Auteur: André Beerten is sinds 2015 zelfstandig adviseur informatiebeveiliging en ook associate bij Verdonck, Klooster en Associates. Hij werkte eerder bij KPN, Getronics en het Groene Hartziekenhuis. Hij is te bereiken onder: andre@octopus-ib.nl of via LinkedIn (1)

De falende CISO

'Hoe we voortmodderen'

Een niet aflatende stroom berichten in de media vertelt ons dat de beveiliging van informatie te wensen overlaat en dat we de strijd tegen de digitale onveiligheid dreigen te verliezen. Voorkomende incidenten onderstrepen deze claim met hun oplopende frequentie en de ernst van de gebeurtenissen. Hoe komt dit en wat is de rol van informatiebeveiligers, (C)ISO's, hierin? Wij zijn immers de professionals, de mannen en vrouwen met security kennis en de fraaie certificaten. Toch!?

We kunnen al lang niet meer wijzen naar de techniek, want er zijn al een hele tijd volop deugdelijke middelen beschikbaar. Wel kunnen we wijzen naar directies en managers, maar die hebben óns, de (C)ISO's, nodig om de beveiliging te snappen en de juiste dingen te doen.

Een onderzoek van CIP (2) (zie kader) schetst geen al te vrolijk beeld van onze beroepsgroep. Wat ik zélf waarneem: we zijn vaak oud, wel al lang in het IT-vak werkzaam, maar nog maar kort (C)ISO: zonder middelen, zonder macht, zonder personeel, soms werkend in deeltijd, veelal met te weinig opleiding voor de specifieke rol en we kijken al uit naar ons pensioen.

Dit is de gemiddelde CISO
Ondanks het gegeven dat de gemiddelde leeftijd van de CISO 55 jaar bedraagt, is de ervaring in de functie van CISO relatief kort. 40% geeft aan slechts 0 tot 2 jaar werkervaring te hebben en nog eens 40% 3 tot 5 jaar.

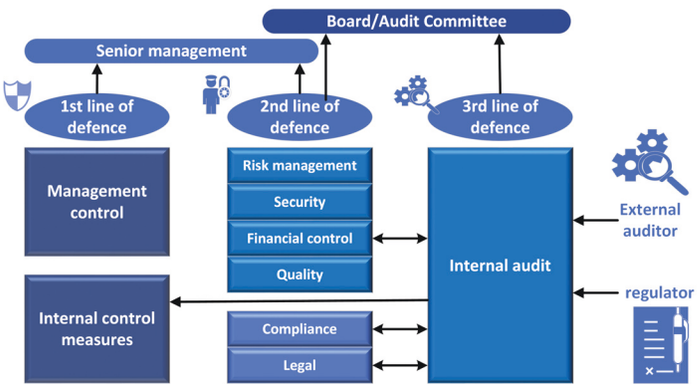
De jongeren moeten het beter gaan doen, maar zij krijgen als vorming het trio CISSP-CISM-CISA opgediend, recht uit de Amerikaanse keuken, niet gericht op je dagelijkse praktijk (met BIO en NEN), maar meer gericht op carrièreperspectief en een mooie uitstraling van het Curriculum Vitae.

Het probleem

Voor mij (en vele anderen die ik spreek) is het zonneklaar dat we falen. We krijgen niet voor elkaar wat we beogen. We slagen er niet in (met name in de non-profit) om onze broodheren op een aantoonbaar volwassenheidsniveau te krijgen. Ondertussen drijft onze digitale veiligheid vooral op de professionaliteit en inzet van IT-afdelingen en andere betrokken ondersteuners.

