GSE - Arbeitskreis BCM

DORA (Digitale Betriebsstabilität im Finanzsektor)
Was kommt auf die Unternehmen zu?

IT Notfall-/Kontinuitätsmanagement (Wolfgang Kubelka, 05.12.2023)

DORA – Digitale Betriebsstabilität

Zeitachse bis zur geplanten Anwendung

2020

- Veröffentlichung von DORA durch die EU-Kommission

2022

- Inkrafttreten der Verordnung durch Veröffentlichung in der EU

2023/24

- Erstellung von Leitlinien und technischen Standards hinsichtlich der Regulierung (RTS) & Implementierung (ITS)

2025

- Anwendung der Verordnung mit ihren Anforderungen an die Resilienz im Finanzsektor in den Ländern

DORA – Digitale Betriebsstabilität

Ziele und Zielgruppe

- Gewährleistung der **Finanzstabilität**, des **Verbraucherschutz** und der **Marktintegrität**
- Beseitigung regulatorischer Hindernisse im Finanzsektor durch eine **Rechtsharmonisierung**
- EU-weites, Sektor übergreifendes Framework, um **Risiken im Zusammenhang mit Informations- und Kommunikationstechnologien (IKT-Risiken) zu steuern** und zu mindern

Betroffen sind

- traditionelle Finanzakteure wie Banken, Versicherungen und Investmentgesellschaften,
- sowie Fin- und Hightechs, Krypto-Dienstleister
- und Handelsplätze

ab einer gewissen Größe.

DORA – Digitale Betriebsstabilität
Kernelemente

DORA (Digital Operational Resilience Act)

Operational Resilience und Risikomanagement
→ Etablieren von professionellen IKT-Sicherheitssystemen und **Maßnahmen zum Schutz gegen Angriffe**
→ Einführung von **Business-Continuity-Richtlinien,** sowie **Notfall- und Wiederherstellungsplänen**

Berichterstattung von Vorfällen
→ Prozessentwicklung zur **Identifizierung**, **Protokollierung** und **Klassifizierung von Vorfällen**
→ Vollumfängliche **Berichtserstattung** im Falle eines IKT-Vorfalls (Anfangs-, Zwischen-, und Abschlussstand)

Digital Operational Resilience Testing
→ regelmäßiges **Testen (jährlich)** der Maßnahmen und Systeme
→ alle **3 Jahre Penetrationstests** (TLPT = Threat Led Penetration Testing – strukturierte Angriffssimulation)
→ umgehende **Gegenmaßnahmen bei bekannten Schwachstellen**, Mängeln oder Lücken

Governance und Management von Drittparteien
→ **vollständiges Register** aller ausgelagerten Aktivitäten einschließlich gruppeninterner Dienstleistungen
→ Risiken aus internen und ausgelagerten Verantwortungsbereichen (**Konzentrations- und Auslagerungsrisiken**)
→ ausreichende **Überwachung der Risiken durch Drittanbieter** (Vertrag, Leistung, Erreichbarkeit, Standort RZ)

Informationsaustausch
→ Informationen und Erkenntnisse über **Cyberbedrohungen** im Finanzsektor
→ **Prozesse zur Überprüfung von geteilten Informationen** und dem entsprechenden Ergreifen von Maßnahmen

DORA – Digitale Betriebsstabilität
Umsetzung (1/2)

- ✓ **Investitionen** in IT-Sicherheitstechnologien

- ✓ **Zusammenarbeit** mit IT-Sicherheitsdienstleistern

- ✓ **Identifizieren** kritischer Geschäftsprozesse und **Risiko minimierende Maßnahmen** umsetzen:
  - → Prozesse sind auch im Falle von Störungen weiterhin zu unterstützen (**Service-/Notfallbetrieb**)
  - → **Abhängigkeiten von Drittanbietern überprüfen** (IT-Dienstleister, Cloud-Service-Provider)
  - → **GAP-Analyse orientiert an Vorgaben der EU**,
    um Lücken zu entdecken und sinnvolle Maßnahmen zu treffen

- ✓ **aktuelle Vorgaben überprüfen** und ggf. Roadmap entwickeln, d. h.
  DORA-Vorgaben in weiten Teilen kongruent mit Vorschriften aus bekannten Regularien, vor allem
  - → MaRisk und BAIT/KAIT/ZAIT,
  - → EBA-Guidelines für Outsourcing von Aktivitäten und
  - → EBA-Guidelines on ICT and Security Risk Management
  - → bestehenden Melde- und Risikomanagementpflichten beachten

DORA – Digitale Betriebsstabilität

Umsetzung (2/2)

✓ **Durchführen von ausführlichen Penetrationstests (TIBER-DE)**

TIBER-DE = Threat Intelligence-based Ethical Red Teaming for the German Financial Sector

→ Rahmenwerk für die Durchführung von Simulationen von Cyberangriffen

→ Ziel: Widerstandsfähigkeit gegenüber Cyberangriffen zu erhöhen

→ realistische Simulation eines Angriffs wird durchgeführt

✓ **Schulung von Mitarbeitern**

→ Mitarbeiter regelmäßig in Bezug auf Cyber-Security schulen

→ sicherstellen, dass diese in Sachen Sicherheitsvorkehrungen auf dem neuesten Stand sind

→ Ziel: Bewusstsein für Cybersicherheitsrisiken schärfen

✓ **Umgang mit Drittanbietern für digitale Dienstleistung**

→ Trend: IKT-Funktionen auslagern an Drittanbieterunternehmen

→ EU-Aufsichtsrahmen für IKT-Drittanbieter: Risiken beurteilen, Empfehlungen aussprechen

→ Dienstleistung von „kritischen Drittanbietern“ sind entsprechend zu begegnen

→ im Ausnahmefall könnte Aufsichtsbehörde sogar Kündigung von Verträgen anordnen

DORA – Digitale Betriebsstabilität
Zusammenfassung

Rechtsharmonisierung in der EU

Resilienz durch Zusammenarbeit im Finanzsektor

Zentrales Auslagerungsregister

Pentrationtest – Tiber-DE (strukturierte Angriffssimulation)

Zentrales Register bekannter Schwachstellen

Resilienz durch Zusammenarbeit der 2nd Line Rollen im Unternehmen

übergreifendes Risikomanagement

Auslagerungs- und Servicemanagement

Informations-/IT-/Cyber-Sicherheit

BCM/Notfall-/Kontinuitätsmanagement

Fragen, Diskussion, Anregungen