DORA: DIGITALE RESILIENZ

Ein Interview mit Joachim Forchheim

Die DORA-Verordnung (Digital Operational Resilience Act) ist am 17. Januar 2025 in Kraft getreten. Doch was bedeutet das konkret? Und wann ist externe Unterstützung sinnvoll? Wir sprachen mit dem Versicherungs-Experten, Juristen und Regulatorik-Berater Joachim (Josch) Forchheim über die Herausforderungen und Chancen von DORA.

Macros: Josch, Du bist zurzeit in mehreren DORA-Projekten tätig. Warum müssen sich Unternehmen überhaupt mit DORA beschäftigen?

Josch: DORA – also der Digital Operational Resilience Act – ist eine EU-Verordnung, die sich direkt auf alle Finanzunternehmen, einschließlich der Versicherer, auswirkt. Es geht nicht mehr nur um Datenschutz, sondern um die Gewährleistung der systemischen Widerstandsfähigkeit ihrer gesamten IKT-Infrastruktur, d. h. ihrer Informations- und Kommunikations-Technologie. Es handelt sich um einen umfassenderen, ganzheitlicheren Ansatz als frühere Verordnungen wie die VAIT. VAIT wird zwar durch DORA im Wesentlichen aufgegriffen und im Übrigen auch abgelöst, aber auch erheblich erweitert. DORA trat vor zwei Jahren in Kraft und kommt ab dem 17. Januar 2025 zur Anwendung.

Macros: Es gibt also da auch neue Themen im Vergleich zu VAIT? Was enthält DORA denn genau?

Josch: DORA konzentriert sich im Wesentlichen auf vier zentrale operative Bereiche: Risikomanagement, KT-Vorfallmanagement, Sicherheits- und Resilienz-Tests sowie das Management von Risiken im Zusammenhang mit IKT-Drittdienstleistern bzw. der Drittanbietersteuerung. Das Risiko-management ähnelt dem, was Versicherer bereits kennen, enthält jedoch detailliertere Anforderungen. Das Störfallmanagement, insbesondere die

Berichtspflicht betreffend schwerwiegender Vorfälle an die BaFin hingegen ist neu. Bisher waren nur Zahlungsdienstleister und Betreiber kritischer Infrastrukturen verpflichtet, Vorfälle ab einer bestimmten Schwelle zu melden. Nun müssen alle Finanzinstitute bedeutende IKT-bezogene Vorfälle melden. DORA verschärft die Anforderungen an das Management von ICT-Risiken bei Drittanbietern erheblich.

Macros: Was resultieren daraus konkret für Anforderungen – kannst Du da ein Beispiel nennen?

Josch: Ein griffiges Beispiel sind die Tests. Die waren bisher eher allgemein gehalten. In DORA werden nun explizit umfassende Sicherheits- und Schwachstellenanalysen, Penetrationstests und sogar Red-Teaming-Übungen genannt.

Macros: Das klingt nach deutlich mehr Testaufwand. Wie kann der geleistet werden, wenn jetzt schon IT und Fachbereiche kaum noch Zeit haben?

Josch: Sobald die aus den DORA-Anforderungen abgeleiteten Testbedarfe definiert sind, sieht man, dass manuelle Tests hier nicht wirklich weiterhelfen. Stattdessen müssen die Tests automatisiert und der ganze Testablauf so strukturiert werden, dass er möglichst aufwandsarm und oft wiederholbar wird. Daher ist das in der Tat ein spannendes Feld, bei dem eine externe Unterstützung sinnvoll ist. Je nach Unternehmensgröße und -historie kann hier auf einer guten Basis aufgebaut werden oder es muss quasi auf der grünen Wiese begonnen werden.

Macros: Da sind sicher auch kleine und große Versicherer unterschiedlich. Wie unterscheiden die sich denn generell bei der DORA-Umsetzung?