Dat leidt niet alleen tot vage en ondermaatse informatiebeveiliging, maar ook tot persoonlijke problemen. Teleurstelling en frustratie liggen voor de (C)ISO op de loer. Soms neemt het zelfs zeer ernstige vormen aan, denk aan burn-outs. Voor veel collega's geldt *'slikken en doorploeteren'*, want vooral in onzekere tijden (zoals er nu weer dreigen) moet je blij zijn dat je een baan hebt. Allereerst wens ik al deze mensen sterkte toe, maar we moeten vooral ook kritisch naar onszelf kijken: *waarom krijgen we zo weinig voor elkaar en welke fouten maken we?*

Ons grootste probleem is mijns inziens dat we (de tweede lijn in informatiebeveiliging - zie figuur 1) blijven proberen *'het probleem'* op te lossen. We maken informatiebeveiliging tot ónze verantwoordelijkheid of hebben ons die verantwoordelijkheid laten opdringen, gaan daarin mee en we zorgen er daarmee ook nog eens voor dat de hele organisatie dat ook zo ziet. We sluiten onszelf op in de welbekende ivoren toren en verstoppen ons achter giga-spreadsheets, onleesbare beleidsstukken en lange e-mails. En áls we dan eens echte mensen spreken, gaan we uitleggen in plaats van luisteren.



Figuur 1 bron: IIA website (3).

Wij denken voortdurend te moeten vertellen *wat* 'zij' moeten doen. We vergeten of kunnen daarbij niet aangeven welk doel bereikt moet worden en al helemaal niet hóe dat doel bereikt kan worden. En dán vinden we het gek dat we geen duidelijke antwoorden krijgen, dat onze opdrachten niet uitgevoerd of 'vergeten' worden.

Als we een vraag krijgen van de business, een roep om ondersteuning, dan nemen we maar wat graag het probleem over van de probleemeigenaar. Wij weten immers wat er moet gebeuren. We nemen het initiatief en de verantwoordelijkheid weg bij diegene(n) waar dat thuishoort. We trainen zo de organisatie om óns het te laten doen. Wij trainen ze om achterover te leunen. Onze adviezen worden uitgevoerd, wij zetten een vinkje en vervolgens wordt de bal weer teruggelegd bij ons. De eerste lijn wacht weer rustig af.

De weg naar een succesvolle aanpak

Er is een middel dat de weg wijst naar een succesvolle aanpak, een adequate invulling van governance vanuit de juiste verantwoordelijkheid (de eerste lijn) en dat is het ISMS in de ISO27001/NEN7510, waarmee governance echt vorm kan worden gegeven.

Helaas slaan we 'dat boekje' meestal over. We pakken dat andere 'boekje' waarin alleen voorbeelden en suggesties staan, de ISO27002, want dat is veel handiger, daar staat gewoon in *wat* je moet doen. Althans dat denken we en als het zo uitkomt dan pakken we het liefst een baseline, nóg simpeler (denken we), want met de BIO ben je sneller klaar.

Er is, door de komst van BIO, flink gewied in baselineland en het moet gezegd: die geeft het ISMS een plek, maar dan wel helemaal op het eind, in de paragraaf 'Naleving' onder 18.2.1.1. Alsof het bijna vergeten was. Dat is geen aanmoediging om die oproep serieus te nemen en er energie in te steken terwijl 'beheersing van risico's', CONTROL dus, het doel moet zijn: het gaat immers om de beheersing van risico's, niet om het verzamelen van vinkjes... *toch*?

Geld en macht

In de bijna zeldzame situaties dat we een werkend ISMS mogen inrichten en ook moeten onderhouden, dan behoren daar ook middelen bij. Daar heb ik in mijn praktijk nog maar weinig voorbeelden van gezien. In het Angelsaksische model lijkt dat wél normaal, daarvoor mag je dan zelfs (soms) in de 'board' optreden.

Maar bij ons? Ik ken vooral (C)ISO's met informele invloed en net genoeg budget om het NEN7510-boekje te kopen en dat alleen in goede tijden. Macht ligt vaak bij de bestuurder en in de lijn, maar je moet wel volledig vrij kunnen rapporteren over risico's naar de bestuurder. En dat zonder tussenkomst van de 'kleilaag' die dingen liever wat 'politieker' formuleert.

Communicatie

Verhalen over hakkelende, onzekere presentaties voor het management kennen we allemaal. Ook ik stond er vaak met klotsende oksels. Dat helpt je natuurlijk niet verder, maar is niet per sé het probleem. Veeleer gaat het over de problematische vorm en inhoud van ons verhaal: veel techniek, te veel details, te veel emotie en te weinig oog voor waar de business echt op aanslaat. We beginnen bovendien vaak met een heel analytisch verhaal en komen pas op het eind toe aan de kernvraag. Dan zijn de meeste toehoorders al afgehaakt.

