CYBERSECURITY? DE GROOTSTE UITDAGING

Cybersecurity is de grootste uitdaging voor accountantskantoren op dit moment. Er gaat geen dag voorbij of we lezen wel weer over een incident bij een bedrijf dat is getroffen door ransomware. Ook accountantskantoren krijgen hier steeds vaker mee te maken. ‘Het is niet de vraag of u wordt gehackt, maar wanneer’ is dan ook een uitspraak die u steeds vaker hoort. Het mag duidelijk zijn dat investeren in cybersecurity van groot belang is.

Accountantskantoren opereren meer en meer in een gedigitaliseerde omgeving. De afhankelijkheid en de impact van incidenten zijn hierdoor sterk toegenomen. Om de digitale weerbaarheid van het kantoor te vergroten, is het van belang dat dreigingen worden onderkend en dat de juiste maatregelen worden getroffen.

GROOTSTE BEDREIGINGEN

Ieder jaar publiceert ENISA, het Europees Agentschap voor Cyber Security, een overzicht* van de meest voorkomende cyberdreigingen. De grootste dreigingen op dit moment zijn:

1. ransomware
2. malware
3. cryptojacking
4. e-mail gerelateerde bedreigingen
5. bedreigingen met betrekking tot data
6. bedreigingen tegen beschikbaarheid en integriteit
7. desinformatie - verkeerde informatie
8. niet-kwaadaardige bedreigingen
9. supply chain-aanvallen

Phishing is daarbij een middel dat veelvuldig wordt gebruikt om u op te lichten.

TRENDS EN ONTWIKKELINGEN

Naast een toenemende dreiging door cybercriminelen, zie je de tendens dat klanten hun accountantskantoren vragen hoe digitaal weerbaar zij zijn. Hebben kantoren zich laten toetsen door een onafhankelijke, externe deskundige, bijvoorbeeld in de vorm van een ISAE3402-II verklaring of een ISO27001-certificaat?

*) Bron: ENISA’s Thread Landscape report - 2021

Vanuit wet- en regelgeving – denk aan de AVG – en toezichthouders worden eisen gesteld aan de informatiebeveiliging binnen het kantoor. Eind 2019 heeft de AFM haar ‘Principes voor Informatiebeveiliging’ gepubliceerd. Hierin spreekt de AFM haar verwachtingen uit over het gewenste gedrag van accountantskantoren.

Was in 2018 het mitigeren van een aantal risico’s door het afsluiten van een cyberriskverzekering relatief eenvoudig, inmiddels stellen ook verzekeringsmaatschappijen steeds hogere eisen aan de maatregelen die kantoren treffen. Eisen die vergelijkbaar zijn met ISO27001 of een vergelijkbaar normenkader, waarop vervolgens premies worden gebaseerd. Risico’s zijn daardoor niet altijd meer standaard (volledig) verzekerd.

AAN DE SLAG IN VIJF STAPPEN

Als kantoor kunt u ervoor kiezen om aan de hand van de ‘Principes voor Informatiebeveiliging’ van de AFM de risico’s rond informatiebeveiliging, cybersecurity en privacy af te grenzen. U kunt ook een stap verder gaan door het invoeren van de ISO 27001-norm, eventueel aangevuld met een externe toetsing. Om kantoren te helpen, heeft SRA een stappenplan ontwikkeld.

STAP 1: STEL HET (BELEIDS)KADER VAST

Om handen en voeten te geven aan (technologische) ontwikkelingen en informatie(beleids)vraagstukken, is een informatie(beveiligings)beleid een must voor ieder accountantskantoor. Dit hoeft geen doorwrocht stuk te zijn. Dit kan ook één A4 zijn met uitgangspunten, kaders en een beschrijving van verantwoordelijkheden.

STAP 2: BRENG RISICO'S IN KAART

Informatiebeveiliging, cybersecurity en privacy zijn onlosmakelijk verbonden aan risico's. Belangrijk is dat u alle risico's in kaart heeft en weet wat het volwassenheidsniveau van uw kantoor is. Begin met een eenvoudige risicoanalyse. Stel de kroonjuwelen vast, dus welke systemen en data zijn cruciaal voor uw kantoor. Maak daarbij een onderscheid tussen bedrijfscontinuïteit en dienstverlening. Stel vervolgens vast welke risico's hierbij horen.

STAP 3: BEPAAL DE GEWENSTE MAATREGELEN VOOR MENS, TECHNIEK EN ORGANISATIE

De risicoanalyse levert een lijst op met dreigingen en de impact hiervan op uw organisatie. De volgende stap is voor elke serieuze dreiging een of meer mitigerende maatregelen te vinden. Stel vast of maatregelen zijn getroffen en zo ja, of deze passend zijn. Hierbij gaat het niet alleen om techniek, maar ook om mens en organisatie.

STAP 4: OMGAAN MET UITBESTEDEN VAN IT-DIENSTEN

Steeds meer applicaties migreren naar de cloud en IT-diensten worden steeds vaker uitbesteed. Daarnaast besteden klanten ook werkzaamheden en diensten uit aan het accountantskantoor. Uitbesteden van IT(-diensten) heeft gevolgen voor risico's en maatregelen. Belangrijk is enerzijds te weten welke vragen moeten worden gesteld aan leveranciers om de kwaliteit te kunnen borgen. Anderzijds: wat zijn de antwoorden op vragen die klanten kunnen stellen?

STAP 5: BEHEERSEN EN VERBETEREN

Incidenten en datalekken komen met regelmaat voor. Belangrijk is dat u bent voorbereid en de juiste respons- en herstelmaatregelen heeft getroffen. Dit begint met het bijhouden van alle incidenten, het analyseren hiervan om vervolgens – waar nodig – maatregelen bij te stellen. Belangrijk is ook het regelmatig testen van de genomen maatregelen. Dit omvat ook het navragen bij leveranciers aan wie processen zijn uitbesteed. Denk hierbij bijvoorbeeld aan de back-up en recoveryprocedure door de cloudprovider.

TOOLS EN HULPMIDDELEN

Het aanbod van tools en hulpmiddelen is groot. Belangrijk is dan ook te weten welke tools beschikbaar zijn en welke eisen u aan de tool en/of leverancier hiervan moet stellen. Het Digital Trust Center (digitaltrustcenter.nl) biedt een aantal gratis tools en hulpmiddelen om u op weg te helpen.

MEER INFORMATIE

Heeft u vragen of wenst u meer informatie? Kijk dan op Dossier Informatiebeveiliging, cybersecurity & AVG of neem contact op met Tony van Oorschot, tvanoorschot@sra.nl of 030 656 60 60.

PROJECT GEIGER

Het is van cruciaal belang dat bedrijven zich bewust zijn van hun risico's met betrekking tot gegevensbescherming, privacy en cybersecurity en de impact hiervan op hun business. Belangrijk daarbij is dat de bedrijven van hun accountant de juiste hulp krijgen bij het nemen van de juiste mitigerende maatregelen. GEIGER helpt hierbij.

GEIGER (een Europees innovatieproject (883588)) biedt een unieke mogelijkheid om enerzijds uw klanten digitaal weerbaarder te maken. Met behulp van de GEIGER-tool wordt inzicht verkregen in de verschillende risico's binnen de organisatie en worden tevens oplossingen geboden om deze risico's direct te ondervangen. Dit is bovendien een continu proces. Anderzijds biedt de tool u de mogelijkheid om uw kennis en ervaring op het gebied van cybersecurity verder uit te breiden en kunt u zich profileren op dit vlak om zo uw rol als trusted advisor te versterken.

Meer weten? Kijk dan op www.sra.nl/geiger.