- Informationssicherheitsrisiken, denen das Unternehmen ausgesetzt ist, festzustellen und zu bewerten;
- Maßnahmen, einschließlich Kontrollen, zur Minderung von Informationssicherheitsrisiken festzulegen;
- die Wirksamkeit dieser Maßnahmen zu überwachen und bei Bedarf weitere Maßnahmen zu ergreifen;
- dem Management Board über Informationssicherheitsrisiken und Kontrollen zu berichten;
- festzustellen und zu beurteilen, ob es Informationssicherheitsrisiken gibt, die auf eine größere Änderung des ISMS (Information Security Management System), der Systeme, Dienste, Prozesse oder Verfahren und/oder einen erheblichen Betriebs- oder Sicherheitsvorfall zurückzuführen sind.

Zusammengefasst sollen Risiken im Rahmen eines kontinuierlichen Prozesses systematisch identifiziert, analysiert, behandelt (vermeiden, mitigieren, verlagern oder akzeptieren) und berichtet bzw überwacht werden. Mit dem Informationsrisikomanagement können Chancen genutzt und (langfristig) Schäden mit einer hohen negativen Auswirkung auf den laufenden Geschäftsbetrieb oder das Unternehmensergebnis vermieden oder transferiert werden.

Ziel ist es, die IT-Sicherheit auf ein für das Unternehmen sinnvolles und betriebswirtschaftlich vertretbares Niveau zu bringen und dort zu halten. Somit ist Informationssicherheitsrisikomanagement immer auch Aufgabe der Geschäftsleitung und es ist essenziell, dafür die notwendigen Ressourcen im Sinne von Personal und Know-how zur Verfügung zu stellen.

3.2. IT-Risikomanagement in Finanzunternehmen mit besonderem Fokus auf Banken

IT-Risikomanagement hat im digitalen Zeitalter in der Finanzbranche einen großen Stellenwert und stellt einen wichtigen Bestandteil der IT-Strategie dar.

Zur systematischen Steuerung der IT-Risiken können verschiedene Methoden herangezogen werden. In diesem Beitrag liegt der Fokus auf der „CRISAM"-Methode, die auch im österreichischen Finanzsektor im Einsatz ist. CRISAM steht für „Corporate Risk Application Method" und ist eine ganzheitliche Methode zur Implementierung eines Information-Risk-Management-Prozesses.

Ziel ist es, alle aus IT-Systemen und Anwendungen resultierenden Risiken für das Unternehmen systematisch zu identifizieren, aufzuzeigen, zu bewerten und entsprechende Maßnahmen zu setzen (behandeln, akzeptieren, verlagern etc).

Mit dem in CRISAM festgelegten und der dem ISO 31000 Standard (Norm für Risikomanagement) entsprechenden Vorgehensmodell sollen mögliche negative Auswirkungen auf den laufenden Geschäftsbetrieb vermieden oder entsprechend

Server nur zu Beginn der Verbindung eine Abfrage von „Credentials" (zB Benutzernamen, Passwort, digitale Schlüssel etc) erfolgt. Ist die Authentizität dieser Credentials bestätigt, vereinbaren die beiden Computersysteme einen Token (auch als „Cookie" bezeichnet), also eine eindeutige Kennung, mit der beide die Datenverbindung (Sitzung oder „Session") wiedererkennen. Diese Wiedererkennung ist notwendig, da Daten im Internet über das „Transfer Control Protocol" (TCP) übertragen werden, welches mehrere parallele Verbindungen zulässt. Der Token ermöglicht Sender und Empfänger, diese einzelnen Verbindungen wieder zusammenzuführen.

Hat ein Angreifer aber nun die Möglichkeit, diesen „Session-Token" zu stehlen oder zu erraten, kann er eine weitere Verbindung aufbauen, die als reguläre, überprüfte Sitzung erkannt wird, obwohl dies nicht der Fall ist. Diese Session-Token sollten im Normalfall nicht für Dritte erreichbar sein, dies kann aber durch Software- oder Konfigurationsfehler bzw durch „Adversary-in-the-Middle"-(AitM, siehe Kap 4.2.3.8.3.)-Angriffe oder Cross-Site-Scripting (als Methode zum Stehlen von Cookies, siehe Kap 4.2.3.7.2.) dennoch der Fall sein.

