Cybersecurity hoort niet thuis in de directiekamer

Auteur: Hugo Leisink
e-mail: hugo@leisink.net
www: https://www.ravib.nl/

25 juli 2018

Om informatiebeveiliging tot een succes te kunnen maken, is het belangrijk om het onderwerp op een juiste manier binnen de directiekamer te introduceren. Beperk je daarbij tot de strategische zaken, namelijk informatie als productiefactor, de waarde van informatie voor de organisatie en de noodzaak om sommige informatie te beveiligen. Bespreek de strategische zaken rondom informatie, zoals beheer, de beveiliging, privacy, et cetera, in een gesprek met de informatiemanager, de ICT- manager en de privacy officer. Laat al deze functies direct onder de directie vallen om de invulling ervan zo efficiënt mogelijk te kunnen maken.

Hoewel cybersecurity belangrijk is, wil het helaas niet voor iedere organisatie lukken om dit onderwerp tot een succes te maken. Bij veel organisaties is cybersecurity beperkt tot vooral technische maatregelen. Securityspecialisten die het onderwerp onder de aandacht willen brengen van directieleden, ervaren vaak genoeg desinteresse of zelfs tegenwerking. De reden hiervoor is dat naar mijn idee het onderwerp verkeerd aangepakt wordt. Dit artikel beschrijft wat er fout gaat en hoe het onderwerp op de juiste manier in de directiekamer kan worden geïntroduceerd.

Informatie als productiefactor

In economische wetenschappen wordt gesproken over verschillende productiefactoren: natuur, arbeid en kapitaal. In de praktijk betekent dat grondstoffen en machines om producten mee te fabriceren, middelen om een dienst aan te bieden, personeel voor geestelijke en fysieke arbeid en financiële middelen om dit alles te bekostigen. Voor al deze zaken geldt, dat als je ze volledig wegneemt, een organisatie een groot probleem heeft. Kans op faillissement is dan zeker aanwezig.

Daarom hebben organisaties vaak een manager aangesteld om alles rondom zo'n onderdeel te organiseren. Een manager voor productie, logistiek, voorraad, ICT, et cetera, een P&O manager voor de medewerkers en een CFO voor de financiën.

Maar hoe zit het eigenlijk met 'informatie'? Organisaties maken er veel gebruik van en zijn er ook vaak van afhankelijk. Natuurlijk gebruikten organisaties vroeger ook informatie, maar zonder een computer kost het verwerken van informatie veel meer tijd en moeite. Door de komst van de computer is het gebruik van informatie geëxplodeerd. Maar wat nu als alle informatie binnen een organisatie wordt weggenomen? De e-mailserver, de fileserver, de boekhouding, het CRM-systeem, de personeelsdossiers, alles leeg of weg. Heeft een organisatie dan niet ook een groot probleem? Is kans op faillissement dan niet ook aanwezig? We kunnen dus eigenlijk wel stellen dat, gezien de omvang van het gebruik van informatie en de afhankelijkheid daarvan voor veel organisaties, informatie een op zichzelf staande productiefactor is. Maar wie managet al die bedrijfsinformatie? Een organisatie die goed omgaat met bedrijfsinformatie heeft daarvoor een informatiemanager. Maar neemt uw organisatie het vak van informatiemanagement wel serieus?

De positie van de informatiemanager

Zoals ik eerder heb beschreven[1], is zicht en grip op informatie een belangrijke voorwaarde voor zicht en grip op informatiebeveiliging. Het beheren van informatie binnen een organisatie kost dusdanig veel tijd dat daarvoor het beste een aparte manager kan worden aangesteld. Echter, veel organisaties die een informatiemanager hebben aangesteld, plaatsen deze functie onder de ICT-manager. Dit is een totaal verkeerde positie. Voor de argumentatie hiertoe nemen we personeel als voorbeeld. Waar het kunnen bieden van een dienst of het leveren van producten het doel is, zijn medewerkers een middel. Waar het kunnen laten werken van de medewerkers het doel is, zijn bedrijfspanden en werkplekken het middel. Voor de medewerkers hebben organisaties meestal een P&O- manager en voor de panden en de werkplekken een manager facilitaire zaken. Als je zou voorstellen om de P&O-manager onder de manager facilitaire zaken te plaatsen, vind je denk ik niet veel medestanders. De manager voor het doel en die voor het middel horen voor een goede balans tussen vraag en aanbod naast elkaar te staan, niet boven of onder de ander.

