DORA aus der Perspektive von bankgeschäftlichen Prüfungen

Die Bedeutung der Digitalisierung ist in der Finanzindustrie erheblich gestiegen. Allerdings sind Daten sowie Informations- und Kommunikationstechnologien (IKT) nicht nur Treiber des Fortschritts, sondern auch Quellen materieller Risiken. Die Verflechtungen und Abhängigkeiten innerhalb des Finanzsektors sowie zwischen Finanzunternehmen[1)] und IKT-Drittdienstleistern haben sich intensiviert, was die Anfälligkeit für systemweite Störungen erhöht. So sehen sich Finanzunternehmen, die essenzielle Dienstleistungen für die Volkswirtschaft bereitstellen, mit einer wachsenden Bedrohung durch Cyberangriffe und IKT-Störungen konfrontiert. Ein prägnantes Beispiel ist die globale Großstörung, die von einem Drittanbieter im Juli 2024 durch eine fehlerhafte Aktualisierung eines weit verbreiteten IKT-Produkts verursacht wurde.

Diese Risiken, die sich aus der tragenden Rolle, zunehmenden Abhängigkeit und mannigfaltigen Gefährdungen von digitalen Systemen ergeben, können nicht durch herkömmliche finanzielle Sicherheitsnetze[2)] abgefangen werden. In Deutschland haben insbesondere die BaFin-Rundschreiben der Mindestanforderungen an das Risikomanagement (MaRisk) seit 2005 sowie die Bankaufsichtlichen Anforderungen an die IT (BAIT) seit 2017 das im KWG geforderte angemessene Risikomanagement und somit die Erwartung der Aufsicht an die Banken konkretisiert, bevor die European Banking Authority (EBA) in 2019 ihrerseits Leitlinien für das Management von IKT- und Sicherheitsrisiken veröffentlichte. In der Praxis gibt es neben erkennbaren Fortschritten weiterhin regelmäßig Schwachstellen und, aufgrund der dynamischen Entwicklung der Bedrohungslandschaft, kontinuierlichen Verbesserungsbedarf beim Betrieb, der Weiterentwicklung und der Sicherheit von IKT-Systemen sowie im IKT-Risikomanagement. Dies zeigen die aufsichtlichen Prüfungen der Bundesbank bei Banken sowie deren IKT-Drittdienstleistern.

Die Einführung des Digital Operational Resilience Act (DORA) markiert einen wesentlichen Wendepunkt im Umgang mit IKT-Risiken und IKT-Drittdienstleistungen. Die DORA-Anforderungen zur digitalen operationalen Widerstandsfähigkeit nebst den weiteren in der Verordnung getroffenen Regelungen sind wesentlich und notwendig, um die Stabilität des Finanzsektors regulatorisch angemessen zu flankieren. Durch eine EU-weite und den gesamten Finanzsektor umfassende Harmonisierung der Anforderungen an die digitale operationale Resilienz durch den europäischen

---

1 Gemäß Artikel 2 (2) DORA werden die in Artikel 2 (1) DORA, Buchstaben a bis t genannten Unternehmen zusammen als „Finanzunternehmen" bezeichnet, hierzu zählen unter anderem Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister, E-Geld-Institute, Wertpapierfirmen, Anbieter von Krypto-Dienstleistungen und Emittenten wertreferenzierter Token.

2 Wie beispielsweise private oder öffentliche Einlagensicherungssysteme.

Gesetzgeber werden bestehende nationale und sektorspezifische Vorgaben wie unter anderem die BAIT ersetzt, was zu einer effizienteren und kohärenteren Risikomanagementlandschaft des Finanzsektors der EU führen soll.

