Drs. P.W.A. Kasteleyn EMFC RC

Wikileaks en de controller

Wikileaks levert ons al weer enkele maanden interessante informatie over het geheime berichtenverkeer vanaf de ambassades van de Verenigde Staten. Eerder heeft WikiLeaks vertrouwelijke documenten gepubliceerd van de banken Julius Baer, Kaupthing Bank en Barclays Bank en bijvoorbeeld over de dumping van chemisch afval door Trafigura. Welke lessen kan de controller hieruit trekken?

1. Zorg voor een goede informatiebeveiliging

Hoe is het mogelijk dat een gewone soldaat toegang heeft tot 250.000 geheime documenten en deze ook nog weet te ontvreemden? Maar tot welke informatie hebben de medewerkers bij uw bedrijf toegang? Managementrapportages, gedeelde netwerkschijven, ERP-systemen, intranetsites en e-mails bevatten een schat aan informatie. Veel ondernemingen kennen autorisaties aan medewerkers toe om toegang tot bepaalde informatie te kunnen verkrijgen, of juist informatie af te schermen. Dit gebeurt echter veelal op basis van de tekentafel: welke (groepen) medewerkers mogen toegang tot de informatie hebben? Maar hoe werkt dit autorisatiebeleid in de praktijk? Hoe zijn de autorisaties voor bijvoorbeeld ICT-medewerkers geregeld (veel ICT-ers hebben toegang tot meer informatie dan noodzakelijk is voor de uitoefening van hun functie)? Naast autorisaties kunnen fysieke beveiligingen helpen, zoals de uitschakeling van USB-poorten of de afscherming van de mogelijkheid een cd of dvd te branden.

2. Werk aan een open cultuur en ontwikkel een klokkenluidersregeling

De doelstelling van Wikileaks is niet verkeerd: het is een plek waarop klokkenluiders anoniem documenten kunnen laten plaatsen om misstanden aan de kaak te stellen. Zo ver zou het echter niet moeten komen. Medewerkers moeten misstanden binnen de eigen organisatie kunnen melden. Om dit te bereiken is een open cultuur nodig, waarbinnen integer handelen, het uiten van kritiek, voorbeeldgedrag en het aanspreken van elkaar worden gestimuleerd en gewaardeerd. Toch blijft intern klokkenluiden omstreden. Met name als de niet-integere handelingen betrekking hebben op de directie of bestuurders is een onafhankelijke behandeling van de klacht lastig. Immers de directie moet in dat geval een oordeel vormen over het eigen handelen. Een klokkenluidersregeling biedt mogelijk een oplossing. De regeling moet bevorderen dat (vermeende) misstanden worden gemeld en dat een vertrouwenspersoon deze kan (laten) onderzoeken en desgewenst eventuele maatregelen kan nemen. De boodschapper van het nieuws moet op basis van een melding niet worden bestraft, noch door de werkgever, noch door collega's of anderen.

3. Wees zelf transparant

Alle informatie die je zelf naar buiten brengt kan niet meer gelekt worden. De onderneming heeft voldoende middelen om transparant te zijn, zoals het jaarverslag, de website, persberichten en informatiemails. Het is van belang niet alleen de successen te communiceren, maar ook onregelmatigheden, mislukkingen en knelpunten. Algemeen aanvaarde standaarden als de Global Reporting Initiative en ISO 26000 kunnen bij de (maatschappelijke) verslaglegging helpen.

4. Bereid een draaiboek voor

Een gedegen voorbereiding helpt. Als er informatie naar buiten komt zoals via Wikileaks, de pers of Twitter moet de onderneming een draaiboek hebben klaarliggen. Dit draaiboek bevat de noodzakelijke maatregelen op het gebied van interne en externe communicatie, een crisisteam en de rolverdeling, de eventuele bescherming van de klokkenluider, het aanpakken van de misstand, het dichten van het informatielek en mogelijke juridische maatregelen.

Men kan zich afvagen of deze Wikileaks-lessen tot de taak van de controller behoren. Ik denk van wel. Het valt onder risicomanagement waaraan veel controllers een bijdrage leveren. Bij grotere bedrijven zijn de risico's van netwerken als Wikileaks zeker aanwezig. Bij kleinere bedrijven hebben de informatierisico's eerder betrekking op het doorgeven van informatie aan de concurrent. Misschien minder schadelijk voor de reputatie, maar des te meer voor de toekomst van de onderneming.

Column

2011-029