	Personeel	**Informatie**
Doel	P&O-manager	Informatie-manager
Middel	Manager facilitair	ICT-manager

Maar hoe zit het op ICT-gebied? Waar het verwerken van informatie het doel is, is ICT het middel. ICT bestaat binnen een organisatie bij de gratie van de behoefte om informatie te verwerken. Organisaties die dit onderwerp serieus nemen, hebben voor het organiseren van alle bedrijfsinformatie een informatiemanager aangesteld. Voor het beheren van alle ICT-middelen hebben de meeste organisaties een ICT-manager. Waar het mis gaat, is dat zij vaak de manager die het doel managet, plaatsen onder de manager die de middelen daartoe managet. Waar deze constructie voor personeelszaken dus bijzonder vreemd zou zijn, is het voor informatie blijkbaar wel acceptabel. Om ook hier een gezonde balans tussen vraag en aanbod te krijgen en de organisatie te kunnen laten groeien in haar volwassenheid in de omgang met bedrijfsinformatie, dienen deze managers naast elkaar te staan.

Informatie als onderwerp in de directiekamer

Informatie zien als een aparte productiefactor en daar binnen de organisatie op een goede manier mee omgaan, is een belangrijke eerste stap om informatiebeveiliging tot een succes te maken binnen een organisatie. Ga met directieleden het gesprek aan over bedrijfsinformatie en het belang van sommige bedrijfsinformatie voor de organisatie. Laat directieleden inzien dat informatie gezien de omvang, de afhankelijkheid en alle ontwikkelingen op dat vlak echt een productiefactor is. Laat directieleden zelf tot de

[1] *https://www.ravib.nl/informatiemanagement*

conclusie komen dat sommige informatie het waard is om goed te beveiligen. Het is beter om het onderwerp zo aan te pakken dat de directieleden informatiebeveiliging bij de CISO komen halen, dan dat de CISO dit onderwerp moet brengen.

Informatie als productiefactor, de noodzaak om belangrijke informatie te beveiligen en de middelen die daarvoor nodig zijn, is het enige dat binnen de directiekamer besproken hoeft te worden. Informatiebeveiliging zelf is namelijk vooral een tactisch en operationeel onderwerp. Het is alleen een strategisch onderwerp als een organisatie informatiebeveiliging als concurrentiepositie wil gebruiken, maar dat laten we voor nu buiten beschouwing. Ik denk dat het niet efficiënt is om informatiebeveiliging te bespreken in een één-op-één gesprek tussen de CISO en een directielid. Wat naar mijn idee een betere aanpak is, is om 'informatie' als onderwerp te gebruiken. Betrek bij dat onderwerp daarom ook de informatiemanager, de ICT-manager en de privacy officer. Op die manier kan er beter zicht en grip verkregen worden op deze productiefactor in brede zin. Beveiliging is namelijk minder efficiënt als je er niet de noodzaak, de technische middelen en de privacy-zaken bij betrekt.

Ik gebruik in dit artikel bewust 'informatiebeveiliging' in plaats van 'cybersecurity'. De term 'cyber' is namelijk een erg ruim begrip en daardoor eigenlijk nietszeggend. Wil je het onderwerp makkelijk bespreekbaar kunnen maken met collega's die niet goed inhoudelijk bekend zijn met dat onderwerp, dan kan het mogelijk beter zijn om duidelijk te benoemen wat het is: het beveiligen van (bedrijfs)informatie, dus informatiebeveiliging. Ik doe hiermee geen poging om het woord 'cybersecurity' uit te bannen. Als voor jouw organisatie deze wat hippere term beter werkt dan de oude, misschien wat stoffige, term 'informatiebeveiliging', dan is dat prima. Wat ik hier alleen mee wil zeggen, is dat je je goed moet realiseren dat managers vaak geen techneuten zijn en ze dus mogelijk onvoldoende zicht hebben op de hele ICT-wereld. Door duidelijk aan te geven waar je het over hebt en wat je van ze verlangt, loop je minder kans dat de directie geen interesse zal tonen in het onderwerp.

Samenvattend

Om informatiebeveiliging tot een succes te kunnen maken, is het belangrijk om het onderwerp op een juiste manier binnen de directiekamer te introduceren. Beperk je daarbij tot de strategische zaken, namelijk informatie als productiefactor, de waarde van informatie voor de organisatie en de noodzaak om sommige informatie te beveiligen. Bespreek de strategische zaken rondom informatie, zoals beheer, de beveiliging, privacy, et cetera, in een gesprek met de informatiemanager, de ICT- manager en de privacy officer. Laat al deze functies direct onder de directie vallen om de invulling ervan zo efficiënt mogelijk te kunnen maken.

Over de auteur

Hugo Leisink is senior adviseur bij het Nationaal Cyber Security Centrum. Hij is bereikbaar via hugo@leisink.net. Dit artikel is op persoonlijke titel geschreven.