbeleid SCIPR
- Dreigingsbeeld IV-HO
- Cyberdreigingsbeeld hoger onderwijs
- Beroepsprofielen Informatiebeveiliging
- SURFaudit
- Cybersecurity white paper