Infosec-Freelancer.de IT Security Consulting

microfin enables transformation.

Wahlweise als Inhouse-Seminar oder Webinar buchbar

Digital Operational Resilience Act (DORA) im Kontext von IKT- und Cloud-Auslagerungen

Zielgruppe: Banken, Finanz- und Zahlungsdienstleister, E-Geld-Institute, Wertpapierunternehmen, Versicherungen, IKT-Anbieter und Cloud-Service-Anbieter

Dauer: ca. 4 Stunden je Teil 1 und 2
Teile einzeln oder zusammen buchbar

Preis: EUR 500,- p. P. je Teil 1 und 2, zzgl. MwSt., zzgl. Reisekosten bei Durchführung vor Ort. Mindestteilnehmerzahl 4 Personen. Im Preis sind die Vorbereitung und die Durchführung des Seminars bzw. Webinars inkl. Unterlagen enthalten.
Bei kleineren oder größeren Gruppen Preis auf Anfrage.

Kurzbeschreibung

Mit DORA hat die EU eine Verordnung zur Stärkung der digitalen Resilienz des Finanzsektors vorgelegt. Damit sollen bestehende Regelwerke unter enger Einbeziehung der europäischen Finanzaufsichtsbehörden EBA, EIOPA und ESMA zugleich harmonisiert und gestärkt werden. Finanz- und Dienstleistungsunternehmen stehen dabei gleichermaßen vor der Frage, wie sich die Anforderungen auf IKT- und Cloud-Auslagerungen auswirken. Seit Jahresbeginn ist die Verordnung wirksam, Finanzunternehmen haben nunmehr Zeit für die Umsetzung bis zum Januar 2025. Höchste Zeit also, sich mit den Anforderungen auseinanderzusetzen.

Unsere Referenten erläutern im ersten Teil die wichtigsten Begriffe, Regelungen und Zusammenhänge und ordnen diese in bereits bestehende Anforderungen im IT-Outsourcing sowie in Anforderungen der Nutzung cloudbasierter Lösungen ein. Der zweite Teil stellt den Bezug vor allem zur IT-Sicherheit her und zeigt, wie sich die Anforderungen in der Praxis bewältigen lassen. Bereiten Sie sich frühzeitig auf das bevorstehende Regelwerk und dessen Umsetzung vor.

Stimmen Sie Ihren individuellen Bedarf in einem persönlichen Gespräch mit uns ab

Irina Shapiro

+49 6172 . 177 63 175
anfrage@microfin.de

Übersicht Inhalte Teil 1

Einordnung DORA als Teil des EU-Maßnahmenpakets zur Digitalisierung des Finanzsektors
Zielsetzung und Begriffsbestimmung wie bspw. „digitale Resilienz", „digitale Betriebsstabilität, „Cyber-Abwehr", „Cyber-Hygiene" und „Cyber-Reife"

Rolle und Verantwortung europäischer Aufsichtsbehörden im Zusammenhang mit DORA sowie Rechtsverbindlichkeit im Verhältnis zu nationalen aufsichtlichen bzw. regulatorischen Vorgaben in Deutschland

- Einblicke in die europaweite IT-Regulierung des Finanzsektors
- DORA und die Rolle der European Banking Authority (EBA), European Securities and Markets Authority (ESMA), European Insurance and Occupational Pensions Authority (EIOPA), The European Union Agency for Cybersecurity (ENISA), European Central Bank (ECB)
- Einordnung von DORA im Hinblick auf KWG, MaRisk und BAIT sowie VAG, MaGo und VAIT, insbesondere mit Blick auf sachliche Abhängigkeiten und Abgrenzungen bei IKT-Auslagerungen und Cloud-Nutzung

Potenzieller Adressatenkreises von DORA und die damit verbundene weite Auslegung des Begriffs „Finanzunternehmen" inkl. Beispiele

Erläuterung der wesentlichen Inhalte der einzelnen Regelungsbereiche von DORA sowie damit verbundene Betrachtung praktischer Auswirkungen auf IKT-Auslagerungen und Nutzung cloudbasierter Lösungen

- Einrichtung einer Governance zur IT-Resilienz
- IKT-Risikomanagement
- Meldung IKT-bezogener Vorfälle
- Pflicht zur Überprüfung der IT-Resilienz
- Umgang mit Risiken von IKT-Drittanbietern
- Informationsaustausch mit anderen Finanzunternehmen

Wesentliche Auswirkungen auf IKT-Auslagerungs-/Ausgliederungs-verträge inkl. Beispiele