4.2.3.7.2. Cross-Site-Scripting

Cross-Site-Scripting (XSS) ist eine Art von Sicherheitslücke, die typischerweise in Webanwendungen gefunden wird. Sie tritt auf, wenn ein Angreifer bösartige Skripte in Inhalte von ansonsten vertrauenswürdigen Webseiten einfügen kann. Diese Art von Angriff kann das Vertrauen eines Benutzers in eine bestimmte Website ausnutzen und bösartige Skripte im Kontext des Browsers des Benutzers ausführen. Die gängigste technische Vorgangsweise ist dabei die Ausnutzung von Schwachstellen in Webanwendungen auf Seite der Server. Das Kernproblem ist dabei die Umgehung der „same origin policy", die dazu dient, verschiedene Websites voneinander zu trennen, wodurch Angreifer auf Daten und Funktionen zugreifen können, die sie sonst nicht erreichen könnten. Schutzmaßnahmen umfassen die richtige Validierung und Filterung von Eingaben sowie die Verwendung von sicheren Programmierpraktiken.

4.2.3.7.3. Drive-by attacks

Eine weitere Technik, um das Vertrauen in bekannte oder vermeintlich sichere Informationsquellen auszunutzen, sind „Drive-by"-Angriffe. Dabei wird versucht, Schadsoftware zwischen legitimen und ungefährlichen Inhalten einzuschleusen, um sie dem Ziel „im Vorbeilaufen" anzubieten. Ein einfaches Beispiel dafür ist das Anzeigen von Werbung auf einer legitimen Webseite, die Schadcode enthält. Da Werbebanner in der Regel von den anzeigenden Webseiten automatisiert von Werbeanbietern bezogen und nicht einzeln geprüft werden, kann auf diese Art Schadsoftware auf einer Website untergebracht werden, ohne dass diese dem Websiteverantwortlichen bewusst ist.

Wendet man dieses Klassifikationsschema auf einen identifizierten Vorfall an, muss zu Beginn geprüft werden, ob dieser Vorfall negative Auswirkungen auf kritische Dienste bzw Services hat bzw haben kann. Ist dies nicht der Fall, liegt kein schwerwiegender Vorfall vor. Wesentlich ist, dass **jeder erfolgreiche böswillige unbefugte Zugriff auf Netzwerk- und Informationssysteme** als schwerwiegender IKT-bezogener Vorfall zu klassifizieren ist. Hat (noch) kein erfolgreicher unbefugter Zugriff stattgefunden, müssen insgesamt sechs Entscheidungskriterien geprüft werden. Ist keines oder nur eines dieser Kriterien anwendbar, kann dieser Vorfall als nicht schwerwiegend klassifiziert werden. Treffen zwei oder mehr Kriterien zu, ist der Vorfall als schwerwiegend zu klassifizieren.

Anhand der nachfolgenden Tabelle werden die Entscheidungskriterien und -bedingungen aus dem RTS zusammengefasst, um die Einstufung als schwerwiegender IKT-bezogener Vorfall bzw Sicherheits- oder betrieblicher Zahlungsvorfall zu erleichtern.

Kriterien	Bedingungen	Ergebnis
Negative Auswirkungen auf kritische Dienste bzw Services	Negative Auswirkung auf Dienste oder Services, die kritische oder wichtige Geschäftsfunktionen unterstützen **oder** Services, für die eine Konzession oder eine Registrierung notwendig ist **oder** Services, die von der Aufsicht überwacht werden.	**Nicht erfüllt:** Klassifikation als nicht schwerwiegend.
Erfolgreicher böswilliger unbefugter Zugriff mit potenziellem Datenverlust	Es wurde ein erfolgreicher böswilliger sowie unbefugter Zugriff auf Netzwerk- oder Informationssystem erkannt.	**Erfüllt:** Klassifikation als schwerwiegender Vorfall
Kunden, Finanzpartner und Transaktionen	> 100.000 Kunden nutzen den betroffenen Dienst **oder** > 10 % aller Kunden, die den betroffenen Dienst nutzen **oder** > 30 % der Finanzpartner **oder** > 10 % der Anzahl bzw Wert der täglichen Transaktionen **oder** jegliche festgestellten Auswirkungen auf Kunden oder Finanzpartner, die als relevant eingestuft werden.	**Erfüllt:** In Kombination mit einem weiteren Kriterium Klassifikation als schwerwiegender Vorfall.

