ÖSTERREICHISCHE
FMA · FINANZMARKTAUFSICHT

IT-SICHERHEIT

Karl Machan, CRM
Graz, 24.09.2021

INHALTSVERZEICHNIS

Digital Operational Resilience Act (DORA)

ZIEL:

- Schaffung eines einheitlichen Rechtsrahmens für die digitale operationelle Widerstandsfähigkeit von Finanzdienstleistungen

VON DORA UMFASSTE UNTERNEHMEN:

- Kreditinstitute
- Zahlungsinstitute
- Kontoinformationsdienstleister
- E-Geld-Institute
- **Wertpapierfirmen**
- Krypto-Asset-Dienstleister, Emittenten von Krypto-Assets, Emittenten von Asset-referenzierten Token und Emittenten von signifikanten Asset-referenzierten Token
- zentrale Wertpapierverwahrstellen
- zentrale Gegenparteien
- Handelsplätze
- Transaktionsregister
- **Manager von alternativen Investmentfonds**
- Verwaltungsgesellschaften
- Datenmeldedienstleister
- Versicherungs- und Rückversicherungsunternehmen
- Versicherungsvermittler und Rückversicherungsvermittler
- Einrichtungen zur betrieblichen Altersversorgung
- Kreditrating-Agenturen
- Administratoren von kritischen Benchmarks

Digital Operational Resilience Act (DORA)

HERAUSFORDERUNG:

- Unternehmen sehr unterschiedlich (von systemrelevanten Instituten bis zu Versicherungsvermittler)
- FMA - Laufende Mitgestaltung DORA und Unterstützung des BMF
  - Proportionalität

VORLÄUFIGER ZEITPLAN:

- Inkrafttreten: 2022/2023?
- Übergangsfristen: 2 Jahre nach Inkrafttreten

INHALT:

IT-Governance, Organisation und IT-Risikomanagement:

- **Leitungsorgan** ist für das **IT-Risikomanagement verantwortlich**
- Klare **Aufgaben**- und **Zuständigkeitsverteilung** für alle **IT-bezogenen Funktionen** sind festzulegen
- Bestimmung des angemessenen **Risikotoleranzniveaus der IT-Risiken** im Unternehmen
- solides, umfassendes und gut dokumentiertes **Rahmenwerk für das IT-Risikomanagement** (Strategien, Richtlinien, Verfahren, IT-Protokolle, etc.)
- **Analyse der IT-Risiken** (Identifizierung, Klassifizierung, Bewertung, etc.)
- Einführen eines **Informationssicherheitsmanagementsystems**

IT-Governance, Organisation und IT-Risikomanagement

- **Strategien**, **Richtlinien** und **Verfahren**, um sämtliche IT-Systeme angemessen zu schützen (insbesondere in Bezug auf **Vertraulichkeit**, **Verfügbarkeit** und **Integrität**)
  - solides **Netzwerk-** und **Infrastrukturmanagement**
  - Steuerung des physischen und virtuellen **Zugriffs auf Ressourcen** und **Daten** des IT-Systems
  - starke **Authentifizierungsmechanismen**
- Erstellung einer **IT Business Continuity Policy** (dokumentierte Pläne, Verfahren, etc.) und Erstellung eines **IT-Notfallwiederherstellungsplans**
- Erstellung einer **Sicherungsrichtlinie** (Backup)
- Dokumentation der **Wiederherstellungsmethoden**
- Bereitstellung von angemessenen Ressourcen
- Erstellung von **Kommunikationsplänen bzw. -richtlinien** (Offenlegung von IT-bezogenen Vorfällen oder größeren Schwachstellen gegenüber Kunden bzw. der Öffentlichkeit)

Meldung schwerwiegender IT-bezogener Vorfälle

- Einrichtung eines IT-bezogenes **Incidents Management** (Vorfallsmanagement-) **Prozesses**
- Dieser beinhaltet Verfahren zur Identifizierung, Verfolgung, Protokollierung, Kategorisierung und Klassifizierung von IT-bezogenen Vorfällen)
- Zuweisung von **Rollen** und **Verantwortlichkeiten** im Falle von IT-bezogenen Vorfällen
- Kommunikationspläne (Benachrichtigung an Kunden, interne Eskalationsverfahren, etc.)
- Einrichtung von IT-bezogenen Verfahren zur Reaktion auf Vorfälle, um die Auswirkungen zu mindern und sicherzustellen, dass die IT-Dienste rechtzeitig betriebsbereit und sicher sind.
- Meldung von schwerwiegenden Vorfällen in Form eines Berichts an die FMA
- Wenn ein schwerwiegender IT-Vorfall Auswirkungen auf die finanziellen Interessen von Dienstnutzern und Kunden hat, müssen diese unverzüglich über den schwerwiegenden IT-bezogenen Vorfall informiert werden

Prüfung der digitalen Betriebsstabilität (Digital Operational Resilience Testing)

- Unternehmen sollen über ein **Programm** verfügen, um IT-bezogene Vorfälle zu bewerten, Schwachstellen, Mängel oder Lücken in der Ausfallsicherheit des digitalen Betriebs festzustellen zu können
- Programm zur **Prüfung der digitalen Betriebsstabilität** als Bestandteil des **IT-Risikomanagements**
- Tests durch **unabhängige Parteien** (intern/extern)
- Verfahren zur **Priorisierung**, **Klassifizierung** und **Behebung** von erkannten Problemen
- interne Validierung, um sicherzustellen, dass alle festgestellten Schwachstellen, Mängel oder Lücken vollständig behoben sind
- **Kritische Systeme** und **Anwendungen** sind mindestens **jährlich** zu testen
- Programm zur Prüfung der Ausfallsicherheit umfasst **Schwachstellenbewertungen** und -**scans**, **Open Source-Analysen**, **Prüfung der Netzwerksicherheit**, **Penetrationstests**, **Quellcode-Überprüfungen**, etc.