Communicatie gaat twee kanten op en we vragen ook niet genoeg waar de directie, de business nu echt van wakker ligt. Wij denken immers meestal vanuit de baseline, niet vanuit wat nodig of wenselijk is (vanuit wat de organisatie wil dus).

Ter verdediging

Wij (C)ISO's zijn meestal de mensen met een reeks van subtitels achter hun naam, de CISSP- en CISM- oorkondes. Biedt ons dat steun, hebben we daar ook echt iets aan? Om voor een baan in de informatiebeveiliging in aanmerking te komen, wordt vanwege onbenul bij bemiddelaars en HR vaak alleen naar deze 'stickertjes' gekeken. Maar kun je er ook echt iets mee in je dagelijkse werk?
De vraag stellen is hem beantwoorden: beide opleidingen grossieren in schema's, tabellen en wijsheden uit allerlei verschillende culturen en organisatietypen. Maar voor jouw werkomgeving wordt er geen passend model geboden, geen diagram, best practice of methode die bruikbaar is in de dagelijkse praktijk.

De ambachtelijke kant van je vak, de confrontatie met jouw organisatie en zijn eigenaardigheden en belemmeringen, die komt niet aan de orde. Deze opleidingen laten je achter met een dik boek en een mooi papiertje (en embleem voor LinkedIn). Dit zonder handvatten voor praktische toepassing van de geboden stof en oplossing voor het probleem. Voor het werk als (C)ISO zijn veel meer competenties nodig dan wat een dergelijke certificering biedt.

Het is niet iedereen gegeven weet te hebben van én techniek én organisatie én cultuur én ook nog van risicobeheersing. Het vergt een schaap met vijf poten om dat allemaal in de juiste samenhang te kunnen aanpakken. Het opbouwen van de juiste allianties in de organisatie en het

Van de redacteur

Wellicht kun je je niet helemaal vinden in de opvattingen van de auteur en wil je reageren. Dat kan uiteraard direct naar de auteur, maar we denken dat het interessanter kan worden als de discussie wat breder kan worden getrokken. Reageer daarom via de link naar de LinkedIn-pagina van het PvIB: https://www.linkedin.com/company/pvib/ of scan de QR-code.

- *Herken je het ook - of juist niet - dat je de verantwoordelijkheid voor informatieveiligheid krijgt toegeschoven, maar dat je niet gefaciliteerd wordt in zeggenschap (macht) noch in middelen om deze taak te kunnen uitvoeren?*

- *Herken je het ook - of juist niet - dat onze opleidingen te veel gericht zijn op het dikke boek en de mooie titel en te weinig op ter zake dienende competentie-ontwikkeling?*

- *Ervaar je ook dat binnen jouw organisatie geklaagd wordt dat wij te weinig invulling geven aan de werkelijke wensen/behoeften van de organisatie? Of heb jij juist goede oplossingen weten te realiseren, zo ja welke/hoe, zodat je goed afgestemd bent op het management en kader?*

Laat van je horen!

organiseren van competente ondersteuning is dan heel belangrijk. Dat is niet altijd mogelijk, nooit eenvoudig, maar wel van essentieel belang voor succes.

Conclusie

Is het dan allemaal ónze schuld? Nou niet helemaal, maar we spelen mijns inziens wel een hoofdrol in het falen van informatiebeveiliging. Als we echt het verschil willen maken dan moeten we heel kritisch in de spiegel kijken. We moeten beter leren omgaan met mens en organisatie, we moeten werken aan governance met een goed ISMS én we moeten bereid zijn de opdracht terug te geven als niet aan de randvoorwaarden wordt voldaan.

We moeten weigeren boven onze macht te functioneren. We moeten weigeren om met onvoldoende middelen het onmogelijke doel te bereiken. We moeten onszelf verder scholen om beter die rol van het schaap met de vijf poten te kunnen invullen. Deze aanpak vergt persoonlijke moed, maar zonder moed blijven we doormodderen. Zonder lef geen leven!

Referenties

(1) https://www.linkedin.com/in/andrebeerten/
(2) https://ib-p.nl/download/cip-enquete-onder-overheids-cisos/
(3) https://www.iia.org.uk/threelinesofdefence