Crowe

IT & Cybersecurity als onderdeel van de accountantscontrole

Is er voor uw organisatie jaarlijks sprake van een accountantscontrole? Dan biedt dit u waardevolle inzichten in de mate van risicobeheersing binnen uw organisatie. Dat gaat veel verder dan alleen de financiële bedrijfsvoering.

Tegenwoordig zijn de bedrijfsprocessen van een organisatie grotendeels tot zelfs volledig gedigitaliseerd. Daardoor is de rol van IT enorm gegroeid binnen de organisatie. Sterker nog, we zijn ervan afhankelijk bij de uitvoering van ons dagelijkse werk.

Wanneer de IT-omgeving faalt, door bijvoorbeeld een cyberaanval, dan heeft dit een groot effect op de operatie en continuïteit van de organisatie. Sterker nog, als applicaties en data niet hersteld kunnen worden dan kan dit leiden tot ernstige financiële schade of zelfs een faillissement. Finance en IT staan daardoor dichter bij elkaar dan ooit. Onlosmakelijk met elkaar verbonden, beter gezegd.

Onderzoeksmethode
Bij een accountantscontrole door Crowe Foederer is daarom een IT & Cybersecurity specialist betrokken om te toetsen hoe uw organisatie het IT-beleid, de digitalisering/automatisering en de cyberveiligheid heeft ingericht. De werkwijze wordt hieronder toegelicht.

Aanpak
Afhankelijk van de complexiteit van uw organisatie en of er reeds een gedegen onderzoeksrapport beschikbaar is zetten wij één of beide van onderstaande methodieken in:

1. Een operationeel interview
Centrale vraagstelling: Hoe gaat uw organisatie om met IT en het cybersecuritybeleid?

Op basis van een uitgebreid interview door een IT & Cybersecurity specialist met uw IT-management wordt de werkwijze van de organisatie duidelijk, alsook de hiaten en verbeterpunten op het vlak van cybersecurity en IT.

Dit geeft uw organisatie antwoord op vragen als:
- In hoeverre draagt het organisatiebeleid bij aan de continuïteit en veiligheid van IT-middelen?
- Zijn uw huidige processen omtrent cybersecurity voldoende om de bedrijfscontinuïteit te waarborgen?
- Is uw personeel voldoende bewust van de cyberrisico's?
- Hoe is de veiligheid van uw data geborgd?
- Wat zijn de belangrijkste focusgebieden op het gebied van cyberveiligheid?
- Wat is uw bedrijfsrisicoprofiel in relatie tot cyberveiligheid en welke maatregelen passen hierbij?

2. Een geautomatiseerde scan

Centrale vraagstelling: Hoe kwetsbaar is uw organisatie voor generieke cyberaanvallen?

Tijdens een geautomatiseerde scan onderzoeken we hoe het gesteld is met de cyberweerbaarheid van uw bedrijfsnetwerk en welke kansen cybercriminelen zouden kunnen aangrijpen om binnen te komen.

Dit geeft uw organisatie antwoord op vragen als:

- Zijn er voor de organisatie onbekende kwetsbaarheden die benut kunnen worden door cybercriminelen?
- Zijn er ten opzichte van uw perceptie afwijkingen in uw daadwerkelijke IT-configuraties?
- Voldoet uw basis IT-infrastructuur aan het normeringskader zoals geadviseerd door de Cyber Security Industrie (CSI)?
- Zijn bij bedrijf kritische IT-componenten de laatste patches en updates doorgevoerd en hanteert uw organisatie een effectief beheer op dit vlak?

Normering

Dit onderzoek wordt uitgevoerd volgens de CIS-normering. Dit is een internationale kwaliteitsstandaard van het Center for Internet Security, waarbij aan de hand van een praktijkgericht model de cyberveiligheid kan worden geïdentificeerd, ontwikkeld, gevalideerd en geborgd.

Resultaat

Op basis van de twee genoemde onderzoeksmethodieken wordt een adviesdocument opgeleverd, bestaande uit een managementsamenvatting, conclusies en aanbevelingen. Hiermee beschikt u over een duidelijk overzicht hoe uw organisatie met haar bijbehorende bedrijfsrisicoprofiel scoort op het gebied van cybersecurity maatregelen. Dit geeft uw organisatie een goed beeld in welke mate beleid, procedures en de technische inrichting op het vlak van IT en cybersecurity zijn geborgd. Daaraan verbonden krijgt u concrete aanbevelingen waarbij het verder verhogen van de digitale weerbaarheid van uw organisatie centraal staat.

Adviesrapport

Dit onderzoek is een onderdeel van onze werkzaamheden bij de controle van de jaarrekening. Voor uw organisatie is het een hoogwaardig adviesrapport dat u inzichten geeft in de cyberweerbaarheid van uw organisatie en kwaliteit van uw digitalisering/automatisering.

Vervolgstappen

Zoals aangegeven, IT en cybersecurity zijn van groot belang voor de continuïteit van uw organisatie. Op basis van de onderzoeksresultaten en met name de aanbevelingen kan worden vastgesteld wat de best passende vervolgstappen zijn. Dat kan een verbetertraject zijn op basis van de aanbevelingen en waarmee u de cyberveiligheid van uw organisatie verhoogt. Ook kan het raadzaam zijn om aanvullend onderzoek te doen. Hiervoor kunt u de keuzehulp gebruiken op de website van onze dochterorganisatie ACA IT-Solutions via deze link: **www.aca-it.nl/keuzehulp**

Houdt u er bovendien rekening mee dat het onderzoek een momentopname is. Het is een continuproces om uw IT-omgeving vitaal en veilig te houden.

Wilt u meer informatie of een afspraak maken? Neem dan contact op met uw vaste contactpersoon of via:

Crowe Foederer
Beukenlaan 60
5651 CD Eindhoven
040 - 264 96 10
www.crowe-foederer.nl