De rol van de **CISO** bij het opstellen, uitrollen en adopteren van de **cyberstrategie**

Onze expert over:

- de cruciale rol van de CISO binnen cyberrisicomanagement
- de vijf hoofdtaken van de CISO
- wat onderscheidt een goede CISO van een uitstekende?

Leestijd 12-15 MIN

AON
Empower Results®

De cruciale rol van de CISO binnen cyberrisicomanagement

Cyberweerbaarheid staat bij Nederlandse directies hoog op de agenda. Ze zien de noodzaak van goed cyberrisicomanagement en zijn bereid tijd en geld te investeren om hun organisatie weerbaar te maken. Dit gevoel wordt verder versterkt door het toenemende aantal cyberincidenten in het eerste half jaar van 2020. De Chief Information Security Officer (CISO) speelt een cruciale rol bij de ontwikkeling en uitrol van een cyberstrategie, waarbinnen het cyberrisico de grootste uitdaging is.

Non-stop op de hoogte zijn én blijven

Het bereiken van cyberweerbaarheid start bij het op de hoogte zijn - en blijven - van de ontwikkelingen van het continu evoluerende cyberrisico; buiten en binnen uw organisatie. Dat is waar het zwaartepunt van het werk van de CISO ligt. Hij of zij (hierna hij) is verantwoordelijk voor het gehele proces van informatie- en cyberbeveiliging in de organisatie en heeft daarmee een sleutelrol in de aanpak van cyberrisico's. De CISO verzamelt en analyseert alle data die een rol kunnen spelen bij cyberbedreigingen en vertaalt deze door naar advies en maatregelen. De CISO opereert dus op operationeel, tactisch én strategisch niveau en is een volwaardig gesprekspartner binnen alle afdelingen en niveaus van de organisatie.

Regie op interne en externe processen

Veel organisaties besteden hun IT- en cyberbeveiliging (deels) uit. Dit zorgt ervoor dat de CISO niet allen intern de regie moet voeren, maar ook op alle externe (IT-) partners, wat het monitoren en controleren bemoeilijkt. Vragen de risico's buiten de organisatie om dezelfde managementaanpak? En hoe zit het met toezicht op naleving van wet- en regelgeving door IT-partners? De CISO heeft immers minder zicht op de externe werkprocessen en minder directe invloed op de aanwezige beveiligingsmaatregelen.

Multidisciplinaire samenwerking

De CISO-rol vraagt daarom om een multidisciplinaire benadering en samenwerking. Om tot een succesvol, en breed gedragen, strategisch cyberbeleid te komen, moet de CISO samenwerken met HR, IT(-partners), legal counsels en de directie/ raad van bestuur. Als uw organisatie de financiële ruimte heeft, is het aan te raden om forensische experts en ethische hackers aan het team toe te voegen, om ook over detectieve en reactieve capaciteiten te beschikken. Hoe meer kennis en data, hoe effectiever het programma uiteindelijk wordt.

De rol van de CISO bij het opstellen, uitrollen en adopteren van de cyberstrategie

AON
Empower Results®

De 5 hoofdtaken van de CISO

De CISO bepaalt de strategie rondom alle informatiebeveiliging (waaronder cyber), zorgt ervoor dat deze strategie wordt gecommuniceerd, uitgerold en door alle stakeholders wordt gedragen. Dit laatste kan worden versterkt door de directie en andere afdelingen periodiek te laten zien wat er is voorkomen of beperkt aan cyberincidenten.

We kunnen de kerntaken van de CISO als volgt indelen.

De CISO:

1. is verantwoordelijk voor alles met betrekking tot cyberstrategie; opstellen, uitrollen, uitdragen en adoptie;
2. informeert de directie en andere stakeholders in heldere, concrete taal;
3. brengt de kroonjuwelen en risicobereidheid van de organisatie in kaart;
4. heeft een duidelijke visie omtrent informatiebeveiliging;
5. stelt een duidelijk stappenplan op met maatregelen en adviezen.

1 Inzichten en data verzamelen

Kritieke activa, systemen en operaties moeten identificeren. Beleid en procedures evalueren. Gebruikersgedrag van (externe) medewerkers onderzoeken. Kwetsbaarheden diagnosticeren en prioriteren. Cyberbeveiligingscontroles vergelijken met specifieke bedreigingen en governance en responsbereidheid beoordelen. Het is ‘slechts’ een greep uit de inzichten en data die tijdens de assessmentfase worden verzameld en geanalyseerd.

De absolute meerwaarde van goede assessments

Een goed assessment geeft de CISO de handvatten en vertelt hem wat al is geregeld en welk onderdeel nog aandacht behoeft. Gewapend met dit inzicht, kunnen de juiste beslissingen worden genomen en het cyberbeleid vorm worden gegeven. Dit moet ervoor zorgen dat het cyberrisico van de organisatie strategisch wordt beheerd, gebruikmakend van 1 van de 4 mogelijkheden:
risico vermijden, risico beperken, risico accepteren of het risico overdragen.