Um dies zu gewährleisten, erfordert ein erfolgreicher TIBER-AT-Test die Zusammenarbeit einer Vielzahl von Akteuren mit spezifischen Rollen und Verantwortlichkeiten:[246]

Das **Control Team** (**CT**, zuvor: White Team, WT) ist das zentrale Steuerungsgremium innerhalb des Finanzunternehmens während eines TIBER-AT-Tests. Ihm obliegt auch die Koordination aller anderen Akteure. Es besteht aus ausgewählten Experten, typischerweise Vertreter der IT-Sicherheitsabteilung (ua CISO), optimalerweise ergänzt um ein Vorstandsmitglied (zB CIO, COO), um bei Bedarf eine rasche und vertrauensvolle Eskalation zu ermöglichen. Es wird von einem von der Geschäftsführung des Finanzunternehmens ernannten Control Team Lead (CTL) geleitet und ist verantwortlich für die Planung, Durchführung und Nachbereitung des Tests. Eine besonders wichtige Aufgabe des CT ist die Sicherstellung der strikten Geheimhaltung aller Testaktivitäten sowie das Risikomanagement während des Tests, um Kollateralschäden zu verhindern.

Das **Blue Team (BT)** besteht grundsätzlich aus allen Mitarbeitenden des Finanzunternehmens, die nicht Teil des CT sind. Im Rahmen eines TIBER-AT-Tests sind dies insbesondere die Mitarbeitenden, die für den Schutz der IT-Systeme und Daten verantwortlich sind (Security Operations Center, SOC). Allerdings können auch andere Mitarbeitende Ziel eines entsprechenden Angriffs werden (zB im Zuge von Spear-Phishing oder physischem Eindringen ins Gebäude) und somit Teil des BT sein. Im Gegensatz zum CT weiß das BT nicht, dass ein TIBER-AT-Test stattfindet. Dies gewährleistet, dass die Reaktion auf die Angriffe unter realitätsnahen Bedingungen stattfindet. Das BT spielt die zentrale Rolle in der Verteidigungsstrategie des Finanzunternehmens und wird nach Abschluss des Tests über die Ergebnisse informiert, um daraus entsprechende Lehren zu ziehen und Verbesserungen vorzunehmen.

Der **Threat Intelligence Provider (TIP)** ist ein externer Dienstleister, der die Bereitstellung zielgerichteter unternehmensspezifischer Bedrohungsinformationen verantwortet. Seine Arbeit ist bis zu einem gewissen Grad mit geheimdienstlicher Aufklärungsarbeit vergleichbar. Am Ende seiner Arbeit übergibt der TIP einen Bericht mit spezifischen Schwachstellen und Bedrohungen, die potenziell für einen Angriff auf das Finanzunternehmen genutzt werden können. Der TIP arbeitet eng mit den Red Team Tester (RTT, siehe unten) zusammen, um sicherzustellen, dass im Rahmen der Aufklärungsphase identifizierte Schwachstellen von den RTT verstanden und für die konkreten Angriffe genutzt werden können. Personell müssen TIP und RTT allerdings strikt getrennt sein, um die Diversität der Perspektiven und der untersuchten Szenarien sicherzustellen.

246 Die in manchen Fällen zusätzlich in Klammer angegebenen Bezeichnungen beziehen sich auf die vor Inkrafttreten des RTS on TLPT (siehe Abschnitt 6.3.) im TIBER-EU-Rahmenwerk (und damit auch im ersten TIBER-AT Implementation Guide) gebräuchlichen Bezeichnungen.

nition von IKT-Dienstleistungen soll digitale Dienste und Datendienste enthalten, die seitens eines Dritten über IKT-Systeme fortlaufend bereitgestellt werden. Dabei erwähnen die Unionsgesetzgeber explizit die sogenannten „Over-the-top"-Dienste, die in die Kategorie der elektronischen Kommunikationsdienste einzuordnen sind. Ausgenommen werden dabei lediglich die traditionellen analogen Telefondienste, die als Dienste des öffentlichen Fernsprechnetzes, Festnetz-Dienste, herkömmliche Fernsprechdienste oder Festnetztelefondienste gelten.[267]

Die Änderung bzw Ausweitung des Anwendungsbereichs auf jegliche Inanspruchnahme von Dienstleistern im IKT-Bereich durch DORA macht eine Prüfung und Überarbeitung der bisherigen Klassifizierung der IKT-Auslagerungen durch Finanzinstitute notwendig.