DORA soll die Widerstandsfähigkeit des Finanzsektors stärken und ein einheitliches Schutzniveau etablieren. Finanzunternehmen müssen durch technisch-organisatorische Maßnahmen sicherstellen, dass sie auch bei Eintritt eines schwerwiegenden IKT-Vorfalls arbeitsfähig bleiben und den Normalbetrieb wiederaufnehmen können. Somit werden sich DORA-Sonderprüfungen der Bundesbank bei Banken sowie deren IKT-Drittdienstleistern zukünftig insbesondere auf die Governance und Organisation, den IKT-Risikomanagementrahmen einschließlich des IKT-Drittparteienrisikos sowie der hierfür erforderliche IKT-Systeme, -Protokolle und -Tools erstrecken. Aber auch die Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle sowie das Testen der digitalen operationalen Resilienz in den Finanzunternehmen rücken stärker in den aufsichtlichen Fokus. Die Bundesbank kann bei der laufenden Überwachung der Implementierung der DORA-Anforderungen in Finanzinstituten auf langjährige Erfahrungen aufbauen und wird ihre Expertise sowie Erkenntnisse aus aufsichtlichen Prüfungen gezielt einbringen. Finanzinstitute sind aufgefordert, einen robusten IKT-Risikomanagementrahmen zu implementieren, der alle Aspekte der digitalen operationalen Resilienz und die IKT-Drittdienstleister umfasst.

1 IKT-Risiken im Fokus der Finanzaufsicht

IKT-Risiken stellen zunehmend eine Herausforderung für Finanzinstitute dar. Finanzinstitute und andere Finanzmarktteilnehmer nutzen in hohem Maße Informations- und Kommunikationstechnologien, um Dienstleistungen zu erbringen, die für die Volkswirtschaft zentral sind. Hierfür binden sie verstärkt IKT-Dienstleistungen Dritter in das Geschäftsmodell sowie in interne Prozesse ein. Durch die zunehmende Digitalisierung wächst auch das IKT-Risiko, was das Finanzsystem anfälliger für Cyberangriffe oder IKT-Störungen macht. Bei finanziellen Schieflagen können beispielsweise finanzielle Puffer oder sektorspezifische Mechanismen die Liquidität oder Solvenz eines Finanzinstituts stabilisieren, um damit die systemische Ansteckung anderer Finanzmarktakteure zu verhindern. Bei einer IKT bedingten Schieflage ist dies anders. IKT-Störungen lassen sich nicht allein durch finanzielle Puffer überwinden, sondern das betroffene Institut muss entsprechenden Schäden durch technisch-organisatorische Maßnahmen vorbeugen, sodass es auch bei Eintritt eines schwerwiegenden Ereignisses arbeitsfähig bleibt und den Normalbetrieb wiederaufnehmen kann. So lassen sich zum Beispiel durch eine Ransomware-Attacke verschlüsselte Kundendaten durch finanzielle Puffer nicht entschlüsseln. Vielmehr dürfen solche Angriffe keine Ansteckungseffekte auf Backups entfalten, was deren hinreichend wirksame physische oder logische Segmentierung erfordert. Hier müssen die Finanzinstitute besondere Fähigkeiten aufbauen und Prozesse, wie beispielsweise Notfallkonzepte und Wiederanlaufpläne, implementieren. Diese wurden auch jüngst im Cyber-Stresstest der EZB vor dem Hintergrund eines schwerwiegenden, aber plausiblen Szenario eines Cyber-Sicherheitsvorfalls überprüft, dem sich 109 Banken im gesamten Single Shared Market (SSM) unterzogen haben.[3)]

IKT-Risiken resultieren zunehmend auch aus schwerwiegenden Cyberbedrohungen mit hohem Schadensrisiko. Die Anzahl der im SSM von signifikanten Instituten an die Aufsicht gemeldeten IKT-Vorfälle ebenso wie die Meldungen schwerwiegender Zahlungssicherheitsvorfälle in Deutschland (PSD2-Meldungen) bleiben trotz zunehmender Bedrohungen in den vergangenen Jahren etwa konstant. Allerdings waren die Risiken im Bereich der Informations- und Kommunikationstechnologie vor zwei Jahrzehnten hauptsächlich auf Störungen beschränkt, die zwar die Arbeits- und