Om cyberrisico’s te kunnen managen, is een goed assessmenttraject dus van belang.
Een organisatie die het belang ziet van goed cyberrisicomanagement, is bereid enkele moeilijke vragen te beantwoorden:

- Wat zijn de belangrijkste activa die we moeten beschermen en de meest waarschijnlijke bedreigingen waarmee we worden geconfronteerd?
- Hoe brengen we organisatiedoelen in evenwicht met cyberrisico’s?
- Hoe staat het met onze beveiliging en controles?
- Hoe gebruiken onze mensen onze technologie en data?
- Hoe goed begrijpen onze mensen bestaand beleid en procedures, leven ze deze na en zijn deze bruikbaar in de dagelijkse praktijk?
- Kunnen we aan aandeelhouders, toezichthouders en rechtspersonen laten zien dat we due diligence hebben uitgevoerd om onze cyberweerbaarheid veilig te stellen?
- Hoe goed communiceren we intern met betrekking tot cyberrisico’s, mitigatieactiviteiten en cyberincidenten en respons?
- Heeft het management eenzelfde beeld van wat cyber is en wat cyberweerbaarheid is?
- Waar moet ons budget aan worden besteed?

AON
Empower Results®

2 In **duidelijke** en **heldere taal communiceren**

Het cyberprogramma heeft enkel kans van slagen als de directie en andere belangrijke stakeholders dit steunen. De manieren van communiceren is voor een CISO daarom enorm belangrijk. Hij moet in duidelijke, begrijpelijke taal kunnen uitleggen wat de dreigingen zijn en wat het beste is voor de organisatie. Wat is het juiste beveiligingsniveau? Hoeveel geld heeft hij nodig en waarom is dat bedrag realistisch? Is er genoeg expertise in huis of moeten er externen worden ingehuurd? Wanneer het beleid eenmaal is geaccepteerd, is het zaak om de stakeholders periodiek op de hoogte te houden van het functioneren van het gekozen beleid.

AON
Empower Results®

3 De kroonjuwelen en risicobereidheid van de organisatie

Zonder te weten waar de organisatie het hardst geraakt kan worden in haar continuïteit, heeft beleid schrijven geen zin. In de assessmentfase wordt daarom goed gekeken naar wat de kroonjuwelen zijn die koste wat kost beschermd moeten worden. Een tweede vraag die de CISO aan de directie moet stellen is ‘Hoeveel risico wil je nemen’? Een gezonde risk appetite is prima, maar sommige risico’s wil je als organisatie echt niet nemen. De CISO zal daarom goed en inhoudelijk gemotiveerd moeten aangeven wat wel en wat geen gezonde risicobereidheid is.

4 Duidelijke visie omtrent informatiebeveiliging

Wanneer de CISO de juiste mensen om zich heen heeft verzameld en via datavergaring en assessments alle benodigde input heeft verzameld, is het tijd voor de vervolgstap: cyberstrategie. Maar alvorens hieraan te beginnen, is het zaak een visie te formuleren. Deze visie moet passen bij de organisatiedoelstellingen,cultuur, risicobereidheid, financiële positie en haalbaarheid. Durf breed en vooruitstrevend te denken, maar zorg dat alles op relatief korte termijn is te verwezenlijken en schakel altijd externe expertise in wanneer u denkt dat nodig te hebben.

"Afhankelijk van de samenstelling van de organisatie heeft de CISO, voordat hij start met beleid schrijven, een team van specialisten verzameld. Denk aan IT, HR, Legal, Risk, ethische hackers, forensische experts, specialisten op preventie, detectie en incident response."

AON
Empower Results®

5 Stappenplan opstellen met maatregelen en adviezen

Om ervoor te zorgen dat iedereen tijdens een cyberincident zijn of haar rol goed kent en deze naar behoren uitvoert, is het zaak om alles helder en begrijpelijk vast te leggen in een stappenplan. Wanneer de organisatie dan geconfronteerd met een dreiging of crisis kan iedereen terugvallen op dit plan.

Wij zetten negen acties op een rij die u kunt gebruiken om het cyberbeleid van uw bedrijf succesvol te implementeren.

AON
Empower Results®

Wat onderscheid een goede CISO van een uitstekende

Het functioneren van de CISO is in elke situatie en elke organisatie afhankelijk van tig factoren. Toch waagt Ralf Willems, Managing Consultant bij Aon's Cyber Solutions en voormalig CISO, zich aan een antwoord: “Een uitstekende CISO is iemand is die voortdurend in control is en helder communiceert. Iedereen snapt wat zijn rol is, waarom die rol er is en wat het oplevert als hij zich aan die rol houdt.”

Een niet goed-functionerende CISO wordt ook snel zichtbaar. “Als er te weinig of verkeerde maatregelen zijn geïmplementeerd is het wachten op een cyberincident dat de organisatie hard kan raken. Een cyberaanval is niet altijd tastbaar, terwijl je wel vraagt om investeringen in securitymaatregelen. Afhankelijk van de investering zal de directie vragen: Wat levert het ons op? Maak dit inzichtelijk. Zorg dat u een CISO bent of wordt, waar mensen aan vragen ‘Wat hebben we de afgelopen periode voorkomen?’, zodat u kunt antwoorden ‘We hebben vandaag 58 aanvallen afgewend!’.

Ralf Willems
+31 (0)10 448 77 72
ralf.willems@aon.nl

Aon
Empower Results®