7.2.2.1. Kritikalitätseinstufung

Gem Art 28 Abs 3 hat das Finanzunternehmen bei jeder Inanspruchnahme eines IKT-Dienstleisters zu prüfen, ob die betreffende IKT-Dienstleistung kritische oder wichtige Funktionen unterstützt. Eine Funktion ist dann als kritisch oder wichtig zu klassifizieren, wenn

> der Ausfall derselben die finanzielle Leistungsfähigkeit eines Finanzunternehmens oder die Solidität oder Fortführung seiner Geschäftstätigkeiten und Dienstleistungen erheblich beeinträchtigen würde oder deren unterbrochene, fehlerhafte oder unterbliebene Leistung die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht erheblich beeinträchtigen würde.[268]

Neben dem Begriff der Kritikalität ist der Begriff „Unterstützung" idZ auslegungsbedürftig. Es stellt sich in der Praxis die Frage, ob bei der Klassifizierung jener IKT-Drittdienstleister, die kritische oder wichtige Funktionen unterstützen, eine Wesentlichkeitsschwelle zur Anwendung gelangt. Der Ansicht der ESA folgend ist demnach ein risikobasiertes Vorgehen indiziert. Bei der Einstufung, ob ein IKT-Drittdienstleister eine kritsiche oder wichtige Funktion *unterstützt* ist daher insb die Frage relevant, ob der Ausfall des Systems/Dienstleisters die betroffene(n) Funktion(en) materiell (va im Hinblick auf Kontinuität und Sicherheit) einschränken würde.[269]

Die Unterscheidung zwischen IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, und solche, auf die dieses Kriterium nicht zutrifft, ist deshalb entscheidend, da DORA zusätzliche Anforderungen an die Verwendung von IKT-Drittdienstleistern stellt, die kritische und wichtige Funktionen unterstützen, dabei ua:

267 ErwGr 35.
268 Art 3 Z 22.
269 ESA Q&A ID 2750 – DORA006.

agiert. Neben der internen Koordination und Gewährleistung der einheitlichen Anwendung der DORA-Vorgaben war die Implementierung der DORA selbst in den Jahren 2023 und 2024 eine der Kernaufgaben des DORA-Hubs. So wurde im Jahr 2024 durch die Etablierung eines Umsetzungsprojekts der Grundstein für die technische Adaptierung der bestehenden Systeme gelegt und mit einer eigens für die IKT-Aufsicht entwickelten Software mit dem Namen DORIS ein Werkzeug geschaffen, mit welcher im Sinne einer data-driven supervision insbesondere die Bearbeitung von IKT-bezogenen Vorfällen und die Auswertungen im Rahmen des Informationsregisters bewerkstelligt werden sollen.

Auch auf europäischer Ebene wurde eine sektorübergreifende Struktur zur Implementierung der DORA-Anforderungen etabliert. Hinsichtlich der Details zu dieser Struktur wird insbesondere auf Kapitel 7.3. verwiesen.

8.2. Vor-Ort-Prüfungen

Vor-Ort-Prüfungen (VOP), die in Österreich bei Kreditinstituten durch die OeNB vorgenommen werden, sind ein wichtiges Instrument der Bankenaufsicht. Die durch sie gewonnenen Erkenntnisse fließen nicht nur in die laufende Beaufsichtigung der Banken ein, sondern bilden auch eine der häufigsten Grundlagen für Maßnahmen der Aufsichtsbehörde. Die Kompetenz der OeNB erstreckt sich im Bereich von Vor-Ort-Prüfungen der Bankenaufsicht umfassend auf die **Prüfung aller Geschäftsfelder und aller Risikoarten**,[394] somit auch auf operationelle Risiken und IKT-Risiken. Im Verlauf einer Vor-Ort-Prüfung, die, wie der Name schon sagt, in den Räumlichkeiten des geprüften Instituts stattfindet, werden Risikomanagementsysteme und -prozesse im Detail untersucht sowie stichprobenartige Überprüfungen von einzelnen Geschäftsfällen oder Kontrollmaßnahmen vorgenommen.[395]

