Duurzaam digitaliseren vraagt om scherpe securitystrategie

Steeds meer organisaties slaan de weg van digitalisering in. Dat biedt grote kansen maar brengt ook nieuwe risico's met zich mee. SRA wil een inhoudelijke bijdrage leveren aan het versterken van uw kantoor en de relatie met uw klanten die deze transitie doormaken. Daarom hebben we de samenwerking gezocht met Northwave, een zeer gerenommeerde partij op het gebied van integrale informatiebeveiliging.

Samen met Northwave besteden we in de aankomende edities van de SRAadviseur aandacht aan de 'hot topics' rondom het beveiligen van informatie en de rol die accountants daarbij kunnen en misschien zelfs wel moeten spelen. In dit eerste artikel kijken we naar de strategische keuzes die organisaties kunnen maken over dit onderwerp. We gaan in gesprek met Talitha Papelard, Director Business Security van Nortwhave en co-auteur van het boek 'Critical Success Factors for Information Security'. We vragen Papelard naar haar ervaringen in het mkb.

Risico van de zwakste schakel

"Wat we in het mkb zien, is dat digitalisering grote impact heeft op de bedrijfsvoering. Iedereen wordt steeds afhankelijker van digitale informatie. We zitten allemaal in ketens en zijn daarmee zo kwetsbaar als de zwakste schakel. Wij zien veel incidenten, waarbij meerdere bedrijven slachtoffer worden doordat hackers 'doorstappen' van het ene naar het andere bedrijf. Een recent voorbeeld is een technisch bedrijf dat tonnen schade oploopt omdat een van haar leveranciers wordt gehackt en er via de systemen van die leverancier vervalste facturen naar opdrachtgevers gaan.
Veel mkb-ers weten wel dat ze hier iets mee moeten, maar vinden het moeilijk een passende aanpak te kiezen omdat het onderwerp best complex is en de expertise en ervaring op dit vakgebied vaak ontbreekt."

Accountants helpen hun klanten bij het betrouwbaar houden van de financiële bedrijfsvoering. Dan is het inzichtelijk houden van risico's van groot belang.
In allerlei onderzoek onder ondernemers en managers zien we dat de angst voor cyberrisico's toeneemt. Tegelijkertijd zijn die risico's voor veel bedrijven niet tastbaar. "Wat is dan de strategie om te komen tot een slimme aanpak?"

Strategie is focus

Papelard: "Strategie is focus. De keuze om dit serieus te nemen, is vaak de belangrijkste strategische stap. In mijn boek komt als belangrijkste succesfactor om in control te zijn 'commitment van senior management' naar boven. Zorg dat je in beeld krijgt wat je daadwerkelijke risico's zijn. Ontdoe ze van de hype en de hysterie en maak inzichtelijk wat een concrete situatie in jouw organisatie aan financiële schade of derving zou betekenen. Vraag je dan af wat de werkelijke kans is dat zoiets zich voordoet. Praat er over met je accountant, collega's, klanten en leveranciers. Zo prioriteer je de risico's op basis van feiten en harde euro's en niet op basis van vage veronderstellingen. Focus op jouw top tien met een pragmatisch risicobehandelplan. Kijk daarbij vooral verder dan alleen IT-maatregelen.

Informatiebeveiliging is iets van de hele organisatie. Een goede werkafspraak helpt vaak minstens even goed en kost minder. Alerte mensen zijn goede bewakers van je data. Betrek dus vooral ook je belangrijkste partners en je medewerkers. En nu komt het allerbelangrijkste: herhaal dit proces ten minste ieder jaar en bij grote veranderingen in je bedrijf, zoals een verhuizing, nieuwe vestiging, overname of outsourcing."

Privacybescherming

Veel accountantskantoren zijn het afgelopen jaar bezig geweest met de GDPR, oftewel de AVG. Dat heeft tot veel extra werk en kosten geleid, maar ook tot meer aandacht voor beveiliging en privacy. Nog steeds zijn er veel organisaties die niet voldoen aan de wet. We vragen Papelard wat haar beeld is.

"De GDPR is een Europese aanscherping van onze oude Wet bescherming persoonsgegevens. Het karakter van de wet is: je moet een juridische grondslag hebben voor het hebben en verwerken van die gegevens. Als je ze niet goed beveiligt, mag je persoonsgegevens niet hebben en gebruiken. Dat maakt voor de wet dus strikt genomen alle activiteiten illegaal die niet aan de wet voldoen. Dat de meeste bedrijven nu nog niet voldoen komt doordat ze niet goed hebben begrepen wat de wetgever eigenlijk precies van hen verwacht. We zien vaak na een vraag meteen al wat er ontbreekt: een structurele aanpak voor informatiebeveiliging. Eigenlijk precies het risicogedreven proces dat ik hierboven heb beschreven."

Stel security centraal

Papelard continueert: "Voor veel organisaties is 'compliant zijn' de primaire drijfveer geweest om aan de slag te gaan.

Verwerkersovereenkomsten, registers en procedures voor rechten van gebruikers werden vastgelegd, soms zelfs geïmplementeerd. Maar de meeste organisaties gaan voorbij aan het borgen van wat er elke dag weer opnieuw moet gebeuren om die informatie goed te beveiligen. Wij adviseren om in je strategie niet de ‘compliance’ maar de ‘security’ centraal te stellen en de principes van kwaliteitsmanagement te gebruiken. Die principes kennen veel ondernemers en accountants al uit de praktijk. Denk aan ISO9001.

Of je nu klein of groot bent, dat is altijd de basis voor een gerichte aanpak van je beveiligingsrisico’s. Het voldoen aan de GDPR loopt daarin gewoon mee. Want hoeveel onderscheid kun je nu eigenlijk helemaal maken tussen het beschermen van persoonsgegevens en je andere bedrijfskritische informatie?”

Méér dan alleen IT

Dit onderwerp blijft voor veel organisaties toch een nevenactiviteit, terwijl het hun kernactiviteiten wel heel hard kan raken. Hoe kunnen kleinere organisaties daar nu het beste mee omgaan? “Dat is een uitermate belangrijk vraagstuk. Er is een diversiteit aan expertises nodig, van technisch tot juridisch, van procesmatig tot psychologisch. Dat heb je niet allemaal zelf in huis.

Bedrijven denken dat informatiebeveiliging een IT-aangelegenheid is. De IT is uitbesteed, dus daarmee is dit hele vraagstuk geregeld. Helaas is het tegendeel waar. ICT- leveranciers willen gebruiks- en beheergemak bieden en dat staat vaak haaks op beveiliging. Als deze leveranciers hun werk niet goed of veilig genoeg doen, ontstaan er risico’s wat betreft jouw informatie, terwijl jouw organisatie verantwoordelijk is en blijft, ook voor de wet. Als je daar zelf geen zicht op houdt, ben je niet ‘in control’, niet veilig en niet compliant. Dus terug naar het begin van dit gesprek: pas als je je risico’s begrijpt kun je nadenken over wat je moet doen. Je hoeft niet alles zelf te kunnen, maar neem wel actief de regie over dit onderwerp en begin vandaag”, sluit Papelard af.

Meer informatie

Voor meer verdieping over dit onderwerp, verwijzen wij naar het boek ‘Critical success factors for effective business information security’ geschreven door Talitha Papelard-Agteres MSc. Ook vindt u meer informatie op www.sra.nl en kunt u voor vragen terecht bij afdeling Automatisering, automatisering@sra.nl.

Talitha Papelard

Wij adviseren om in je strategie niet de ‘compliance’ maar de ‘security’ centraal te stellen en de principes van kwaliteitsmanagement te gebruiken