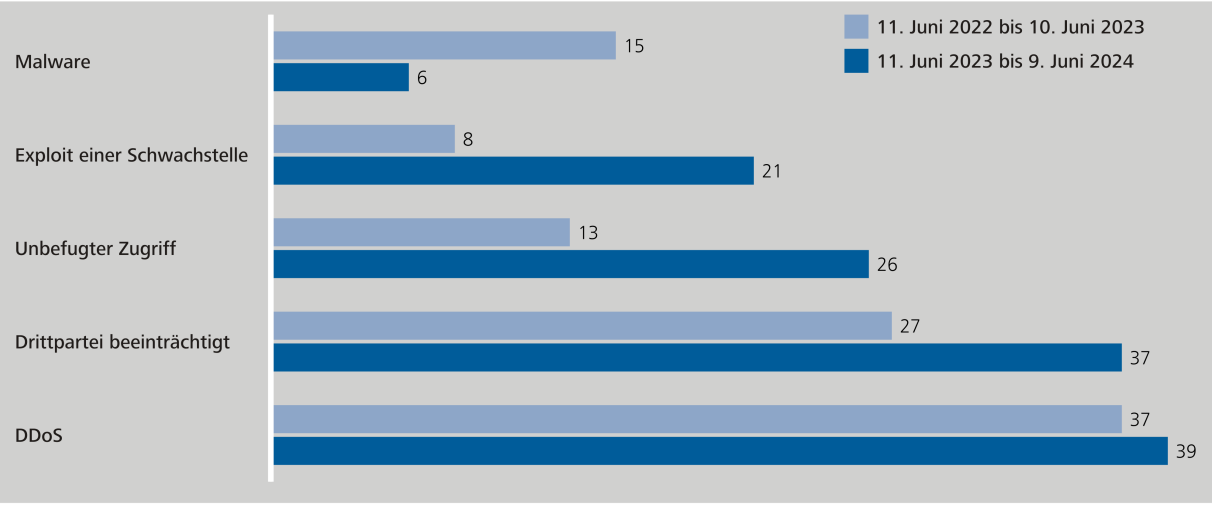
3 Siehe: bankingsupervision.europa.eu sowie bankingsupervision.europa.eu, letzter Abruf: 23. August 2024.

Kundenzufriedenheit beeinflusst haben, aber von geringem Schadensausmaß waren. Ursächlich für PSD2-Meldungen sind noch immer überwiegend Fehler beim Betrieb sowie der Aktualisierung von IKT-Systemen. Doch haben sich die Bedrohungsszenarien signifikant gewandelt: Organisierte Kriminalitätsgruppen und zunehmende geopolitische Spannungen haben Cyberangriffe zu einer ernstzunehmenden Gefahr werden lassen, die ein beträchtlich höheres Schadenspotenzial mit sich bringt. Bei einem Kontowechseldienstanbieter wurden in 2023 etwa Kontodaten von Kunden diverser Banken bei einem Hackerangriff erbeutet.[4] In jüngster Zeit haben sich die IKT-Vorfälle aufgrund des Ausnutzens von Schwachstellen gehäuft: Hierbei gelingt es den Angreifern, schadhaften Programmcode in die Zielinfrastrukturen einzuschleusen. Auch die wesentlich erhöhte Zahl an unberechtigten Zugriffen spricht für Verbesserungspotenziale im Security Information und Event Management System (SIEM)[5], um nicht autorisierte Datenzugriffe oder Berechtigungsänderungen effektiv zu unterbinden.

Ausgewählte IT-Vorfallsarten bei signifikanten Instituten im SSM

Schaubild 4.1

Anzahl



Quelle: EZB.

