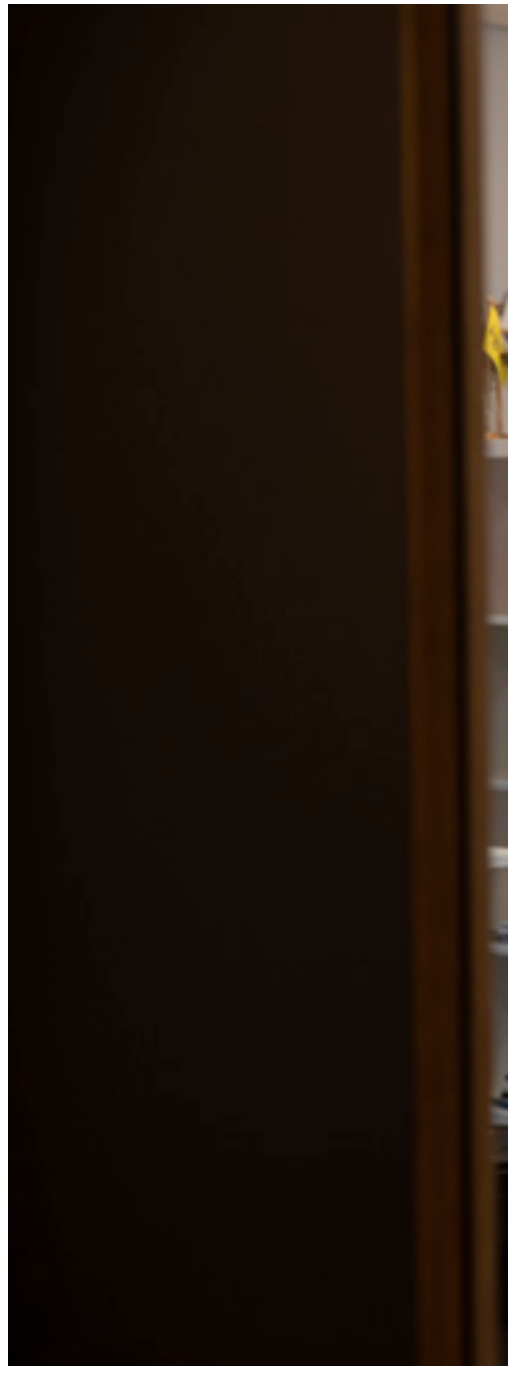
Fotografie: Joost Franken



NEWDAY OVER CYBERSECURITY EN PRIVACYWETGEVING

"ALLEEN EEN BACK-UP MAKEN IS NIET VOLDOENDE"

Randsomware-aanvallen, datalekken, hoge boetes; de afgelopen maanden zijn grote bedrijven die hiermee te maken kregen uitvoerig in het nieuws gekomen. Maar ook het mkb loopt grote risico's indien de cybersecurity en het naleven van de AVG intern niet op orde zijn. Gelukkig weet NewDay op een overzichtelijke manier de risico's in kaart te brengen en om te zetten in een praktische oplossing.

CYBER SECURITY

Het mkb is de afgelopen jaren steeds meer aan het automatiseren geslagen. Dat is volgens Alex Klaassen van IT Risk organisatie NewDay een positieve ontwikkeling. "Maar ik merk ook dat ondernemers op het gebied van cybersecurity flink achterblijven. Gemak en efficiëntie staan vaak voorop, maar daar betaal je de prijs voor in de vorm van diverse IT-risico's. En die risico's zijn nu actueler dan ooit. Sinds het uitbreken van de coronacrisis zijn er onder andere meer en nieuwe randsomware-aanvallen gedaan. Ook thuiswerken via remote desktop via een onvoldoende beveiligde verbinding is een veel genomen risico. Vergeet niet dat hacken tegenwoordig een serieus businessmodel is. Criminelen die zich hiermee bezighouden, verdienen makkelijk geld met weinig stappen. En op het moment dat het slachtoffer beveiligingsmaatregelen onderneemt en het de hacker iets meer moeite kost, is het nog steeds lucratief! Nu denken mkb'ers vaak wel aan het maken van een technische back-up, maar dat is bij een hack echt niet voldoende. Wat nu als de hacker je data op de bestaande servers vernietigt en de data op je back-up versleutelt? Ga je dan vijftig bitcoins betalen of je hele infrastructuur opnieuw opbouwen?"

