DORA nur für die Großen, oder doch auch für die Kleinen?

Wenn man sich die Ausnahmeregelungen ansieht, dann könnte man sich als Kleiner zurücklehnen. So konnte man kürzlich lesen, dass nur 3 Versicherungsmakler in Österreich auf über 250 Mitarbeiter kämen, alle anderen würden wohl unter die Ausnahmeregelungen fallen. Im Finanzbereich gilt die DORA für Wertpapierfirmen, für Wertpapierdienstleistungsunternehmen gibt es Ausnahmeregelungen nach Art 2 Abs 3 lit d DORA-Verordnung (Kleinstunternehmen). Stimmt es also, dass DORA nur für die Großen gilt?

Wie sieht das Michael Herzhofer, Obmann der AFPA?

Im Gegensatz zu anderen Verbänden bin ich überzeugt davon, dass DORA auch den einzelnen Berater/ Vermittler treffen wird. Etwa weil die Produktgeber Vorgaben machen werden müssen, wie man aufgestellt sein muss, um als Berater / Vermittler künftig mit dem Versicherer, der Wertpapierfirma, der Bank etc. zusammenarbeiten zu dürfen. Ich denke, schon alleine deshalb, um z.B. im Hacker-Angriffsfall nicht vorgeworfen zu bekommen, man habe die Sorgfaltspflichten verletzt, etc.. Also wird die DORA, also der „Digital Operational Resilience Act", sehr wohl in den unmittelbaren Arbeitsbereich des einzelnen Beraters und Vermittlers eingreifen.

Die Großen, also Banken, Versicherungen und Co, werden die DORA umsetzen, die eigenen Systeme ganz auf die neuen technischen Sicherheits-Anforderungen ausrichten. Und die firmeninternen Prozesse entsprechend aufstellen.

Danach wird man den Beratern und Vermittlern ganz exakte Vorgaben machen, was man tun muss und auf keinen Fall tun darf. Denken wir nur an die DSGVO, wo der Datenverantwortliche auch alle Aufgaben, Pflichten und Verantwortungen auf den Auftragsverarbeiter überbindet. Und es wird auch bei DORA eine lange Liste geben, unter welchen Bedingungen man künftig weiter mit dem „großen Partner" zusammenarbeiten wird dürfen.

Das wird wohl Vorgaben hinsichtlich der zu verwendenden EDV- und IT-Technik umfassen. Die Prozesse werden neu aufgesetzt. Neue Sicherheitsregeln für Zugriffe von außen und z.B. das Hochladen von Dokumenten, um Risken bewusst zu vermeiden, etc. werden folgen, um einen weitestgehenden Schutz gewährleisten zu können.

Wer diese DORA-Anforderungen der Wertpapierfirma, der Bank, etc. nicht erfüllen kann oder will, wird künftig von der Zusammenarbeit ausgeschlossen werden. Daher: Fragen Sie bei Ihren Partnern schon jetzt an, wie Sie sich die künftige Zusammenarbeit unter DORA vorstellen.

Für die Großen wird die DORA-Umsetzung eine große Herausforderung für die Verantwortlichen von Technik aber auch Organisation werden. Investitionen und neue Aufgaben für die Risikoanalyse und Schulungen der Mitarbeiter (u.a. zum besseren Erkennen von Cybergefahren) werden die regelmäßige Folge sein.

Auch die Geschäftsführung wird sich intensiv um DORA kümmern müssen.

Tipp: Gerade die „üblich gewordenen" Auslagerungen sollte man sich genau ansehen. Denn die oft gehörte Ausrede, Details dazu gehen mich nichts an, dafür habe ich eine Firma, die für die Ordnungsgemäßheit haftet, stimmt keinesfalls mehr. Sie als Geschäftsführer sind dafür persönlich haftbar.

Also ist es wichtig, dass die Geschäftsführung im Blick hat, dass sie selbst durch DORA haftbar werden kann. Die persönliche Verantwortung der Geschäftsleitung stellt eine der wichtigsten Neuerungen durch DORA dar. So ist in Art. 5 Abs. 2 a ausdrücklich festgehalten, dass das Leitungsorgan „die letztendliche Verantwortung für das Management der IKT-Risiken" trägt. Dies bedeutet, dass Geschäftsführer und Vorstand ihre diesbezügliche Verantwortung in Zukunft nicht mehr an die IT-Leitung abgeben können. Gemäß den Anforderungen des Art. 5 DORA kommen auf die Geschäftsleitung umfangreiche Genehmigungs-, Überwachungs- und Überprüfungspflichten zu, deren Nichtbeachtung haftbar macht. Auch müssen Mitglieder des Leitungsorgans in Zukunft regelmäßig spezielle Schulungen absolvieren, um ihre Kenntnisse und Fähigkeit bzgl. IKT-Risiken aktiv auf dem neuesten Stand zu halten. Es ist daher unerlässlich, dass Geschäftsführer und Vorstand sich intensiv mit DORA beschäftigen.

Michael Herzhofer