DORA soll die digitale Widerstandsfähigkeit durch Regulierung erhöhen. Gilt DORA wirklich nur für die Großen?

Kürzlich waren Millionen Computer nach einem fehlerhaften Update einer Sicherheitssoftware ausgefallen. Sie zeigten nur noch einen blauen Bildschirm an („Bluescreen of death"). Folge: Fluglinien und Flughäfen waren ebenso lahmgelegt, wie etwa Rettungsdienste und Krankenhäuser. Aber auch TV-Sender sowie Kassensysteme und Banken waren betroffen. Dass weniger als 1% der Windows-Computer betroffen waren, war nur darauf zurückzuführen, dass es sich um eine selten genutzte Software gehandelt hatte. Leicht vorstellbar, was passiert wäre, wenn eine häufig genutzte Software (Office oder Windows selbst), im Zuge eines Updates die Rechner lahmgelegt hätte. Dieses „kleine Hoppala" zeigt, wie verwundbar unsere heutige digitale Welt ist und welche strukturellen Schwächen unsere (kritische) Infrastruktur aufweist.

Eine andere bedrohliche Realität und möglicherweise Anlass für DORA sind Cyberstraftaten. Regelmäßig liest man von erfolgreichen Hacker-Angriffen auf Unternehmen, egal, ob groß oder klein.

Laut einer aktuellen IBM-Studie „Cost of a Data Breach Report 2024" betrugen die durchschnittlichen Kosten eines Datenlecks in Deutschland 2024 im Schnitt 4,9 Mio. Euro pro Fall. Damit stiegen die Kosten pro Datenleck um 14% gegenüber dem Vorjahr, was zeigt, dass die Auswirkungen von Datenlecks auf den Betrieb immer größer werden und die Anforderungen an Cybersecurity ständig zunehmen.

Ebenso erfährt man in dieser Studie, dass deutsche Unternehmen durchschnittlich 185 Tage benötigten, um diese Vorfälle zu identifizieren und einzudämmen. Damit würden die Deutschen unter allen untersuchten Ländern und Regionen die kürzeste Zeit benötigen. Der weltweite Durchschnitt liege bei 258 Tage.

Das häufigste erste Einfallstor für Angreifer seien gestohlene oder kompromittierte Anmeldedaten. Phishing belegt den zweiten Platz, gefolgt von Fehlkonfigurationen in der Cloud, so die IBM-Studie.

Und damit kommen wir zum Trend zur Digitalisierung und Auslagerung, der seit der Corona-Pandemie nun auch in Österreich sogar in sehr traditionellen Branchen, wie etwa der Finanz- und Versicherungsbranche, enorm Fahrt aufgenommen hat.

Anstatt IT-Wissen intern im Unternehmen aufzubauen, hat es sich bisher meist finanziell bewährt, IT-Angelegenheiten auszulagern. Aber Drittanbieter von Informations- und Kommunikationstechnologien (IKT) unterliegen im Vergleich zu Versicherungsunternehmen keiner regulatorischen Aufsicht. Wenn es zu einem Cyber-Angriff auf den Drittdienstleister kommt, ist davon einerseits das Unternehmen selbst betroffen, darüber hinaus leiden sowohl jene Unternehmen, welche die IT-Dienste nutzen, als auch deren Kunden, an den Folgen.

DORA soll genau diesen Gefahren entgegenwirken und eine Harmonisierung der digitalen Resilienz schaffen. Was DORA ab 17.1.2025 fordert und wie man das umsetzen muss, erfahren Sie im zweiten Teil im Dezember.

Frage: Hätte DORA den eingangs beschriebenen weltweiten Ausfall verhindert?