Josch: Beide rufen uns, wenn interne Kapazitäten oder Know-how fehlen. Große Unternehmen setzen, entsprechend den Proportionalitätsgrundsätzen, auf höchste Qualitätsstandards – quasi “mit Sternchen”. Kleinere Versicherer wählen oft einen pragmatischeren, schlankeren Ansatz. Beide erfüllen die DORA-Anforderungen, das Qualitätsniveau ist jedoch unterschiedlich. Wir unterstützen dabei, die DORA mit dem Qualitätsanspruch zu erfüllen, den sich das Unternehmen vorgenommen hat.

Macros: Um diesen Anspruch zu erfüllen, benötigt es sicher ein strukturiertes Vorgehen. Wie gehst Du in einem DORA-Projekt konkret vor?

Josch: Ich starte meine Projekte – wenig überraschend, aber das hat sich einfach bewährt – mit einer Gap-Analyse: Wir analysieren mit dem Kunden den Ist-Zustand, also den Stand der Umsetzung der bisherigen regulatorischen Anforderungen, gleichen ihn mit der DORA ab und erstellen eine meistens Jira-basierte Roadmap. Dabei berücksichtigen wir die vorhandene IT-Strategien, IT-Strukturen und die spezifischen Bedarfe des Kunden. Beispielsweise haben wir bei einem unserer Kunden zur technischen Unterstützung ganz pragmatisch Excel-Lösungen entwickelt, da in dem Fall eine toolbasierte Softwarelösung für die Unternehmensgröße unangemessen gewesen wäre.

Macros: Das hört sich nach viel “Papier” an und der Vertriebler würde sagen, dass dadurch kein Euro Prämie geschrieben wird. Die DORA bringt also keinen direkten Geschäftsnutzen, sondern ist reiner Kostenfaktor?

Josch: Auf den ersten Blick ja. Auf den zweiten Blick vermeidet eine angemessene DORA-Umsetzung Kosten. Zum einen dadurch, dass das Risiko einer massiv schädigenden Cyberattacke reduziert wird, wenn man den DORA Vorgaben folgt, d. h. alle Sicherheits-Schwachstellen im Unternehmen analysiert und nach und nach bereinigt. Zum anderen drohen tatsächlich auch von Seiten der Aufsichtsbehörden erhöhte Anforderungen an das Risikokapital des Unternehmens, wenn die DORA Umsetzung unvollständig bleibt und die BaFin Mängel in der IT-Sicherheit des Unternehmens feststellt.

Macros: Das klingt teuer – gibt es also für die DORA-Umsetzung doch einen Business Case?

Josch: DORA verlangt von den Finanzunternehmen ein sorgfältiges Management der IKT-Risiken: Festgestellte Risiken sind mit entsprechend risikomitigierenden Maßnahmen auf ein akzeptables Niveau zu reduzieren. Das schlussendlich verbleibende Nettorisiko muss mit Risikokapital abgedeckt werden. Ein Business Case lässt sich demzufolge aufstellen, wenn man die Kapitalkosten für das erhöhte Risiko den ersparten Aufwendungen für die Umsetzung risikomitigierender Maßnahmen gegenüberstellt.

Macros: Aber zum Spaß-Projekt wird die DORA-Umsetzung dadurch immer noch nicht, oder?

Josch: Tatsächlich hören wir von vielen Versicherungsunternehmen, die über die hohen Aufwände bei der DORA-Umsetzung klagen. Aus unserer Sicht ist es für ein DORA-Umsetzungsprojekt wichtig, DORA nicht nur als Last, sondern auch als Chance für einen erhöhten Schutz der gesamten IT-Struktur des Unternehmens zu sehen. DORA ist inhaltlich richtig und wichtig, denn insbesondere die Risiken von Cyberattacken nehmen dramatisch zu. Auch die Tendenz zur Auslagerung von IKT-Prozessen an Dienstleister und z. B. die Bündelung von Services bei entsprechend spezialisierten Dienstleistern schafft möglicherweise neue Risiken.

Macros: Hast Du ein Beispiel dafür?

Josch: Ein Informationsregister ist zunächst einmal nur lästiges Datensammeln. Wenn es dann aber erstellt ist und die Anzahl an Drittdienstleistern, sowie der Umfang des ausgelagerten Geschäfts und dessen Kritikalität sichtbar wird, wird allen Beteiligten das Risiko z. B. eines Cyberangriffs auf den Dienstleister schlagartig klar. Insbesondere, wenn da Dienstleister genannt werden, die auch von anderen Versicherern genutzt werden und dementsprechend spezifische Geschäftsprozesse bündeln.

