Duthler Associates
law, ICT & organisation

Factsheet

IT-riskmanagement in de cloud

Aanleiding

Het merendeel van de bedrijven maakt gebruik van clouddiensten van toonaangevende clouddienstenleveranciers zoals Microsoft, Google en Amazon. De belangrijkste reden zijn meer veiligheid voor bedrijfs- en persoonsgegevens (waaronder bedrijfsgeheimen) tegen lagere kosten.

Voor veel bedrijven was/ is het managen van IT op locatie een uitdaging en dat is het ook voor IT-clouddiensten. Als gevolg van het volwassen worden van cybercriminaliteit blijft het centrale vraagstuk van het borgen van de continuïteit van de bedrijfs-IT actueel. De clouddienstenleveranciers reageren alert op innovaties van cybercriminelen met passende en effectieve beheers- en beveiligingsmaatregelen.

Bedrijven zijn zelf verantwoordelijk om de maatregelen te implementeren en te beheren. Dit vraagt van de organisatie kennis- en verandermanagement dat niet altijd voorhanden is. Wij zien dan ook dat bedrijven het beheren van de IT-clouddiensten uitbesteden aan IT-bureaus.

Het uitbesteden van de IT-clouddiensten aan IT-bureaus garandeert niet dat voorkomen wordt dat het bedrijf getroffen wordt door cybercriminaliteit. Als onbevoegden binnentreden op het netwerk en schade toebrengen komt snel de vraag op tafel wie verantwoordelijk was voor het voorkomen van incidenten. Het antwoord ligt in het contract dat het bedrijf heeft gesloten met het IT-bureau. In dergelijke contracten spreekt het IT-bureau vaak een inspannings- en geen resultaatsverplichting af. De gevolgen van het incident komen dan voor rekening en risico van het bedrijf.

Het bedrijf kan de effectiviteit van getroffen beheers- en beveiligingsmaatregelen verbeteren door gebruik te maken van riskmanagement.

Riskmanagement

Riskmanagement richt zich op de instandhouding van de bedrijfscontinuïteit. Dit door kwetsbaarheden in de bedrijfsvoering te signaleren en inventariseren, bedrijfsrisico’s in te schatten en voorstellen te doen voor het treffen van (aanvullende) effectieve beheers- en beveiligingsmaatregelen.

Onderdeel van riskmanagement is IT-riskmanagement voor cloud. Het gaat bij IT-riskmanagement voor cloud om de instandhouding van de IT-clouddiensten die de basis vormen voor de bedrijfscontinuïteit. Het IT-riskmanagement inventariseert op IT-clouddiensten de kwetsbaarheden, maakt inschattingen van de bedrijfsrisico’s en stelt effectieve beheers- en beveiligingsmaatregelen voor die de operationele organisatie of het IT-bureau dat belast is met IT-beheer, implementeert. Tijdens en na implementatie monitort IT-riskmanagement de effectiviteit van de getroffen beheers- en beveiligingsmaatregelen. Veelal voorzien clouddienstenleveranciers het IT-riskmanagement van passende rollen op de IT-clouddiensten.

Functiescheiding aangebracht tussen operationeel IT-beheer (al dan niet uitbesteed aan een IT-bureau) en IT-riskmanagement resulteert in een versterking van de effectiviteit van de IT-clouddiensten en daarmee wordt de bedrijfscontinuïteit beter geborgd.

Zie de blog: ‘Taken, bevoegdheden en verantwoordelijkheden in MS 365 en Azure’.

Duthler Associates vervult de rol van IT-riskmanager

Onze professionals, met een IT audit en of compliance achtergrond die kennis en ervaring hebben opgedaan met beheren van IT-clouddiensten, vervullen voor bedrijven de rol van IT-riskmanager. De IT-riskmanager rol is veelal onderdeel van de bredere riskmanager rol.

De IT-riskmanager maakt gebruik van een rol die toegewezen wordt in de IT-clouddiensten van het bedrijf. Op basis van de uitkomsten van een bedrijfsonderzoek en de inventarisatie van kwetsbaarheden uit de IT-clouddiensten en hieruit voortvloeiende bedrijfs- en beveiligingsrisico’s stelt de IT-riskmanager een plan van aanpak op. De prioriteiten van het plan worden bepaald door het uitgangspunt te hanteren van: wat “moet” en wat “kan”.

Als de bedrijfsleiding het plan heeft goedgekeurd zorgt het operationele beheerteam (veelal het IT-bureau) voor de realisatie van beheersmaatregelen. De IT-riskmanager houdt de vinger aan de pols dat de maatregelen op een goede manier worden uitgevoerd en effectief zijn. Het is een continue bezigheid omdat aan de ene kant het dreigingslandschap wijzigt en aan de andere kant de stand der techniek verbetert waardoor effectievere beheersmaatregelen mogelijk worden.

De inzet van onze professionals is structureel (vanaf een halve dag per week) en incidenteel als er sprake is van beveiligings- en beheers-incidenten.

Zie de blog: ‘Een praktische aanpak voor het toepassen van IT-clouddiensten’.

Toegevoegde waarde en businesscase

Het aanstellen van een IT-riskmanager zorgt ervoor dat de bewaking van IT-clouddiensten effectief is georganiseerd, de kans op cyberincidenten afneemt en de bedrijfscontinuïteit is beter geborgd. Operationeel wordt het IT-beheer effectiever en veelal goedkoper.

Het benoemen van de toegevoegde waarde van riskmanagement is afhankelijk van de bestaande organisatie van de IT-clouddiensten. Wij zijn graag bereid een inschatting te maken van de toegevoegde waarde en de daarbij behorende businesscase voor het inzetten van een IT-riskmanager. Wij kunnen ook een oriënterend gesprek voeren over het implementeren en beheren van IT-clouddiensten.

Vertrouwensdiensten

Wij voeren in opdracht van MYOBI gesprekken met gebruikers van het MYOBI Vertrouwensnetwerk over de Accountability Seal als verantwoording voor het organiseren van compliance met de gedragscode AVG. In de afgelopen jaren maken meer en meer bedrijven gebruik van IT-clouddiensten en ontwikkelen daarmee ook de compliance-aanpak. Ook voor gebruikers van het vertrouwensnetwerk is het IT-riskmanagement-voorstel van harte aanbevolen.

Duthler Associates
law, ICT & organisation

Afspraak maken en contact

Wilt u meer weten? Neem dan contact op met ons via onderstaande gegevens. Of bezoek onze website: www.duthler.nl

Kantoor:

Frankenslag 137

2582 HH Den Haag

+31 (0) 70 392 22 09

info@duthler.nl

Direct contact:

drs André J. Biesheuvel RE RA RFG

a.j.biesheuvel@duthler.nl

Caroline Willemse RE AA RFG

c.willemse@duthler.nl