PRIVACYWETGEVING

Een ander actueel thema is het naleven van de Algemene verordening gegevensbescherming (AVG). Organisaties die de AVG overtreden, riskeren een boete van maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet. Ook kan de Autoriteit Persoonsgegevens, die controleert of de AVG wordt nageleefd, een dwangsom of een verwerkingsverbod opleggen, of een berisping of een waarschuwing afgeven. Alex: "Vanuit de privacywetgeving moet je kunnen aantonen dat je een grondslag hebt om de persoonsgegevens die binnen je bedrijf aanwezig ook daadwerkelijk te verwerken."

Als het verwerken van de gegevens een hoog privacy risico oplevert voor

de mensen van wie de organisatie gegevens verwerkt, dan ben je verplicht om een data protection impact assessment (DPIA) uit te voeren. “Met dit instrument worden vooraf privacy risico’s van een gegevensverwerking in kaart gebracht. Ook kan het aanstellen van een Functionaris gegevensbescherming (FG) verplicht zijn. Bijvoorbeeld wanneer er bijzondere informatie over iemands gezondheid, ras, politieke opvatting of geloofsovertuiging wordt verwerkt. Of wanneer de gegevens worden gebruikt voor bijvoorbeeld profilering van mensen, het maken van risico-inschattingen, cameratoezicht of personeelsvolgsystemen.”

ACTUEEL DOSSIER

In aanloop naar de inwerkingtreding van de AVG op 25 mei 2018 hebben veel bedrijven de nodige stappen ondernomen, “maar deze stappen waren te vaak vooral cosmetisch van aard”, zegt Alex. “Men liet een blik op het personeelsregister en de klantgegevens werpen, of liet de jurist een nieuw contract en een privacyverklaring opstellen. Of men huurde een ethical hacker in om te toetsen of er lekken in de beveiliging waren. Dat zijn allemaal gefragmenteerde oplossingen. Privacy is echter te omvattend om eendimensionaal aan te pakken, het is vervlochten met je bedrijfsvoering. Bovendien hebben veel bedrijven na de invoering

van de AVG de aandacht voor dit onderwerp (deels) losgelaten. Maar een ondernemer moet wel te allen tijde met een actueel dataregister kunnen aantonen dat hij of zij zorgvuldig met persoonsgegevens omgaat. Dat geldt ook voor elke nieuwe bedrijfsactiviteit waarbij een nieuwe verwerking van persoonsgegevens plaatsvindt."

SPECIALISME VOOR HET MKB

De diensten die NewDay aanbiedt om bedrijven te helpen bij het op orde brengen en houden van cybersecurity en naleving van de privacywetgeving, zijn gebaseerd op zeer specialistische kennis. Deze wordt normaal gesproken met name voor grote bedrijven, organisaties zoals ziekenhuizen en overheidsinstellingen zoals gemeenten ingezet. Alex benadrukt echter dat hij met NewDay ook het mkb wil helpen. "Middel- en kleine organisaties zijn vanwege onze kennis, expertise en klantenkring soms bang dat ze een lawine aan informatie over zich heen krijgen. Voor deze partijen hebben we juist een aantal standaardtools ontwikkeld die een gedegen risicoanalyse maken op het gebied van privacyrisico's, cybersecurity, compliance en/of IT-security. Aan de hand van die analyses weet je concreet welke onderdelen al goed geregeld zijn, welke bedrijfsonderdelen risicogebieden vormen en hoe je deze risico's het beste af kunt dekken. Bij het maken van deze analyse kan een multidisciplinair team worden betrokken van juristen, ethical hackers, data-analysten en informatiebeveiligingsdeskundigen. Indien nodig schakelen we ook een communicatiedeskundige in om de boodschap op de juiste manier te verwoorden en deze intern te verspreiden. Uiteindelijk komt er, afhankelijk van de omvang van de bedrijfsactiviteiten en de gevonden risico's, een document op tafel te liggen met een plan van aanpak en een duidelijk takenpakket per afdeling. Zo kan een hr-manager voor de privacy-aspecten rond het personeelsbestand bepaalde kpi's ontwikkelen, bijvoorbeeld welke onderdelen relateren aan de privacywetgeving."

