mbo digitaal

CISO as a Service

De menukaart

Datum	*Versie*	*Status*	*Auteur*
6 oktober 2023	1.0	Definitief	Henry Meutstege

Management Samenvatting:
In dit document beschrijven we hoe de dienst CISO as a Service eruitziet. Deze dienst wordt opgezet als Pilot vanuit het programma Cyberveiligheid in het MBO, en zal bij succes ondergebracht worden bij het Security Expertise Centrum van SURF.

De dienst heeft als doel de digitale weerbaarheid van een instelling aantoonbaar te verbeteren. Dit doen we door een ervaren CISO beschikbaar te stellen vanuit het programma. Deze CISO zal vanuit de behoefte van de instelling helpen bij het maken van een plan om te groeien in cyber volwassenheid. Als normenkader zal het SURFaudit Toetsingskader Informatiebeveiliging (het NBA-model) gebruikt worden. De dienst CISO as a Service moet bijdragen aan de ambitie om te groeien naar streefniveau 3 van volwassenheid.

Dit document beschrijft de dienst CISO as a Service als een menukaart. Je kunt als instelling kiezen voor een compleet “diner”, of je kiest een enkel “gerecht”.

mbo digitaal

Inhoudsopgave

Bijlagen

Bijlage 1: Aanvraagformulier
Bijlage 2: Functieprofiel CISO

Leeswijzer

Hoofdstuk 1 dienstbeschrijving.
Hoofdstuk 2 proces om de dienst aan te vragen inclusief de voorwaarden

1 De dienst CISO as a Service

In dit hoofdstuk beschrijven we hoe de dienst CISO as a Service eruitziet. Wat is het doel wat we willen bereiken. Welke onderdelen zitten erin en welke stappen worden doorlopen.

1.1 Aanleiding

De MBO Raad en het platform MBO Digitaal hebben een plan van aanpak opgesteld om de cyberveiligheid in het mbo te verbeteren. Dit plan van aanpak is voor de komende jaren de roadmap op het gebied van informatiebeveiliging en privacy, met een breed palet aan maatregelen om als mbo-sector weerbaarder te worden tegen cyberaanvallen en de privacy beter te borgen.

Het programma Cyberveiligheid wordt uitgevoerd door MBO Digitaal, het digitaliseringsplatform van de MBO Raad. Dat gebeurt in nauwe samenwerking met de netwerken van MBO Digitaal, waaronder het Netwerk IBP in het mbo, de Regiegroep IBP en het CSC-netwerk van SURF-contactpersonen.

De ambitie van ons als sector is om de Cyberveiligheid te verhogen, vertaald in het bereiken van ambitieniveau 3 van volwassenheid. Niveau 3 wordt in het algemeen beschouwd als een goede balans tussen veiligheid en de kosten van de te nemen maatregelen. Het valt op dat op het gebied van informatiebeveiliging er grote verschillen zijn in volwassenheid. Vooral kleinere instellingen zijn steeds minder goed in staat om aan de toenemende eisen op het gebied van cyberveiligheid te voldoen. Vanuit het programma Cyberveiligheid willen we extra aandacht besteden aan het ondersteunen van de kleine instellingen. Wij geloven sterk in het gezamenlijk optrekken van de mbo-instellingen. Juist door niet steeds opnieuw het wiel uit te willen vinden, maar actief kennis te delen zijn we in staat om samen sterk te zijn, ook in de verdediging tegen cybercriminaliteit.

Vanuit SURF is een werkgroep CISO as a Service actief geweest, waarbij met een aantal onderwijsinstellingen (mbo en HO) is geïnventariseerd wat het profiel van een CISO is, wat de ambities zijn, de mogelijke knelpunten en de gewenste invulling kan zijn van de dienst CISO as a Service. De uitkomsten van deze werkgroep worden meegenomen bij het uitwerken en opzetten van deze dienst. In bijlage 2 is een functieprofiel opgenomen van de CISO rol, zoals opgesteld door de werkgroep CISO as a Service van SURF. Dit profiel gebruiken we als referentie om deze dienst vorm te geven.

