Invloed technologische ontwikkelingen op kleine IAF’s

12 oktober 2017

De PAS Commissie van het IIA en de Ledengroep Intern en Overheidsaccountants (LIO) van het NBA organiseren regelmatig gezamenlijk een verdiepingssessie voor kleine internal auditafdelingen. Op 12 oktober 2017 stond het onderwerp *‘Invloed technologische ontwikkelingen op kleine IAF’s’* op het programma.

Ongeveer 40 auditors van kleine en middelgrote auditdiensten kwamen bijeen om van gedachten te wisselen over de technologische ontwikkelingen en cybersecurity. De aandacht ging vooral uit naar de gevolgen van technologische ontwikkelingen voor (kleine) IAF's en welke rol audit hierin moet pakken. Verschillende specialisten deelden hun visie.

Technnologische ontwikkelingen en tools

Arjan ten Cate en Bas Sluijsmans van Deloitte Risk Advisory gingen in op de technologische ontwikkelingen en de tools die beschikbaar zijn om hier analyses op los te laten. Allereerst liet Arjan de aanwezigen aangeven op welke termijn zij een forse disrupty verwachten als gevolg van technologische ontwikkelingen. De meeste aanwezigen hadden het idee dat dit binnen enkele jaren zal gebeuren. Deze stemming werd gevolgd door voorbeelden van technieken die een wezenlijk verandering veroorzaken. Amazon.go, een winkel in de VS zonder personeel, trok hierin veel aandacht.

Hierna nam Bas het over en liet zien hoe gigantische bestanden met bijvoorbeeld e-mails geanalyseerd kunnen worden. Dit is een voorbeeld van nieuwe technologieën die gebruikt kunnen worden om analyses uit te voeren om bijvoorbeeld fraude op een doeltreffende manier zichtbaar te maken.

Hoe vinden hacks plaats?

Na een korte (netwerk)pauze nam Michiel van Veen van KPMG Cyber het presentatiestokje over. Hij gaf de deelnemers inzicht in de wijze waarop hacks plaatsvinden (inclusief een live demonstratie) en hoe eenvoudig dit eigenlijk is. Het bleek dat het openen van links in een e-mail echt gevaarlijk kan zijn. Daarnaast heeft hij een aantal praktische tips gegeven hoe je als (kleine) internal auditafdeling met cybersecurity kunt omgaan. Zorg vooral voor bewustzijn van de risico's. Velen zullen hiermee te maken krijgen, Absolute zekerheid om dit te voorkomen is niet mogelijk, dus is een plan hoe hiermee om te gaan essentieel. Dit zijn aspecten waar audit een bepalende rol kan vervullen.

Gevolgen hacks en ransomware

Lars Jacobs van KPMG Cyber liet zien wat de gevolgen van een hack of ransomware/malware kunnen zijn. Als organisaties hier niet op voorbereid zijn, kan de schade veel groter uitvallen dan met een goed plan. Uiteraard werden deze presentaties opgeluisterd met meer praktijk cases die meteen praktische handvatten gaven om mee aan de slag te gaan.