Der Vollständigkeit halber ist darauf hinzuweisen, dass zur Vor-Ort-Tätigkeit der OeNB neben den beschriebenen Vor-Ort-Prüfungen auch die Begutachtung von Risikomodellen der Kreditinstitute gehört. Da jedoch im Bereich des IKT-Risikos keine genehmigungspflichtigen Risikomodelle zur Risikomessung und Eigenmittelberechnung zum Einsatz kommen, werden Vor-Ort-Modelbegutachtungen in weiterer Folge nicht mehr explizit erwähnt.

8.2.1. Prüfinhalte und -schwerpunkte bei IKT-Risiko-Prüfungen

Jede Vor-Ort-Prüfung hat einen thematischen Fokus, innerhalb dessen die Prüfinhalte und -schwerpunkte festgelegt werden. In der Regel orientieren sich diese Schwerpunkte im Fall von IKT-Risiko-Prüfungen an den Unterkategorien dieser

394 § 70 Abs 1 Z 3 BWG.

395 Vgl „Vor-Ort-Prüfungen und Modellgutachten", OeNB-Homepage, https://www.oenb.at/finanzmarkt/bankenaufsicht/vor-ort-pruefungen--modellgutachten.html (abgerufen am 2.11.2024).

Der Aufbau der FMA ICT Security Toolbox begann 2019 mit den FMA Cyber und Cloud Maturity Level Assessments. 2022 folgte der erste Durchlauf des FMA Blackout Assessments.

2022 hat die FMA die bis dorthin verfolgte Methodik um eine realitätsnähere Komponente erweitert: Im Rahmen eines simulierten, für den Finanzsektor relevanten Cyberangriffs wurden die von den zu dieser Cyber Exercise eingeladenen Unternehmen unter Zeitdruck gesetzten Reaktionen evaluiert. Aus Ressourcengründen wäre es nicht möglich, diese Übung mit allen beaufsichtigten Unternehmen durchzuführen, weshalb 2023 ein Assessment zu Sicherheitsmaßnahmen, zu Controls, die zur Bewältigung einer Cyberattacke gesetzt werden, implementiert worden ist. Dabei wurde das für die Cyber Exercise entwickelte Angriffsszenario herangezogen.

2024 führt die FMA eine Analyse zur Austrian Digital Landscape durch. Diese enthält neben dem Fokus auf den Grad der Digitalisierung des Geschäftsbetriebs Evaluierungen zum Stand der Vorbereitungen der Unternehmen auf die ab 17.1.2025 anwendbaren DORA-Vorgaben.

In der ICT Security Toolbox sind auch weitere Elemente, die im Rahmen der davor durchgeführten Digitalisierungsstudien erhoben worden sind, umfasst, nämlich das Assessment zu Post-Covid-19-bezogenen IKT-Risiken, Evaluationen zu Vernetzungen von beaufsichtigten Unternehmen mit IKT-Drittdienstleistern sowie Analysen zu IKT-bezogenen Vorfällen.[485]

Die nächsten Abschnitte beschreiben diese Maßnahmen.

9.3.1. Cyber Maturity Level Assessment

Seit 2019 stellen die Cyber Maturity Level Assessments der FMA einen der Eckpfeiler der Beaufsichtigung im Thema IT-Security bei Versicherungen und Pensionskassen dar. Dabei handelt es sich um ein umfassendes, fragebogenbasiertes Self-Assessment, bei dem in letzter Iteration 57 Fragestellungen in folgenden 13 Themenbereichen betrachtet wurden:

- Cybersicherheitsstrategie
- Mitarbeiter
- Risikomanagement & Informationssicherheitsmanagement
- Testmethoden & Praktiken
- Incident Management
- Notfallmanagement
- IT-Assets
- Schwachstellenmanagement und Patch Management

485 FMA, Studie „Digitalisierung Finanzmarkt“, https://www.fma.gv.at/publikationen/studie-digitalisierung-finanzmarkt/ (29.5.2024).

