De vitale rol van de CISO

Cybercriminaliteit is een probleem voor de hele organisatie

Cyberrisico's behoeven inmiddels geen introductie meer. Omdat cyberveiligheid een organisatiebrede uitdaging is en een integrale aanpak vraagt, hebben veel organisaties inmiddels een Chief Information Security Officer (of een 'light-variant') in dienst. Hij of zij is verantwoordelijk voor het opzetten van een cyberstrategie en het adviseren, meenemen en meekrijgen van de directie, stakeholders en overige medewerkers. De CISO heeft daarmee een sleutelrol in de omgang met cyberrisico's.

Cyberveiligheid ligt maar voor een klein deel bij de IT-afdeling

Veel organisaties pakken cyberrisico's onvoldoende aan, omdat zij denken dat de (externe) IT-beheerder zorgt dat hen niets overkomt. Zij vergeten dat deze IT-beheerder er vooral voor zorgt dat de systemen werken. Hij is niet verantwoordelijk voor afspraken met leveranciers en klanten aangaande het verwerken van gegevens. Hij is ook niet verantwoordelijk voor de processen die u heeft ingeregeld en hoe uw mensen met gegevens omgaan. De CISO moet er daarom voor zorgen dat de directie hiervan is doordrongen en begrijpt dat cyberveiligheid een uitdaging is voor de gehele organisatie.

Medewerkers bewust maken van cyberrisico's

Veel organisaties beseffen niet wie de zwakste schakel is als het gaat om cyberincidenten: de medewerker. In de praktijk blijkt dat onwetende, nalatige of kwaadwillende medewerkers de oorzaak zijn van bijna driekwart van de cyberincidenten. Dus zonder bewuste medewerkers geen veilige organisatie. De rol van de CISO is ook hier helder: zorg dat echt iedereen in de organisatie voldoende aandacht heeft voor cyberrisico's. Draag het belang en de urgentie uit, welke toegangsrechten hebben uw medewerkers en worden deze periodiek gecontroleerd. Kijk ook of de rechten van medewerkers niet beperkt kunnen worden, zonder dat hun werk daarmee onmogelijk wordt. Zo verkleint de CISO het 'insider risico' en de kans op een cyberincident.

"Zonder bewuste medewerkers geen veilige organisatie. De CISO moet ervoor zorgen dat iedereen in de organisatie voldoende aandacht heeft voor cyberrisico's

AON
Empower Results®

Directie en stakeholders overtuigen

De CISO staat voor de zware taak cyberbewustzijn te creëren in alle lagen van de organisatie. Wat het extra lastig maakt, is dat cyberveiligheid niet vanzelfsprekend direct zichtbaar is, maar wel een hoop tijd en geld kost. De CISO moet de directie daarom in duidelijke, begrijpelijke taal kunnen uitleggen wat de dreigingen zijn en wat het beste is voor de organisatie. Wat is het juiste beveiligingsniveau? Wat is de risicobereidheid van de directie? Hoeveel geld heeft hij nodig en waarom is dat bedrag realistisch? En hoe intensief moeten medewerkers worden getraind en geïnformeerd?

Werk een cyberbeleid uit en creëer draagvlak

Wanneer deze en andere sleutelvragen zijn beantwoord, kan de CISO aan de slag met een cyberbeleid dat gebaseerd is op preventie, detectie en reactie. Het is belangrijk dat de CISO de technische maatregelen van dit beleid bespreekt met de IT-afdeling en het beleid op een toegankelijke manier deelt met de rest van de organisatie. Alleen zo kan het benodigde cyberbewustzijn ontstaan. Wanneer de CISO goed functioneert, is hij of zij een volwaardig gesprekspartner binnen alle afdelingen en niveaus van de organisatie. En dat is nodig, want informatiebeveiliging is een organisatievraagstuk dat om een integrale aanpak vraagt.

Zelf aan de slag met een cyberstrategie?

Wilt u weten hoe u als CISO een cyberstrategie uitstippelt? Aon's cyberspecialisten helpen u in elke fase van de strategieontwikkeling met advies op maat.

Wij helpen u graag succesvol te ondernemen.

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

Empower Results®

20.081-01-CISO-Awareness-20200817-2