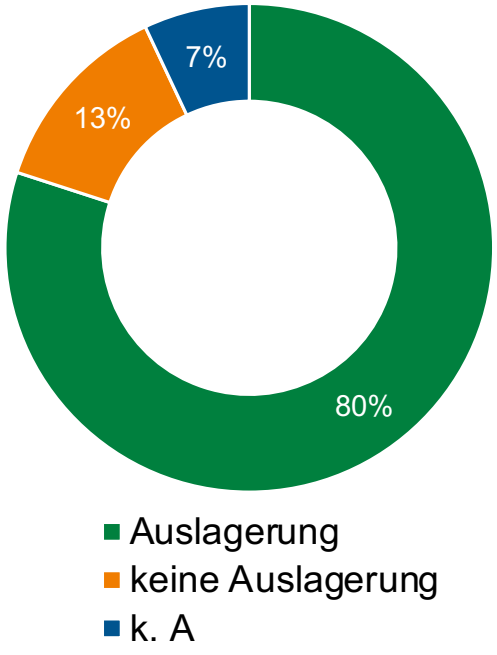
Steuerung des Risikos durch IT-Drittanbieter

- **Drittanbieter-Risiko** (Outsourcing-Risiko) ist integraler **Bestandteil** des **IT-Risikomanagements**
- **Register** aller vertraglichen Vereinbarungen zu **IT-Diensten von Drittanbietern**
- Zeitnahe **Meldung** von geplanten wichtigen/kritischen Vergaben an Drittanbieter an die **Aufsicht**
- **Due Diligence-Prüfungen** für potenzielle IT-Drittanbieter durchführen, um die **Geeignetheit** des IT-Drittanbieter sicherzustellen
- Anforderungen in Bezug auf vertragliche Vereinbarungen zwischen IT-Drittanbietern und Finanzunternehmen
  - Zugangs-, Prüf- und Einschaurechte
  - Regelungen zur Vertragsbeendigung, Ausstiegsszenarien
  - Etc.

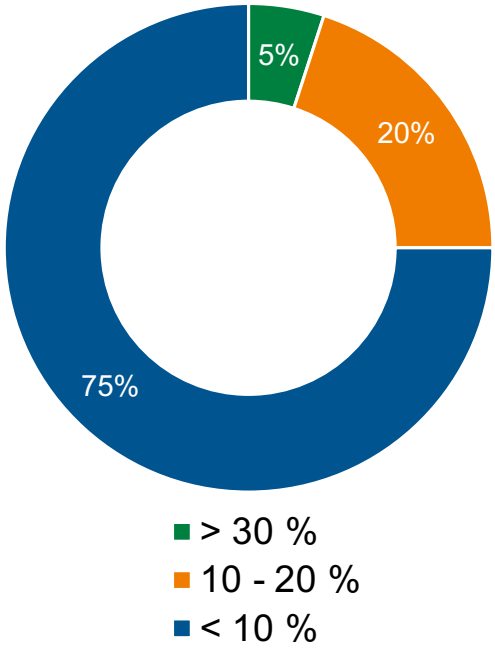
Erkenntnisse Analysefragebogen zum Thema IT

ERKENNTNISSE ANALYSEFRAGEBOGEN

IT-VERWALTUNG



Prozentueller Anteil der IT-Kosten an den Betriebsaufwänden



ERKENNTNISSE ANALYSEFRAGEBOGEN

Automatisierung der Erbringung von Wertpapierdienstleistungen

Von 111 befragten Unternehmen:

- **Anlageberatung**
  - 15 Teilautomatisierung
- **Portfolioverwaltung**
  - 20 Teilautomatisierung
  - 1 Vollautomatisierung
- **Annahme und Übermittlung**
  - 17 Teilautomatisierung
  - 1 Vollautomatisierung

ERKENNTNISSE ANALYSEFRAGEBOGEN

IT-Sicherheitsvorfälle:

Von 111 befragten Unternehmen:

- 7 betroffene Unternehmen
  - Kein finanzieller Schaden
  - Phishing, gefälschte e-mails, Virenbefall

Regelmäßige Sicherheitsüberprüfungen:

- **44 % der Unternehmen führen keine regelmäßigen Sicherheitsüberprüfungen durch!**

IT-Notfallplan:

- **22 % der Unternehmen verfügen über keinen IT-Notfallplan!**

ERKENNTNISSE ANALYSEFRAGEBOGEN

Cloud-Services:

- **50 % der Unternehmen nehmen Cloud-Services in Anspruch**
- **ESMA - Leitlinien zur Auslagerung an Cloud-Anbieter**
  - **Die Leitlinien gelten ab dem 31. Juli 2021 für alle Auslagerungsvereinbarungen mit Cloud-Anbietern, die an oder nach diesem Tag geschlossen, verlängert bzw. geändert werden**
  - **Die Unternehmen sind dazu angehalten, bestehende Auslagerungsvereinbarungen mit Cloud-Anbietern zu überprüfen und entsprechend zu ändern, um sicherzustellen, dass sie diese Leitlinien ab dem 31. Dezember 2022 berücksichtigen**
  - **FMA-Homepage unter „Recht->EU->ESMA-Leitlinien und andere Konvergenzinstrumente“**

FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz