#CYBER & COMPLIANCE

DORA steht vor der Tür: Was Versicherungen wissen müssen

von Tim Glenewinkel · 10. Oktober 2024

Die Uhr tickt: in drei Monaten, am 17. Januar 2025, wird der Digital Operations Resilience Act (DORA) rechtskräftig. Ab diesem Tag können Versicherungen abgestraft werden, wenn sie die Mindestanforderungen der EU-Verordnung an die digitale Resilienz ihrer kritischen Funktionen nicht erfüllen können.

Was bedeutet das für Versicherungen? Wir bieten einen Überblick.

Was ist DORA?

Der Digital Operations Resilience Act DORA ist eine EU-Verordnung, die sicherstellen soll, dass europäische Finanzdienstleister – inklusive Versicherungen – eine resiliente Infrastruktur haben, sodass keine kritische Funktion ausfallgefährdet ist. Dabei geht es sowohl um das Vermeiden von Pannen im Betrieb als auch um die Widerstandsfähigkeit gegen Cyberangriffe.

Kritische Funktionen nach DORA

Eine kritische Funktion liegt nach der DORA-Definition vor, wenn der Ausfall dieser Funktion eine erhebliche Beeinträchtigung …

a. der finanziellen Leistungsfähigkeit,
b. der Geschäftsfortführung oder
c. regulatorischer Art

darstellen würde.

Was bedeutet DORA in der praktischen Umsetzung?

Es ist wichtig zu beachten, dass DORA die gesamte Infrastruktur des Unternehmens betrachtet. Es geht über die reine IT der Versicherung hinaus und betrachtet auch die Mitarbeitenden sowie jegliche involvierte Drittparteien, bspw. Dienstleister, die den Betrieb von Software übernehmen, o. Ä.

Die Anforderungen von DORA decken das IKT-Risikomanagement, das Management des Drittparteienrisikos sowie eine Standardisierung der Meldung von IKT-Vorfällen ab. Neben der technischen Umsetzung von bspw. Fraud Prevention, Identity- und Accessmanagement, einer umfassenden IT-Governance oder des ordnungsgemäßen IT-Outsourcings geht es auch um die Awareness der Mitarbeitenden. Das bedeutet, dass Mitarbeitende einschließlich Geschäftsleitung geschult werden müssen. Vorgesehen ist etwa ein jährliches Aufsichtsgespräch, bei dem der Vorstand in der Lage sein muss, Auskunft zu geben.

Welche Strafen drohen bei Nichtbeachtung von DORA?

Wenn Versicherungen die Anforderungen nicht erfüllen, sieht DORA Strafen vor. Die Behörden können Bußgelder in Höhe von bis zu 10 Milliarden EUR oder 5 % des weltweiten Vorjahresumsatzes verhängen.

Wie groß ist der Umsetzungsaufwand von DORA?

Wie lange die DORA-Umsetzungszeit dauert, hängt von der Ausgangslage sowie der Größe des Unternehmens ab. Nach unseren Erfahrungen liegt der Mindestaufwand bei 300 Personentagen (PT). Bei größeren Häusern mit veralteter und/oder ineffizienter Infrastruktur, die noch keine Änderungen angestoßen haben, kann das Projekt aber auch 800 PT überschreiten.

Das Aufsetzen des Projektes inklusive Gap Analyse, Zielbilddefinition, Benchmarking, Playbook und Roadmap zur Umsetzung kann innerhalb von zehn Wochen erfolgen.

DORA kommt, aber noch ist Zeit zum Handeln!

Der Stichtag für DORA ist der 17. Januar 2025. Das ist nicht mehr lange hin. Zu spät, ein DORA-Projekt anzustoßen, ist es aber nicht. Gerade kleinere Häuser können ihre Infrastruktur innerhalb der gegebenen Zeit noch rechtzeitig resilient transformieren. Für Größere wird die Zeit knapp. Hier gilt: nicht mehr lange zögern! Wir stellen unsere Projekterfahrungen aus zwei Jahren DORA-Umsetzungsprojekten gerne zur Verfügung. Kontaktieren Sie uns über unsere Landingpage.

TAGS: Digital Insurance | DORA | Informationssicherheit | Insurance | Regulatorik

Tim Glenewinkel

KOMMENTARE ANZEIGEN (0)

— VORHERIGER ARTIKEL
SHUK 4.2 – Neue Trends im Standardsoftwaremarkt

NEUESTE ARTIKEL

DORA steht vor der Tür: Was Versicherungen wissen müssen
10. Oktober 2024

SHUK 4.2 – Neue Trends im Standardsoftwaremarkt
26. September 2024

Bearbeitungsstau in der Schadenbearbeitung bei Versicherungen: Innovative Lösungsansätze zur Überwindung von Rückständen (Teil 3)
29. August 2024

TAGS

Cyber
Intelligente Prozessautomatisierung
KI IPA Cysmo Digitalisierung RPA
Blockchain Mal quergedacht Big Data
Projektpraxis Digitale DNA InsurTechs
Cyberwiki Cyberabc
Projektmanagement Innovation
Digital Insurance Fintechs
Prozessautomatisierung Fintech Ökosystem
Insurance Data Analytics Esg Product Owner
Migration Workflow Risikobewertung
Dezentralität SHUK
Digitales Produktmanagement
Informationssicherheit Chatbot EU-DSGVO
Changemanagement Input Management
Testautomatisierung Process Mining
Private Cyberversicherungen Outputmanagement
Scrum Versicherung Digitale Transformation
Regulatorik Darknet

VERWANDTE ARTIKEL

#CYBER & COMPLIANCE

DLP – Des einen Freud, des anderen Leid
von Frederik Wulff · 17. Juli 2024
Data Loss Prevention (DLP) und Data Protection-Systeme sind unverzichtbare Werkzeuge für Organisationen, um ihre sensiblen Daten zu schützen und Compliance-Anforderungen zu erfüllen. Vereinfacht gesagt sind…

#CYBER & COMPLIANCE

ISO 27001:2022 – Der aktuelle internationale Standard für Informationssicherheitsmanagementsysteme
von Frederik Wulff · 6. Juni 2024
Die digitale Transformation hat unsere Welt revolutioniert und Unternehmen jeder Größe und Branche sind zunehmend von digitalen Prozessen und Daten abhängig. Doch mit dieser Abhängigkeit…

#CYBER & COMPLIANCE

Bedrohungsorientierte Red Team Tests: An den richtigen Stellen in Cybersicherheit investieren mithilfe von TIBER-EU
von Vincent Reitemeier · 25. April 2024
Immer häufiger findet man neue Meldungen zu Cyberangriffen auf große Unternehmen und Behörden. Die Auswirkungen: In der Regel haben Opfer hohe finanzielle Schäden, Reputationsschäden sowie…

#CYBER & COMPLIANCE

Versicherungsfall Google?
von Jonas Schwade, Marcel Arnold · 12. Januar 2023
Anwendungen von Google sind praktisch, haben es aber in sich. Denn mir nichts, dir nichts können Daten auf den Servern des US-Mutterkonzerns landen. Für das…