1.2 Doel

Het programma Cyberveiligheid heeft als doel om de cyberweerbaarheid van de mbo-sector te verbeteren. De dienst CISO as a Service moet de instellingen helpen om gestructureerd en volgens een concreet plan de digitale weerbaarheid van een instelling te verbeteren. Daarbij wordt het SURF audit toetsingskader gebruikt als volwassenheidsmodel en toetsingskader, waarbij de ambitie is om een gemiddelde volwassenheid van niveau 3 te behalen.

Daarbij is het belangrijk om te onderzoeken waar de exacte behoefte ligt binnen het mbo. Is dat inderdaad de ondersteuning van een CISO als een dienst? Willen de mbo's het zelf invullen, door bijvoorbeeld een CISO te delen over meer instellingen? Of ligt het zwaartepunt toch meer op technische ICT ondersteuning en weerbaarheid? Daarom beginnen we met deze dienst in pilot vorm en zullen we de komende maanden samen gaan ervaren of er voldoende draagvlak is voor deze dienst. Mocht de pilot succesvol zijn, is het de bedoeling dat deze dienst door het Security Expertise Centrum van SURF geadopteerd wordt en van daaruit wordt aangeboden aan de leden van SURF. De uiteindelijke dienst zal dan ook in nauwe samenwerking met SURF verder ontwikkeld worden (inclusief businessplan en een business case).

Tijdens de pilot zal vooral gericht worden op het ondersteunen van een beperkte groep mbo-instellingen. Opbrengsten, bijvoorbeeld een bepaalde aanpak, voorbeelddocumenten, templates etc. zullen geanonimiseerd ter beschikking komen voor de gehele sector.

1.3 De aanpak en planning

Wanneer een mbo-instelling een aanvraag heeft gedaan voor ondersteuning van de dienst CISO as a Service en de aanvraag is goedgekeurd[1] en door het programma in behandeling genomen is, zijn er een aantal mogelijkheden. Als metafoor gebruiken we "de Menukaart" met daarop het drie gangen diner beschreven. Wil je als instelling groeien op alle thema's van het SURFaudit Toetsingskader zal er een volledig diner besteld kunnen worden. Van intake met de bestuurder, het opstellen en het realiseren van een plan (inclusief tijdslijnen en budget) tot en met de borging in de organisatie zelf. Maar het kan ook zijn dat de mbo-instelling behoefte heeft op tijdelijke ondersteuning bij 1 van de hieronder beschreven onderdelen. Dan kan er gekozen worden voor een afzonderlijk "gerecht" net waar op dat moment behoefte aan is.

1.3.1 De intake

Belangrijk is dat er commitment is van het bestuur van een instelling bij het afnemen van de dienst CISO as a Service. Er moet commitment zijn voor het te behalen ambitieniveau en de daarbij horende invulling van de CISO rol (inclusief mandaat). Daarom zal er ook altijd begonnen worden met een intake bij de instelling, waar de CISO vanuit MBO Digitaal in gesprek gaat met de bestuurder van de instelling over de dienst CISO as a Service. Het belangrijkste doel van dit gesprek is om de wederzijdse verwachtingen uit te spreken en als resultaat op te nemen in een opdrachtomschrijving. Deze opdrachtomschrijving zal als "contract" worden ondertekend door de bestuurder van de mbo-instelling, waarbij de belangrijkste eigenaren van de instelling het contract kennen en ondersteunen. Eigenaren zijn bijvoorbeeld het bestuur, de IT verantwoordelijke, de HR manager en de verantwoordelijke voor facilitaire dienstverlening. Algemene voorwaarden onderdeel zijn van dit "contract".

1.3.2 De randvoorwaarden

De dienst CISO as a Service is vooral bedoeld als katalysator om de instelling te helpen de juiste stappen te nemen in de gewenste groei van digitale weerbaarheid. Daarbij gebruiken we een bij voorkeur een risicoanalyse van de instelling zelf. Als die nog niet beschikbaar is, zal een risicoanalyse (aan de hand van het SURFaudit Toetsingskader/NBA model) 1 van de eerste stappen zijn die uitgevoerd moet worden. Belangrijk is dat de instelling zelf betrokken is bij de uitvoering en ook in staat is om na afloop van de dienst zelf de verantwoordelijkheid voor informatiebeveiliging

[1] Zie hoofdstuk 3 voor het proces van aanvragen en goedkeuren van de dienst

te dragen. Keuzes worden gemaakt op basis van de risico inschatting en van daaruit worden te nemen maatregelen gedefinieerd. De dienst CISO as a Service kan en zal gedurende de opdracht betrokken zijn en blijven als adviseur en expert.