Deutsche Bundesbank

4 Siehe: handelsblatt.com, letzter Abruf: 26. August 2024.

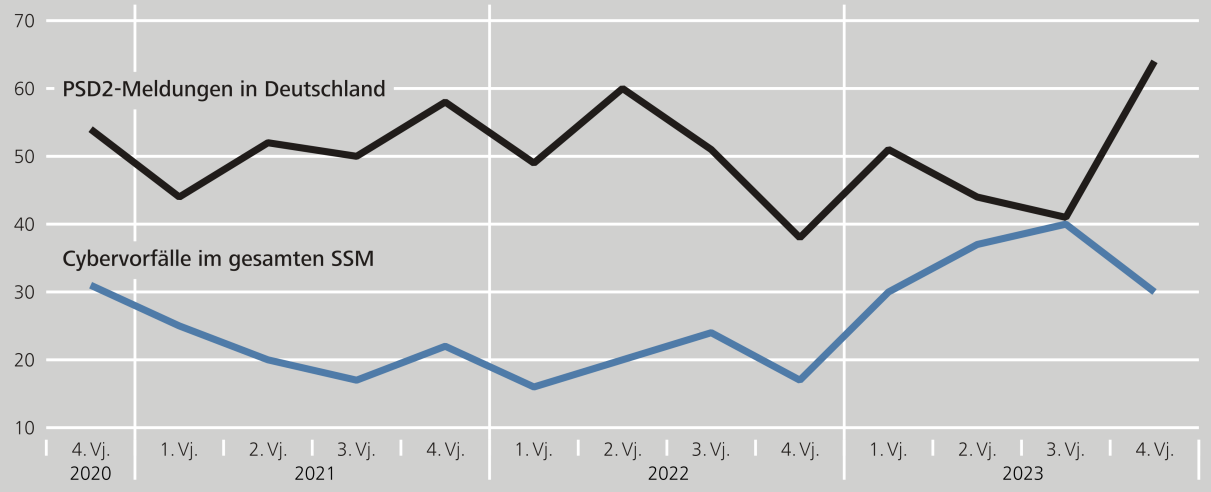
5 Hierbei handelt es sich um ein System, dass Sicherheitsinformationen sowie Ereignisse (wie etwa Zugriffe) in einer IKT-Infrastruktur sammelt, analysiert und überwacht. Siehe: csrc.nist.gov, letzter Abruf: 26. August 2024.

6)

PSD2-Meldungen und Cybervorfälle

Schaubild 4.2

Anzahl



Quelle: EZB.

Deutsche Bundesbank

Digitalisierung und Vernetzung bergen auch Risiken für die Finanzstabilität. Mit der Digitalisierung des Finanzsektors gehen auch stärkere Verflechtungen innerhalb dieses Sektors sowie grundlegende Abhängigkeiten von IKT-Drittdienstleistern einher. Cyberangriffe oder Störungen bei IKT-Drittdienstleistern oder der flächendeckende Einsatz von bestimmten IKT-Produkten oder IKT-Services stellen aufgrund ihrer Auswirkungen für den gesamten Finanzsektor eine zunehmende Gefahr für die Finanzstabilität dar. Ein aktuelles Beispiel hierfür ist die weltweite Großstörung, welche im Juli 2024 durch ein Update eines Produktes der Firma CrowdStrike ausgelöst wurde. Diese betraf weltweit über acht Millionen Geräte und beeinträchtigte teilweise wichtige und kritische Funktionen von hunderten Unternehmen, darunter auch Finanzinstitute. [7)] Die weltweiten Auswirkungen zeigen deutlich, wie vernetzt die gesamte Finanzindustrie ist und wie groß die Abhängigkeiten von IKT-Drittdienstleistern sind. Dabei können die tatsächlichen Risiken noch größer sein als auf den ersten Blick angenommen, da IKT-Drittdienstleister ihrerseits durch Weiterverlagerungen auf dieselben kritischen IKT-

6 Fußnote zu Schaubild 4.1: Bei einer sogenannten "verteilten DoS-Attacke" (Distributed Denial of Service, kurz DDoS) kommt anstelle eines einzelnen Angriffssystems eine Vielzahl von unterschiedlichen IKT-Systemen in einer großflächig koordinierten Angriff zum Einsatz. Durch massenhafte Anfragen, beispielsweise an eine Website oder einen Server, wird versucht, die Zielressource zu überlasten. Aufgrund der hohen Anzahl der gleichzeitig angreifenden Rechner sind die Angriffe besonders wirksam. bsi.bund.de, letzter Abruf: 26. August 2024.