IT-AUDITS

Naast het controleren of bedrijven zelf voldoen aan de huidige eisen op het gebied van cybersecurity en het naleven van de AVG, kunnen ook bedrijven die informatiesystemen aanbieden aan derden bij NewDay terecht. "Aan de hand van een IT Audit of EDP Audit vellen we op een onafhankelijke en deskundige manier een oordeel over de kwaliteit van de ICT-beveiliging, signaleren we tekortkomingen en geven we advies over mogelijke verbeteringen. Denk aan een ISAE 3402-verklaring voor IT-dienstverleners waarmee zij onder andere kunnen aantonen dat zij met hun producten en diensten voldoen aan bepaalde wet- en regelgeving en die van de partners.

Bedrijven die producten en diensten met een DigiD-aansluiting leveren aan de overheid, moeten jaarlijks een DigiD audit laten doen. De audit moet worden uitgevoerd onder verantwoordelijkheid van een register IT auditor."

"AAN DE HAND VAN EEN IT AUDIT OF EDP AUDIT VELLEN WE OP EEN ONAFHANKELIJKE EN DESKUNDIGE MANIER EEN OORDEEL OVER DE KWALITEIT VAN DE ICT-BEVEILIGING."

COLUMN

De komende edities zal Alex in een column nader ingaan op deze onderwerpen. "Met dit verhaal en de columns wil ik het mkb een duidelijk beeld geven van de risico's die zij lopen en hoe NewDay hierbij kan helpen. Ik hoop hiermee de zogenoemde risk appetite van ondernemers aan te spreken. Ik begrijp maar al te goed dat een ondernemer onderneemt voor eigen rekening en risico. Maar als je pas tot actie overgaat wanneer je ervaringsdeskundige bent geworden, is de schade natuurlijk al berokkend."

Meer informatie vind je op newdayriskservices.nl

MAATSCHAPPELIJKE FUNCTIE

NewDay is aangesloten bij NOREA, de beroepsorganisatie van IT auditors. Deze organisatie telt inmiddels 1.800 leden. NOREA houdt toezicht op de kwaliteit van de beroepsuitoefening van deze leden en toetst deze om de drie jaar. Hiervoor wordt onder andere een aantal onafhankelijke tools gebruikt. NOREA is net zoals de Nederlandse Beroepsorganisatie van Accountants, aangesloten bij de wereldwijde beroepsorganisatie van accountants, waardoor de IT auditors, oftewel RE's, op gelijke voet met registeraccountants opereren.
Alex Klaassen: "Alle medewerkers van NewDay werken volgens de regels en richtlijnen van deze beroepsgroep. Zij hebben een postacademische opleiding gevolgd en hebben aantoonbaar voldoende ervaring om tot het register te worden toegelaten, of zijn daarmee bezig. Daarnaast volgen de medewerkers een minimaal aantal uren opleiding en cursussen per jaar. Het NOREA-lidmaatschap vind ik zeer waardevol. Door als IT auditor je functie grondig, gedegen en betrouwbaar en onafhankelijk te verrichten, lever je een essentiële bijdrage aan het in stand houden van de processen en systemen die cruciaal zijn voor de economie en de maatschappij."