Het is belangrijk om vanaf het begin de belangrijkste eigenaren van de opdracht bij de dienst CISO as a Service te betrekken. Denk daarbij aan de verantwoordelijke voor IT, de HR-manager en de facilitair manager van de instelling. Vanuit de instelling zal ook een Informatie Beveiliging en Privacyfunctionaris betrokken zijn, veel van de uitvoerende taken zullen hier belegd moeten worden. Ook is het belangrijk om een 'wegwijzer' aan te stellen, die de CISO as a Service helpt om zo snel mogelijk de betrokken instelling te leren kennen.

Belangrijk is ook om vanaf het begin de Functionaris Gegevensbescherming te betrekken in het te maken plan en zijn goedkeuring te krijgen bij de uitvoering.

Als laatste belangrijke stakeholders zijn de eerste lijns verantwoordelijken. Zij moeten vooral op de hoogte zijn van dit plan en begrijpen dat dit ook gevolgen heeft voor al het onderwijzend en het ondersteunend personeel. Het is een opdracht die vanuit de gehele organisatie gedragen moet worden en is zeker niet alleen een ICT-probleem.

1.3.3 Planning

De verwachte doorlooptijd bij een instelling is erg afhankelijk van de uitgangspositie die uit de nulmeting en de risicoanalyse komt. Bij elke instelling beginnen we met een intake en worden er ook afspraken gemaakt over de verwachte doorlooptijd en de benodigde inspanning vanuit de instelling zelf. In de pilotfase zal de doorlooptijd maximaal 4 maanden zijn. Wanneer het daadwerkelijk een dienst wordt zal de verwachte doorlooptijd van het gehele traject bij een instelling tussen de 3 maanden en 1 jaar liggen.

1.3.4 Financieel

De dienst CISO as a Service zal door het programma Cyberveiligheid gefinancierd worden. Maar de instelling moet wel bereid zijn om de realisatie van de onderdelen van het plan zelf te financieren. Het kan bijvoorbeeld zijn dat er een awareness programma onderdeel is van het plan. De uitvoering van dit onderdeel zal vanuit de instelling zelf moeten komen. Natuurlijk zal de CISO ondersteunen bij het inzichtelijk maken van eventuele kosten, en zal helpen bij zoveel mogelijk hergebruik van kennis en ervaringen bij andere instellingen en/of bij SURF. De instelling moet zich ervan bewust zijn dat de realisatie van de groei ook budget vraagt vanuit de instelling.

1.4 Het Diner

1.4.1 Het voorgerecht

Na de intake en de getekende opdracht vanuit het bestuur is het als allereerste belangrijk om een beginpunt te kiezen. Vrijwel elke instelling heeft een nulmeting liggen op basis van het SURF toetsingskader. Deze nulmeting nemen we als uitgangspunt.

De eerste stap die de CISO zal uitvoeren is het toetsen van het eerder uitgevoerde assessment. We doen het assessment niet over, maar wel kijken we naar de actualiteit van het assessment en waar

eventuele punten ter verbetering liggen. Het uitgangspunt hierbij is dat de instelling zelf het beste beeld heeft en natuurlijk ook eindverantwoordelijk is voor het resultaat van de toetsing.

Met de uitkomsten van het assessment wordt een risicoanalyse uitgevoerd, waar we samen met de instelling de belangrijkste verbeterpunten definiëren en risico gebaseerd keuzes maken. De CISO as a Service zal op basis van de risicoanalyse de thema's benoemen met verbetervoorstellen en zal ze prioriteren op basis van de uitkomsten van de risicoanalyse. Daarmee wordt tevens bepaald wat de "hoofdgerechten" zullen zijn in het menu.