Infosec-Freelancer.de, IT Security Consulting
Milcheshohl 35b
61462 Königstein im Taunus
www.infosec-freelancer.de

microfin Unternehmensberatung GmbH
Rathausplatz 12
61348 Bad Homburg
www.microfin.de

Übersicht Inhalte Teil 2

Auf DORA vorbereiten: Maßnahmen zur Mitigation und zur Erreichung einer höheren Abwehrreife

Methoden und Mittel zur Prüfung der digitalen Betriebsstabilität

- **Software-Supply-Chain-Sicherheit** – Qualitätssicherungsmaßnahmen zur Bewertung von Fremdartefakten in der IT-Umgebung – (GitLab Stars, Anzahl Commits, Verbreitung, Peer Reviews etc.)
- **Scan-Lösungen & Runtime Protection** – statische Code-Analyse (TFSec, checkov, Sonarcube etc.), Runtime Protection und Layer-7-Überwachung
- **Schutz vor Ransomware** – Desaster Recovery und die erweiterte 3-2-1-1-0-Regel für Backup und Restore
- **Netzwerk- und Kommunikationssicherheit** – Die Zero-Trust-Idee oder „Perimeter waren gestern". Was davon nützt wirklich, und wo sollten Sie zuerst ansetzen?
- **Threat Intelligence Services** – Der richtige Fokus: Technik unterstützt, aber wer nur einen Hammer hat, hält jedes Problem für einen Nagel.
- **To SIEM or not to SIEM** – Warum klassisches Security Information & Event Management nicht mehr zeitgemäß ist.
- **Risiko Innentäter** - Was hat es eigentlich mit PAM auf sich, und welche Rolle spielen funktionierende IAM-Prozesse dabei?

Informationsaustausch zur Früherkennung und Vermeidung von Ansteckungseffekten

- **Austauschformate** – Was gibt es schon, was funktioniert? Was ist standardisiert? Kocht die Aufsicht hier ihr eigenes Süppchen?
- **STIX 2.1** – Structured Threat Information Expression (STIX) ist eine Sprache und ein Serialisierungsformat für den Austausch von Informationen über Cyberbedrohungen.
- **TAXII 2.1** – Trusted Automated Exchange of Intelligence Information (TAXII) ist ein Anwendungsschicht-Protokoll für die einfache und skalierbare Kommunikation von Informationen über Cyber-Bedrohungen. Es wurde speziell für den Austausch von in STIX dargestellter Cyber Threat Intelligence (CTI) entwickelt, ist aber nicht auf STIX beschränkt.

Nach Bedarf: Allgemeine Ableitung und erste Bewertung möglicher Auswirkungen für Ihr Unternehmen
(gilt für Teil 1 und 2)

Steffen Müller, Infosec-Freelancer.de
Mein Claim: „Ohne Durchblick keine Sicherheit!"

Mit dem be@ware Ansatz etabliere ich mit Ihrem Team gemeinsam eine durchgängige Strategie und verständliche Sicherheitsarchitektur mit Durchblick, die Angriffe auf Ihre IT-Infrastruktur früher entdeckt, das Schadenrisiko reduziert und schneller zum Normalablauf zurückführt.

microfin Unternehmensberatung

microfin ist eine auf IT-Transformationen spezialisierte Beratung. Wir lieben den technologischen Fortschritt und die damit verbundenen komplexen Herausforderungen. Immer nach vorne schauend, schaffen wir einen neuen Status quo, damit die Komplexität in der IT trotz des zunehmenden Veränderungstempos beherrschbar bleibt.

Auf diese Weise helfen wir Unternehmen, durch den intelligenten Einsatz von Cloud, Outsourcing und Big Data & AI echte Innovationssprünge zu machen und sich dauerhaft für die Zukunft zu positionieren.

Mit Beratung, Lösungen und Wissensaufbau befähigen wir Menschen und Unternehmen, Transformation zu gestalten.

microfin – driven by enabling transformation

Ihre DORA-Experten und -Trainer

Sebastian Dosch
microfin
Principal Consultant & IT-Volljurist

+49 151 . 52 617 47 2
s.dosch@microfin.de

Stefan Wendt
microfin
Managing Partner

+49 172 . 69 800 21
s.wendt@microfin.de

Steffen Müller
Infosec-Freelancer.de
vCISO & vTISO

+49 6174 . 221314
steffen.mueller@infosec-freelancer.de

Infosec-Freelancer.de, IT Security Consulting
Milcheshohl 35b
61462 Königstein im Taunus
www.infosec-freelancer.de

microfin Unternehmensberatung GmbH
Rathausplatz 12
61348 Bad Homburg
www.microfin.de