- Die Abhilfemaßnahmen, die zur Behebung von Schwächen, Mängeln und Lücken im vereinfachten IKT-Risikomanagementrahmen ermittelt wurden, und der voraussichtliche Termin für die Durchführung dieser Maßnahmen, einschließlich der Folgemaßnahmen zu den in früheren Berichten festgestellten Schwächen, Mängeln und Lücken, sofern diese noch nicht behoben wurden.
- Zusammenfassende Erkenntnisse aus der Überprüfung des vereinfachten IKT-Risikomanagementrahmens sowie eine Übersicht über geplante Weiterentwicklungen.

10.2. IT-Risiko-Beaufsichtigung bei Verwaltungsgesellschaften

10.2.1. Einleitung und Geltungsbereich

Die Verwalter alternativer Investmentfonds und die Verwaltungsgesellschaften werden in Art 2 Abs 1 lit k und l der DORA-VO ausdrücklich angeführt, daher sind sämtliche einschlägigen Rechtsakte der DORA-VO auf diese Gesellschaften anwendbar. Eine Beschränkung im Umfang der von DORA-VO vorgesehenen Anforderungen an die Verwaltungsgesellschaften ist möglich, sofern die Kriterien für das Kleinstunternehmen gemäß Art 3 Abs 60 DORA-VO erfüllt sind.

Die betrieblichen Vorsorgekassen sind nicht ausdrücklich in Art 2 Abs 1 der DORA-VO, also dem Geltungsbereich, angeführt. Das liegt daran, dass sie ein österreichisches Spezifikum sind, das in dieser Form dem europäischen Aufsichtsregime nicht eindeutig zuzuordnen ist. Es handelt sich jedoch um Finanzunternehmen, daher wurden sie im Rahmen des österreichischen DORA-Vollzugsgesetzes in den Anwendungsbereich aufgenommen.

Bereits vor Inkrafttreten der DORA-VO waren im AIFMG und dem InvFG 2011 Regelungen zum Schutz von Informationen vorgesehen, beispielsweise über die allgemeinen organisatorischen Vorschriften, welche sich an die eingesetzten Systeme richten (§ 10 Abs 2 InvFG 2011 und Art 57 Abs 2 EU-AIFM-VO). Dementsprechend sind Systeme und Verfahren einzurichten, die die Sicherheit, die Integrität und die Vertraulichkeit von Informationen gewährleisten. Im Bereich der betrieblichen Vorsorgekasse finden sich entsprechende Vorgaben in §§ 3, 4 und 11 KI-RMV.

Auch im Bereich des Risikomanagements hatten Verwaltungsgesellschaften bereits bisher dafür Sorge zu tragen, dass angemessene und verhältnismäßige Strategien und Verfahren für das Risikomanagement festgelegt und umgesetzt werden (§ 13 Abs 2 AIFMG). Die entsprechende Risikomanagement-Funktion ist dauerhaft und unabhängig einzurichten (§ 17 Abs 1 InvFG 2011).

Hinsichtlich einer angemessenen Notfallplanung hatten die Unternehmen auch bisher einschlägige Vorschriften zu beachten, um sicherzustellen, dass die Konti-

13.1.3. Strafrechtliche Sanktionen

Art 52 DORA räumt Mitgliedstaaten die Möglichkeit ein, keine Vorschriften für verwaltungsrechtliche Sanktionen oder Abhilfemaßnahmen festzulegen, wenn Verstöße gegen DORA nach deren nationalen Recht strafrechtlichen Sanktionen unterliegen. Gemeint ist hier eine gerichtliche Strafbarkeit der jeweiligen nationalen Rechtsordnungen für Verstöße gegen die DORA. Der österreichische Gesetzgeber hat keine gerichtliche Strafbarkeit von Verstößen gegen die DORA vorgesehen und die verwaltungsrechtlichen Sanktionen und Abhilfemaßnahmen im DORA-VG geregelt. Für die DORA-Verstöße bedeutet dies, dass für sie das Verwaltungsstrafverfahren (VStG) zur Anwendung gelangt und eine Bestrafung nach DORA-VG keine gerichtliche Verurteilung, sondern eine Verwaltungsstrafe darstellt.