1.4.2 Het hoofdgerecht

Als hoofdgerecht wordt er gekeken naar de thema's uit het SURFaudit Toetsingskader (NBA model) op basis van de uitgevoerde risicoanalyse. De thema's waar naar gekeken wordt zijn:

- Governance:
    - Van strategie tot beleid, inclusief risicomanagement
    - Is er een plan/roadmap om informatiebeveiliging en privacy te verbeteren
    - Vindt er periodiek een (formele) toetsing plaats
- Processen:
    - Het bewustzijn binnen de instelling
    - Zijn de basis beheerprocessen op orde (ITIL)
    - Zijn de systemen en de data geclassificeerd?
    - Zijn de personeel procedures in lijn met de gewenste veiligheid?
    - Hoe is het toegangsbeheer geregeld (fysiek en logisch).
    - Wat zijn de afspraken met de leveranciers (incl. cloud leveranciers).
    - Is Bedrijfscontinuïteit en crisismanagement ingericht.
- Technische weerbaarheid van de instelling
    - Hoe zijn de operationele procedures ingericht
    - Hoe is het netwerk beveiligd
    - Hoe zijn de werkplekken beveiligd
    - Hoe worden kwetsbaarheden gedetecteerd en verholpen
    - Is er een patchbeleid
    - Is monitoring en logging ingeregeld, bij voorkeur met ondersteuning van een SOC/SIEM dienst?
    - Zijn er backup en restore procedures?
    - Vind er periodiek een technische toets plaats door het uitvoeren van kwetsbaarheden scans, een penetratie test of een red team test?

De verbetervoorstellen vormen de basis voor een plan van aanpak die vanuit de instelling ondersteund en onderschreven wordt. De instelling krijgt vervolgens het stuur om het plan daadwerkelijk uit te voeren. De CISO as a Service blijft beschikbaar als adviseur of zal voor een afgesproken periode de expert rol invullen. De CISO as a Service zal periodiek een voortgangsgesprek houden met de belangrijkste stakeholders en zal de voortgang rapporteren naar de bestuurder van de instelling.

In beginsel zal de CISO een ondersteunende rol vervullen bij de instelling. Tijdens de pilot zal dit wel onderwerp van ons onderzoek zijn, en moeten we bepalen in welke mate er behoefte is aan bijvoorbeeld meer operationele ondersteuning.

Tenslotte zullen er afspraken gemaakt worden op na een afgesproken termijn een formele toetsing op de voortgang te doen (eventueel door een externe auditor). Ook deze formele toetsing zal vanuit de CISO as a Service begeleid worden, waarbij de rapportage opgeleverd zal worden aan de bestuurder.

1.4.3 Het nagerecht

Het voorstel is om de dienst af te sluiten op een vooraf afgesproken termijn, en de dienst dus af te sluiten met een formele toetsing. Tijdens de pilot is de periode beperkt tot een termijn van 3 tot 4 maanden.

Belangrijk voor het succes van de gehele dienst is dat opgedane kennis en ervaring gedeeld zal worden binnen de sector. Elke mbo-instelling is vooraf bereid zijn kennis en ervaring te delen, zodat initiatieven te kopiëren zijn naar collega instellingen. Alleen door samenwerken worden we sterker. En belangrijk is dat de opgedane kennis en ervaring geborgd kan worden in de instelling zelf, zodat de instelling steeds minder afhankelijk zal zijn van externe ondersteuning.

1.5 De gerechten in detail

1.5.1 De opdrachtomschrijving

Samen met de bestuurder en de belangrijkste eigenaren komen tot een opdrachtomschrijving die als “contract” door alle partijen ondertekend wordt. In het contract worden afspraken gemaakt over de te behandelen thema’s inclusief de doorlooptijd van de te nemen acties en de benodigde financiering (wat betaald het programma, welke bijdrage wordt van de instelling verwacht).
De opgedane ervaringen en kennis wordt na afloop gedeeld met de sector.

1.5.2 Toetsen

De dienst kan een toetsing uitvoeren (als self assessment, of als peer review) op de uitgevoerde verbeteringen. Waarbij de resultaten input zijn voor het op te stellen plan om de informatiebeveiliging binnen de instelling op een hoger volwassenheidsniveau te brengen.

1.5.3 Risicoanalyse

De basis voor de te nemen maatregelen is altijd een risicoanalyse. Keuzes worden gebaseerd op daar waar voor de instelling de grootste risico’s zitten. We zullen wel altijd beginnen met een risicoanalyse op de technische weerbaarheid, het is erg belangrijk om daar eerst de meest basale maatregelen ingericht te hebben. Bij de technische weerbaarheid zal ook gekeken worden naar de mate waarin de instelling kan herstellen van een eventuele aanval (incidentproces, crisismanagement). Daarna zal er vanuit de besturing (governance) gekeken worden of de organisatorische randvoorwaarden voldoende zijn ingevuld (beleid en risicomanagement). Tenslotte komen thema’s als toegangsbeveiliging, dataclassificatie, leveranciersmanagement en business continuïteit aan de orde.

1.5.4 Ondersteuning

De CISO as a Service kan ondersteuning leveren op specifieke thema’s. Dit kan als volledige dienst (het complete menu), maar kan ook op onderdelen (het gerecht) ingevuld worden.

Een ondersteuning op aanvraag kent een vaste afbakening en zal uitgevoerd worden op een vooraf afgesproken thema of thema's. De volgende thema's worden daarbij gebruikt als afbakening:

- De besturing, inclusief risicomanagement
    - Het beleid op basis van de aanwezige standaard templates. Zowel strategisch beleid als thema beleid is aanwezig. Beleid is uitgewerkt in duidelijke operationele richtlijnen en procedures.
    - Hoe ziet de organisatie eruit, hoe is de IT geregeld en welke personen hebben een dagelijkse verantwoordelijkheid in dit domein, is er iemand aangesloten bij SCIPR.
    - Eigenaarschap. Wat betekent eigenaarschap voor de bestuurder, wat betekent het voor het management.
    - Risicomanagement als vliegwiel om continu te verbeteren. Keuzes worden gemaakt op basis van afwegingen. Keuzes worden vastgelegd, en de eigenaar accepteert een eventueel te nemen risico. Is er een risicoregister, worden risico acceptaties bijgehouden en geadministreerd.
    - Is er een verbeterplan, met een duidelijke planning en benodigd budget gespecificeerd
    - Is er een architectuurmodel waar de instelling zich aan heeft verbonden en ook actief volgt?
    - Vind er periodiek een formele toetsing plaats op de voortgang, wordt de voortgang gerapporteerd aan het bestuur. Is er een rapportage proces waar de organisatie ook rapporteert over de informatiebeveiliging en privacy maatregelen.
    - Wordt de volwassenheid op het gebied van informatiebeveiliging en privacy gemeten en worden de resultaten gedeeld via de SURFaudit benchmark en eventueel opgeslagen in een GRC-omgeving van de instelling.
- Het bewustzijn binnen de instelling
    - Security awareness programma opzetten op basis van CyberSafe Yourself (van SURF), eventueel aangevuld met specifieke acties
    - Wordt er periodiek gemeten wat de volwassenheid van de instelling is op het gebied van bewustzijn?
    - Wat is de gemeten volwassenheid, welke interventies zijn nodig? Zijn er doelgroepen die specifieke aandacht vereisen
    - Is er een onboarding programma voor nieuwe medewerkers
    - Is er een basis training op het gebied van IB en P, die "verplicht" is voor alle medewerkers
- Hoe zijn de HR procedures ingeregeld
    - Is er een screening procedure voor nieuw personeel en wordt ook bestaand personeel periodiek gescreend
    - Is er aandacht voor training en opleiding van personeel (ook op gebied van informatiebeveiliging en privacy)
    - Is er aandacht voor sleutel personen binnen de organisatie, en is er een back up plan beschikbaar bij uitval van sleutel personen
- Worden systemen en de gebruikte data geclassificeerd? Is duidelijk wat de gewenste Beschikbaarheid, Vertrouwelijkheid en Integriteit is van de systemen en de gebruikte data?
    - Is de eigenaar betrokken bij de classificatie?
    - Wat zijn de belangrijkste systemen van de organisatie (de kroonjuwelen). Zijn deze in voldoende mate beschermt en is deze bescherming in lijn met de classificatie van deze systemen
    - Wordt ongestructureerde data geclassificeerd (office documenten, mail, etc.).