DORA bringt sicherlich eine Verbesserung der Situation. Etwa bei Hard- und Software und Organisation im Unternehmen durch die eigenen Anstrengungen im Zuge der DORA-Vorbereitung und regelmäßigen Prüfungen (auch durch die Aufsicht). Auch wird wohl die Auswahl der eigenen IKT-Lieferanten einer genaueren Prüfung und Dokumentation unterzogen werden, wodurch weitere Fehlerquellen ausgeschlossen werden. Regelmäßige Schulungen der Mitarbeiter helfen sicher auch, die eine oder andere Phishing-Mail als solche zu erkennen und damit eine Hacker-Attacke bereits im Keim zu ersticken.

Aber zu glauben, dass DORA alle Gefahren für unsere digitale Welt beseitigt, ist weltfremd. Es kann und wird wohl weiterhin fehlerhafte Software geben, die irgendwelche Schäden verursachen wird. Aber wenn man dann ein aktuelles Backup der eigenen Daten, Prozesse etc. hat, dann hält sich der Schaden „durch den Stillstand des Unternehmens" in engen Grenzen.

Von RA Mag. Stephan Novotny

RA Mag. Stephan Novotny ist ein auf Versicherungs- und Datenschutzrecht spezialisierter Anwalt, der seit mehr als zehn Jahren mit eigener Kanzlei in Wien tätig ist. Er berät und vertritt Agenten, Makler, Finanzdienstleister, Vermögensberater, Banken und Versicherungen zu allen relevanten Bestimmungen und Haftungsfragen, insbesondere im Zusammenhang mit der Umsetzung der IDD, DSGVO und anverwandten Gesetzesmaterien.

Foto: Stefan Huger

Michael Herzhofer, Obmann der AFPA, zur Frage, ob DORA nur die Großen, oder doch auch die Kleinen betrifft:

Michael Herzhofer ist AFPA-Obmann und Geschäftsführer der Secura Gruppe (Foto: Fineart Photos by Andrea Schober)

Wenn man sich die Ausnahmeregelungen in der DORA ansieht, dann könnte man sich als Kleiner zurücklehnen. Und kürzlich konnte man im Fonds professionell lesen, dass nur drei Versicherungsmakler in Österreich auf über 250 Mitarbeiter kämen, alle anderen würden wohl unter die Ausnahmeregelungen fallen.

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.

Daher 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 Risiken bewusst zu vermeiden etc. werden folgen, um einen weitestgehenden Schutz gewährleisten zu können. Wer diese DORA-Anforderungen des Versicherers, 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.

AFPA

Direkt vertreten.
Direkt informiert.

AFPA, gegründet 2011, ist der unabhängige Branchenverband der selbständigen Versicherungsvermittler und Finanzberater Österreichs und Mitglied im europäischen Branchenverband FECIF mit Sitz in Brüssel. Damit ist AFPA nicht nur direkt in die EU-Regulationsprozesse eingebunden, sondern bietet ihren Mitgliedern auch dauerhaft einen direkten Vertretungs- und Informationsvorsprung in der EU und in Österreich.

AFPA-Mitgliedsunternehmen bieten Konsument:innen eine breite Auswahl an Finanz- und Versicherungsprodukten an, zum Unterschied zu angestellten Beratern von Banken und Versicherungen. In Summe arbeiten mehr als 13.000 Agenten, Makler und Vermögensberater mit den AFPA-Mitgliedsbetrieben zusammen. Für 540.000 Kundinnen und Kunden sichern unsere Mitglieder die tägliche finanzielle Versorgung in den Bereichen Versicherung, Investment und Finanzierung.

Um Konsument:innen auch in Zukunft den Zugang zu selbständiger Versicherungs- und Finanzberatung zu gewährleisten, bringt sich AFPA aktiv in die Regulierung des europäischen und österreichischen Finanzmarktes ein. Denn ein funktionierender Finanz- und Versicherungsmarkt ist nicht nur die Basis für eine erfolgreiche Zukunft, sondern letztendlich auch der beste Konsumentenschutz.

Für Rückfragen:

RA Mag. Stephan Novotny, kanzlei@ra-novotny.at
Michael Herzhofer, mh@afpa.at

Von AFPA