13.2. Adressaten der Verwaltungsstraftatbestände

13.2.1. Rechtsträger

Die Strafbestimmungen des § 7 DORA-VG und auch des § 8 DORA-VG adressieren Verantwortliche (§ 9 VStG) eines der nachstehenden Rechtsträger gemäß Art 2 Abs 1 lit a bis t DORA.

a) Kreditinstitute,
b) Zahlungsinstitute, einschließlich gemäß der Richtlinie (EU) 2015/2366 ausgenommene Zahlungsinstitute,
c) Kontoinformationsdienstleister,
d) E-Geld-Institute, einschließlich gemäß der Richtlinie 2009/110/EG ausgenommene E-Geld-Institute,
e) Wertpapierfirmen,
f) Anbieter von Krypto-Dienstleistungen, die gemäß einer Verordnung des Europäischen Parlaments und des Rates über Märkte von Krypto-Werten und zur Änderung der Verordnungen (EU) Nr 1093/2010 und (EU) Nr 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 (im Folgenden „Verordnung über Märkte von Krypto-Werten“) zugelassen sind, und Emittenten wertreferenzierter Token,
g) Zentralverwahrer,
h) zentrale Gegenparteien,
i) Handelsplätze,
j) Transaktionsregister,
k) Verwalter alternativer Investmentfonds,
l) Verwaltungsgesellschaften,
m) Datenbereitstellungsdienste,
n) Versicherungs- und Rückversicherungsunternehmen,
o) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit,

ringsten Umsetzungsaufwand und Komplexität. Der Test der digitalen Resilienz zieht einen höheren Aufwand bei der Umsetzung nach sich, während sich das IKT-Risikomanagement durch eine Erhöhung der Komplexität auszeichnet. Größte Herausforderung ist allerdings die Steuerung der IKT-Drittdienstleister, die durch die Verordnung auf eine neue Ebene gehoben wird.

Was dies für die Finanzinstitute bedeutet wird im Folgenden beleuchtet.

14.2.1.1. Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle

Ein wesentlicher Bestandteil von DORA ist die Erkennung, Behandlung und Meldung von IKT-bezogenen Vorfällen. Im Folgenden sollen die für die Umsetzung relevanten Anforderungen betrachtet werden. Es gilt standardisierte Prozesse für die Behandlung aber auch für die Dokumentation von IKT-Vorfällen zu etablieren, welche auch einen verpflichtenden Lernprozess beinhalten.

Zu beachten ist, dass DORA zwischen IKT-bezogenen Vorfällen und Cyberbedrohungen unterscheidet. Gem Art 3 Nr 8 DORA ist ein IKT-bezogener Vorfall ein von einem Finanzunternehmen nicht geplantes Ereignis bzw eine entsprechende Reihe verbundener Ereignisse, das bzw die die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigt und nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Finanzunternehmen erbrachten Dienstleistungen hat. Dies können bspw Systemausfälle, technische Störungen, Fehler in der Software oder Hardware oder menschliches Versagen sein. Cyberbedrohungen bezeichnen hingegen gem Art 2 Nr 8 der Verordnung (EU) 2019/881 einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnten. Zu diesen zählen bspw Phishing, Ransomware, unautorisierte Zugriffe oder das Ausnutzen von Datenlecks.

In Bezug auf die Behandlung von IKT-bezogenen Vorfällen auf dem Weg zur DORA-Compliance sind robuste Mechanismen zur Behandlung von IT-Sicherheitsvorfällen zu implementieren. Ein zentraler Bestandteil davon ist der Einsatz von SIEM-(Security Information and Event Management)-Systemen zur Überwachung schwerwiegender Vorfälle. Die Aggregation und Korrelation von Daten stellt einen wesentlichen Aspekt bei der Erkennung von Sicherheitsvorfällen dar. In diesen erfolgt eine Korrelation der Daten, um Muster und Anomalien zu erkennen, die auf Sicherheitsvorfälle hinweisen könnten.

Unter IT-Sicherheitsvorfallbehandlung werden dabei alle Maßnahmen und Prozesse subsumiert, die zur Erkennung, Analyse, Eindämmung, Behebung und Meldung von Sicherheitsvorfällen erforderlich sind. Das übergeordnete Ziel besteht in der Minimierung der Auswirkungen von IT-Sicherheitsvorfällen sowie der Gewährleistung der Wiederherstellung des normalen Geschäftsbetriebs.