    - Is er een afgesproken procedure om data te delen buiten de organisatie, wordt er gecontroleerd op ongewenst gebruik van data sharing omgevingen (zoals dropbox, wetransfer, etc.)
- Hoe is het toegangsbeheer geregeld, hebben medewerkers de juiste rechten om hun werk te kunnen doen (niet meer, en niet minder)
    - Is er een beleid op basis van rollen gebaseerde toegang?
    - Wat is er geregeld voor instroom, doorstroom en uitstroom van personeel
    - Zijn de belangrijkste applicaties voorzien van een autorisatiematrix en vind er regelmatig controle plaats op de uitgegeven autorisaties?
    - Is er een wachtwoordbeleid, en hoe wordt daar op toegezien? Is er een procedure om meerdere inlogpogingen te detecteren en te bewaken.
    - Is multi factor authenticatie ingeregeld?
- De technische weerbaarheid van de instelling (het ICT-domein)
    - Zijn er security baselines (standaard configuraties) van de belangrijkste infrastructuur componenten in het ICT-domein.
    - Zijn de IT Service managementprocessen ingeregeld (incident, change, problem, configuratie management, …)
    - Is er iemand van de instelling aangesloten bij SCIRT, is er een verbinding met het SURF Cert
    - Zijn de basis security management processen geregeld (patch management, netwerk security (incl firewalls, IPS/IDS)
    - Hoe zijn de endpoints beschermd? Virus scanners, malware scanners, etc.
    - Zijn er maatregelen genomen voor logging en monitoring. Is de instelling aangesloten op de SOC/SIEM oplossing van SURF (SURFsoc)?
    - Zijn de backup en restore processen ingeregeld? Worden die getest? Zijn er backups op een offline locatie beschikbaar?
    - Is er een proces om kwetsbaarheden te detecteren en te managen? Wat is de status van de door SURF uitgevoerde IV-metingen? Is er een responsible disclosure beleid? Worden er periodiek security testen uitgevoerd (penetratie testen, red teaming oefeningen)?
- Leveranciersmanagement, hoe zijn de afspraken met de leveranciers (incl. cloudleveranciers) vastgelegd en zijn daar de juiste informatiebeveiliging afspraken gemaakt
    - Welke contracten zijn er, incl verwerkersovereenkomsten en SLA’s
    - Wat gebeurt er bij incidenten bij een leverancier
    - Is er een right to audit afgesproken
- Bedrijfscontinuïteit en crisismanagement. Als er toch iets ernstigs gebeurt, is een instelling dan in staat om te herstellen?
    - Zijn er herstelplannen?
    - Is er een crisismanagement proces (CSIRT, Calamiteiten procedure, relatie met SURF Cert)

De CISO as a Service zal indien nodig specialisten op de betreffende thema’s betrekken bij het geven van ondersteuning. Dit zijn specialisten vanuit het programma Cyberveiligheid of specialisten vanuit SURF.

2 Het aanvraagproces

Om alle instellingen de kans te geven gebruik te maken van deze dienst is er een gestructureerd aanvraagproces ingericht.

2.1 De aanvraag

Een (mbo-) instelling kan een verzoek[2] indienen voor ondersteuning. De gewenste ondersteuning kan op een specifiek thema, of kan voor een complete aanpak. De aanvraag wordt zo specifiek mogelijk omschreven, door de aanvrager. De kosten van de ondersteuning worden gedragen door het programma cyberveiligheid.

De aanvraag wordt ingediend bij het programma Cyberveiligheid en zal vanuit het programma beoordeeld worden.

2.2 De toedeling van de aanvraag

Aanvragen worden op volgorde van binnenkomst behandelt en beantwoord. Vanuit het programma Cyberveiligheid zal de aanvraag beoordeeld worden door de programmamanager en de dienst eigenaar van de dienst CISO as a Service.

De criteria op basis waarvan de toedeling plaats vindt:

- De risicoanalyse en de ernst van de dreiging; de instelling waar de hoogste risico's worden gezien krijgen voorrang. Ook de uitkomsten van eerder uitgevoerde nulmeting wordt hierin meegewogen
- De betrokkenheid van de benodigde stakeholders van de instelling (bestuur, ICT). De instelling waar er een hoge mate van betrokkenheid blijkt krijgt voorrang
- Is de instelling in staat om de ondersteuning uiteindelijk te borgen in de eigen organisatie. De mate waarin dit mogelijk lijkt wordt meegewogen
- Is de instelling duidelijk bereid de geleerde lessen te delen met de overige mbo-instellingen. Daar waar de bereidheid om kennis te delen hoog is, krijgt de instelling voorrang.

Wanneer het programma Cyberveiligheid positief adviseert zal in het wekelijkse programma overleg het definitieve besluit genomen worden over de toedeling van de aanvraag. Daar wordt ook gekeken welke expertise nodig is om de aanvragende instelling goed te ondersteunen, waarbij ook een afweging gemaakt wordt op basis van beschikbare capaciteit in het programma Cyberveiligheid.

De instelling wordt geïnformeerd over de toedeling (zowel positief als wanneer het een afwijzing betreft).

[2] Zie bijlage 1 voor het Aanvraagformulier. Deze kan via de mail verstuurd worden.

Wanneer de pilot succesvol is zullen de resultaten opgenomen worden in het SURF Security Expertise Centrum.

2.3 Voorwaarden

De aanvraag wordt vertaald in een standaard opdrachtomschrijving, waarin een duidelijke afbakening is opgenomen. De Opdrachtomschrijving bevat onder andere de op te pakken thema's, de afgesproken doorlooptijd en de contractuele voorwaarden. De opdrachtomschrijving wordt ondertekent door het bestuur van de aanvragende instelling.

Belangrijk onderdeel van de opdracht is de borging van de kennis in de aanvragende instelling. De opdracht zal dan ook altijd in nauwe samenwerking met personeel van de mbo Instelling uitgevoerd moeten worden. De betrokken medewerkers worden vrijgemaakt voor deze opdracht voor een vooraf af te spreken aantal uur per week.

Instellingen conformeren zich aan standaarden en afspraken zoals afgesproken vanuit MBO Digitaal en SURF (zie hiervoor ook het opgestelde Convenant Cyberveiligheid MBO).
Instellingen zijn bereid en helpen ook actief om opgedane kennis bij het uitvoeren van de opdracht te delen met collega instellingen. Alle opgedane kennis en ervaring is vrij om te gebruiken bij het ondersteunen van de overige instellingen. De kennis zal verzameld worden bij het SURF Security Expertise Centrum en van daaruit beschikbaar gemaakt worden.

mbo digitaal

BIJLAGE 1: **Aanvraagformulier**
Versturen naar het programma Cyberveiligheid

Instelling: _____
Naam: _____
Functie: _____
E-mail: _____
Telefoon nr.: _____

Wat zie jij als de grootste risico's op het gebied van cyberveiligheid voor jouw instelling?

Hoe kan deze dienst jou helpen bij het beperken van deze risico's?

Wat is de huidige volwassenheid op het gebied van Informatiebeveiliging en wanneer is dit voor het laatst gemeten?

Op welke wijze denk je de opgedane kennis & ervaring tijdens het uitvoeren van deze dienst te kunnen borgen in jouw instelling?

Denk je dat het geschetste risico/probleem breder speelt in de mbo-sector en is de beoogde oplossing breder bruikbaar?

Bijlage 2: Functie profiel CISO

Dit profiel beschrijft de CISO-functie, met als doel duidelijkheid te geven wat de CISO-functie inhoudt, inclusief te verantwoordelijkheden, taken, benodigde kennis en vaardigheden. Dit functieprofiel is opgesteld onder regie van SURF in de workshop 'Ciso as a Service'. In deze workshop waren vertegenwoordigers van WO, HBO en MBO aanwezig en betrokken.

Doel CISO-functie
De informatie van de organisatie is veilig en beschermd tegen bedreigingen of verlies, zoals ongeoorloofde toegang, diefstal of beschadiging. De Chief Information Security Officer (CISO) vervult een sleutelrol in het versterken van de cyberweerbaarheid en vergroten van het cybersecurityvolwassenheidsniveau. Binnen instellingen is de CISO verantwoordelijk voor het informatiebeveiligingsbeleid. Dit betreft zowel het definiëren en implementeren van beleid als het sturen van, toezichthouden op en ondersteunen in de uitvoering daarvan. De CISO is een gesprekspartner op strategisch niveau van de organisatie.