Macros: Das ist sicher ein Mehrwert. Aber wie soll ein Versicherer mit diesen Erkenntnissen umgehen und vermeiden, dass er sich dabei verzettelt?

Josch: DORA sollte als Anstoß genutzt werden, lang bestehende hochrisiko-behaftete Sicherheitslücken in der IT des Unternehmens zu schließen oder auch Kompromisse zu bereinigen, die in der Vergangenheit situativ bedingt eingegangen wurden – wir alle kennen den leider wahren Spruch, das nichts länger hält als ein Provisorium. Wenn man diesen nutzenbringenden Aspekt im Blick behält, bekommt man auf ganz natürliche Weise Leitplanken und eine Roadmap, entlang derer sich das Projekt bewegen und immer wieder die Frage beantworten kann, ob man in ein Thema mehr oder weniger an Aufwand und Zeit investiert.

Macros: Auch wenn dadurch eine Orientierung ermöglicht wird, bleibt es dennoch viel Arbeit, die manchmal kein Ende zu nehmen scheint. Sind denn Unternehmen, die sich auf die DORA vorbereitet haben, jemals „wirklich fertig“?

Josch: Nein, Unternehmen sind im Kontext der DORA nie vollständig „fertig“, da sich Bedrohungen und Risiken für die IKT-Sicherheit fortlaufend weiter entwickeln. Gerade kleinere Versicherer können daher die Aufwände allein schwer stemmen. Solche Versicherer profitieren oft davon, auf spezialisierte Dienstleister zurückzugreifen, da sie nur damit die umfangreichen Anforderungen, wie regelmäßige Penetrationstests oder das Management von Drittanbieter-Risiken erfüllen können. Große Versicherer haben zwar häufig interne Ressourcen, benötigen aber meist ebenfalls Unterstützung, sei es für spezialisierte Aufgaben wie Red-Teaming oder bei der strategischen Weiterentwicklung ihrer Prozesse. Die DORA verlangt kontinuierliche Anpassung und Überwachung, insbesondere im Risikomanagement – das ist kein einmaliger Aufwand, sondern ein fortlaufender Prozess.

Macros: Das hört sich nach Schlusswort an. Dann halten wir Dich nicht länger auf, so dass Du weiter in diesem fortlaufenden Prozess arbeiten kannst – dass es da mehr als genug zu tun gibt, daran hast Du keine Zweifel gelassen. Josch, vielen Dank für das Gespräch!

FAZIT: DORA fordert Finanzunternehmen heraus. Gerade mittelständische Versicherer profitieren von externer Expertise für eine effiziente, kostengünstige und zielgerichtete Umsetzung. Frühzeitige Auseinandersetzung mit der DORA ist unerlässlich, um IKT-Risiken zu reduzieren und die digitale Resilienz zu stärken. Macros Reply unterstützt auch Sie gerne – lassen Sie uns reden.

Macros Reply GmbH
Erika-Mann-Strasse 57
80636 München

Tel.+49 89 411142-400
www.macrosreply.de

Macros Reply ist der spezialisierte Technologiedienstleister für die Optimierung von Geschäftsprozessen in den Bereichen Finanzdienstleistungen, Versicherungen und Energiewirtschaft. Macros Reply liefert innovative Lösungen, die Unternehmen dabei unterstützen, ihre Abläufe effizienter und intelligenter zu gestalten. Ob Input-Management, elektronische Postkörbe und Akten, regel- und KI-basiertes Routing oder Dokumentenmanagement: Das Unternehmen liefert nahtlos integrierte 360°-Lösungen und Automatisierung mit GenAI, Machine Learning und RPA, damit sich die Kunden voll und ganz auf ihr Kerngeschäft konzentrieren können. Zusätzlich berät Macros Reply umfassend bei regulatorischen Anforderungen, um höchste Compliance in allen Prozessen zu gewährleisten.