SC175 DORA - Der Countdown läuft

Kurzbeschreibung:

Der Digital Operational Resilience Act (DORA) ist ein wichtiger Bestandteil der digitalen Finanzstrategie der Europäischen Union, der darauf abzielt, die Cybersicherheit und die operative Widerstandsfähigkeit des Finanzsektors zu stärken. Angesichts der zunehmenden Digitalisierung der Finanzdienstleistungen und der damit verbundenen Cyberbedrohungen ist DORA eine Antwort auf die dringende Notwendigkeit, ein einheitliches Regelwerk zu schaffen, das die Sicherheit und Stabilität des Finanzsystems in der EU gewährleistet.

Die im Workshop **SC175 DORA - Der Countdown läuft** behandelten Schlüsselaspekte von DORA sind:

1. **Risikomanagement:** Unternehmen müssen ein solides IT-Risikomanagement etablieren, das regelmäßige Assessments und Tests umfasst.
2. **Incident Reporting:** Es gibt klare Vorgaben für die Meldung von Sicherheitsvorfällen, um eine schnelle Reaktion und Begrenzung von Schäden zu ermöglichen.
3. **Digitale Operational Resilience Testing:** Unternehmen müssen regelmäßige Tests ihrer digitalen Widerstandsfähigkeit durchführen, einschließlich Penetrationstests und Szenarioanalysen.
4. **Management von Drittanbieter-Risiken:** Finanzinstitute müssen sicherstellen, dass ihre Drittanbieter, einschließlich Cloud-Dienste, ebenfalls hohe Sicherheits- und Resilienzstandards erfüllen.
5. **Aufsichtsrahmen:** DORA etabliert einen EU-weiten Aufsichtsrahmen, der eine kohärente Anwendung der Vorschriften gewährleisten soll.

Die Bafin formuliert in ihrer Aufsichtsmitteilung vom Juni/2024 wichtige Informationen als Erläuterung zur DORA zum Thema **„Stärkung von Schulung und Kommunikation“**
DORA betont Schulungspflichten deutlich stärker als BAIT/VAIT. So haben Finanzunternehmen für ihre Mitarbeiter und die Geschäftsleitung Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz zu entwickeln (Art. 13 Abs. 6 DORA). Darüber hinaus haben die Mitglieder des Leitungsorgans ihre Kenntnisse und Fähigkeiten zu IKT-Risiken auf dem neusten Stand zu halten, auch durch spezielle Schulungen (Art. 5 Abs. 4 DORA). Generell sollen die Schulungen auf den Aufgabenbereich abgestimmt sein und ggf. auch eingesetzte IKT-Drittdienstleister abdecken.

Zielgruppe:

- IT-Verantwortliche
- Security-Verantwortliche
- Compliance- und Risikomanagement-Fachkräfte
- Start-ups von FinTech-Unternehmen
- BCM-Verantwortliche
- Führungskräfte
- Drittanbieter und IT-Dienstleister für den Finanzsektor

Voraussetzungen:

Interesse und Fähigkeit, querschnittliche Themen aus GRC und Security zu verbinden.

Sonstiges:

Dauer: 3 Tage

Preis: 2350 Euro plus Mwst.

Ziele:

Das Training **SC175 DORA - Der Countdown läuft** gibt einen Überblick für Anforderungen, Begrifflichkeiten, Zusammenhänge, Pflichten im Kontext Dora. Die Teilnehmer werden nicht nur mit den DORA-Anforderungen vertraut gemacht, sondern erhalten auch Einblicke in eine mögliche Implementierung von Strategien zur Erhöhung der digitalen Resilienz: durch Fallstudien, Best Practices und Diskussionen über die Herausforderungen und Lösungen bei der Umsetzung von DORA in verschiedenen Typen von Finanzinstitutionen.

Im Fokus steht die Bedeutung einer Kultur der Cybersicherheit, die von der Führungsebene gelebt und durch das ganze Unternehmen getragen wird.

Inhalte/Agenda:

- **Einführung**
- ♦ **Einführung in die Digital Operational Resilience Act (DORA)**
  - ◊ Grundlegende Definition und Zielsetzung
  - ◊ Hintergrund und Vorteile der Einführung
- ♦ **Wer ist betroffen? Bedeutung und Ziele von DORA**
  - ◊ Betroffene Sektoren und Unternehmen
  - ◊ Hauptziele: Einhaltung der vier Schutzziele
- ♦ **Übersicht und Struktur von DORA sowie der begleitenden Dokumente**
  - ◊ Grundsätzliche Struktur von DORA
  - ◊ Erläuterung der RTS (Regulatory Technical Standards), ITS (Implementing Technical Standards) und Guidelines
- ♦ **Vereinfachte Strukturmöglichkeiten von DORA?**
  - ◊ Wie können Unternehmen DORA effektiv in ihre bestehende Struktur integrieren?
- ♦ **Ableitung DORA aus dem allgemeinen Resilienz-Konzept**
  - ◊ Vergleich mit bestehenden Resilienz-Konzepten und Rahmenwerken Governance, Risk Management und Compliance (GRC)
  - ◊ Informationsmanagementsysteme
- ♦ **Schwerpunkt und Inhalte der DOR-Strategien**
  - ◊ Anforderungen an eine Strategie für die operationale Resilienz
  - ◊ Fokussierung auf das IKT-Risikomanagement
- ♦ **Technische Anforderungen**
  - ◊ Spezifische Anforderungen an Informations- und Kommunikationstechnologie (IKT)
  - ◊ Implementierung und Überwachung
- ♦ **Mögliche Vorgehensweisen und Erfolgsfaktoren zur Einführung von DORA**
  - ◊ Erfolgsfaktoren und Best Practices
  - ◊ Bedeutung des richtigen Mindsets
  - ◊ Strategien für erfolgreiches Veränderungsmanagement
  - ◊ Konzept der Dalton-Methode für die Unternehmensmultiplikation
- ♦ ◊

- **Vertiefung DORA durch (Mini)-Workshops und Best Practices**
- ♦ **Business Continuity Management (BCM)**
  - ◊ Herausforderungen durchzunehmende Cyberangriffe und Risiken der Betriebsstabilität
  - ◊ Auswirkungen von DORA auf das Notfallmanagement
  - ◊ Aufbau eines effektiven BCM/DR-Programms
  - ◊ Praxisempfehlungen für BCM und IT-Notfallmanagement
- ♦ **IKT-Risikomanagement (z.B. Cobit, ISMS nach ISO 27001)**
  - ◊ Gruppenübung zur Erstellung eines IKT-Risikomanagement-Plans
- ♦ **Cloud Computing im Kontext der BaFin (Feb. 2024)**
  - ◊ Grundlagen des Cloud Computing
  - ◊ Cloud Security
  - ◊ Anforderungen der BaFin und deren Umsetzung
- ♦ **Incident Management**
  - ◊ Prozesse zur Erkennung und Bewältigung von IKT-Vorfällen
  - ◊ Meldepflichten und Berichtswesen
- ♦ **Resilienztests**
- ♦ ◊ Durchführung von Basis- und Fortgeschrittenen-Tests
  - ◊ Planung eines Threat-Led Penetration Tests (TLPT)
- ♦ ◊

- **Abschluss und Q&A**
- ♦ Zusammenfassung der wichtigsten Punkte
- ♦ Offene Fragerunde und Diskussion
- ♦

Am ersten Tag sind Sie herzlich zum gemeinsamen Abendessen eingeladen. In entspannter Atmosphäre können Sie Erfahrungen mit anderen Teilnehmern austauschen und unterschiedliche Sichtweisen beleuchten.