Welke verantwoordelijkheden en taken heeft de CISO-functie?
- De CISO: is verantwoordelijk voor het waarborgen van de veiligheid van de informatie en gegevens van een organisatie/ instelling;
- is verantwoordelijk voor het ontwikkelen en implementeren van beleid en procedures om de informatiebeveiliging van de organisatie / instelling te waarborgen;
- definieert de informatiebeveiligingsstrategie, in afstemming met en als onderdeel van andere beveiligingsdomeinen en management (zoals bijvoorbeeld privacybescherming, fysieke beveiliging, kennisveiligheid, continuïteits-management, risicomanagement);
- zorgt voor organisatie brede richtlijnen, standaarden, methoden, technieken en architectuur (proces, data- en systeemarchitectuur) voor informatiebeveiliging, waaronder vereisten op het gebied van wet- en regelgeving en organisatie behoeften;
- inventariseert de informatiebeveiligingsbehoefte van de organisatie / instelling, en stelt mede op basis daarvan de beveiligingsmaatregelen op;
- monitort de naleving van informatiebeveiligingsbeleid, -richtlijnen en -standaarden, onder meer door het (laten) uitvoeren van informatiebeveiligings-audits – en assessments;
- toetst proces (-ontwerpen) aan de uitgangspunten van informatiebeveiliging (Informatiebeveiliging by design);
- rapporteert en adviseert over informatiebeveiligingsrisico's aan management en bestuur;
- borgt het informatiebeveiligingsbewustzijn bij in- en externe stakeholders en partners;
- richt de calamiteiten- en incidentenorganisatie in, gericht op informatiebeveiliging.

Welke kennis en vaardigheden bezit de CISO?
Het goed uitvoeren van de CISO-functie vraagt om de volgende kennis en vaardigheden:
- Ruime expertise in informatiebeveiliging: een diepgaand begrip van de concepten, technologieën en strategieën die betrokken zijn bij informatiebeveiliging. Dit omvat kennis van beveiligingsstandaarden en -praktijken, zoals ISO27001, NIST, CIS-controls, COBIT en vaardigheden in het beheren van verschillende beveiligingsdomeinen, waaronder netwerkbeveiliging, applicatiebeveiliging, identiteits- en toegangsbeheer en cryptografie.
- Risicomanagement: ervaring met het (onder druk) doen van (IB) risicobeoordelingen, in combinatie met het kunnen opstellen van een passende risicostrategie, maatregelen en onderbouwing met een business case.
- Leiderschapskwaliteiten: de CISO heeft een bewezen staat van dienst als leider en verandermanager, mede op basis van een inspirerende stijl, communicatief vaardig, is in staat complexe beveiligingsproblemen uit te leggen aan niet technische belanghebbenden.

- Technische vaardigheden: de CISO heeft een goed begrip van de technologieën die worden gebruikt voor informatiebeveiliging en houdt deze kennis actueel.
- Organisatiesensitiviteit: de CISO is in staat om de beveiligingsbehoeften van de organisatie / instelling te begrijpen en om te zetten in een informatiebeveiligingsstrategie die aansluit bij en bijdraagt aan de bredere doelen en doelstellingen van de organisatie / instelling. Dit omvat ook het vermogen om effectief te communiceren met directie, bestuur en ander senior management binnen de organisatie / instelling.

Met wie werkt de CISO samen?
De CISO-functie werkt over het algemeen samen met in- en externe stakeholders zoals:

- Strategisch management
- Tactisch management
- Informatie- en/of IT-management, projectleiders, systeem- en data-architecten, functioneelbeheer
- Juridische zaken
- Control en auditors
- Functionaris Gegevensbescherming
- Externe (keten) partners en specialisten

Best practices
Deze beschrijving van de CISO-functie komt voort uit de workshop 'CISO as a Service' en zou daarmee ook herkenbaar moeten zijn voor de deelnemers. Uiteraard is het mogelijk om de beschrijving zo beknopt of juist uitgebreid als wenselijk te maken. Er zijn vast nog taken, verantwoordelijkheden en expertises aan te vullen en/of aan te scherpen. Het is ook mogelijk om gebruik te maken van beschrijvingen die al als best practices beschikbaar zijn zoals de Handreiking IB-functieprofiel Chief Information Security Officer (CISO) van de Informatiebeveiligingsdienst.[3]

[3] https://www.informatiebeveiligingsdienst.nl/product/handreiking-ciso-functieprofiel/