7 Vgl. beispielsweise: Tremmel (2024).

Drittdienstleister Konzentrationsrisiken erhöhen oder weil die Lieferketten der bezogenen IKT-Services nicht hinreichend überwacht werden.

2 DORA-Implikationen für die Finanzaufsicht

2.1 Ein Blick zurück – die nationale sektorspezifische Überwachung von IKT-Risiken

Der klassische Ansatz zum Umgang mit operationellen Risiken zielt insbesondere darauf ab, ausreichend Eigenkapital für den Schadensfall vorzuhalten. Daneben müssen qualitative Anforderungen an ein angemessenes Risikomanagement sicherstellen, dass sowohl die Eintrittswahrscheinlichkeit als auch die Schadenshöhe von IKT-Vorfällen so weit begrenzt werden, dass die Risikotragfähigkeit laufend gegeben ist. In Deutschland haben die BaFin-Rundenschreiben MaRisk seit 2005 sowie BAIT seit 2017 das im KWG geforderte angemessene Risikomanagement und somit die Erwartung der Aufsicht an die Banken hinsichtlich einer angemessenen technisch-organisatorischen Ausstattung und des Notfallmanagements für IKT-Systeme konkretisiert. Dies galt, bevor die EBA in 2019 ihrerseits Leitlinien für das Management von IKT- und Sicherheitsrisiken veröffentlichte. Diese Leitlinien wurden in den Novellen der MaRisk sowie der BAIT von der BaFin in enger Zusammenarbeit mit der Bundesbank umgesetzt. Eben dies erfolgte in 2021 im Rundschreiben Zahlungsdienstliche Anforderungen an die IT (ZAIT).[8)]

Die Prüfungen der Bundesbank zeigen trotz signifikanter Fortschritte bei den Instituten aufgrund der dynamischen Bedrohungslage anhaltenden Handlungsbedarf im IKT-Risikomanagement auf. Seit mehr als einem Jahrzehnt wird die Bundesbank regelmäßig unter anderem mit aufsichtlichen Vor-Ort-Sonderprüfungen beauftragt, die sich auf die Ordnungsmäßigkeit der Geschäftsorganisation gemäß der §§ 25a,b KWG in Verbindung mit MaRisk-BAIT beziehungsweise § 27 ZAG in Verbindung mit ZAIT bei Finanzinstituten und deren IKT-Drittdienstleistern erstrecken. Im Laufe dieser Zeit hat sich der Reifegrad es IKT-Risikomanagements einschließlich des Managements von Auslagerungsrisiken in den geprüften Unternehmen mehrheitlich deutlich erhöht. Angesichts zunehmender Bedrohungen sind jedoch auch die Anforderungen an das Management von IKT-Risiken gestiegen. Trotz der Fortschritte ermitteln Prüfungen nach wie vor wesentliche

8 Vgl. beispielsweise: bundesbank.de, letzter Abruf: 16. August 2024.

Schwachstellen, kritische Problembereiche und einen kontinuierlichen Verbesserungsbedarf im Hinblick auf den Umgang mit IKT-Risiken. So wurden auch im Jahr 2023 Prüfungsfeststellungen in elementaren Bereichen des IKT-Risikomanagements getroffen, wobei über die Hälfte dieser Feststellungen gewichtig oder schwerwiegend waren.

2.2 Der Blick nach vorn – DORA als sektorübergreifende EU-Verordnung

Ein wesentliches Ziel von DORA ist es, die digitale operationale Widerstandsfähigkeit des gesamten Finanzsektors der EU zu stärken. Die Finanzunternehmen sollen insbesondere gegenüber Cyberangriffen oder IKT-Störungen bei Finanzmarktteilnehmern und IKT-Drittdienstleistern robuste Mechanismen etablieren, die ein einheitlich hohes Schutzniveau sicherstellen. DORA verpflichtet die drei Europäischen Aufsichtsbehörden (ESAs)[9] zudem, Entwürfe für gemeinsame technische Regulierungs- sowie Durchführungsstandards für DORA auszuarbeiten und diese an die Europäische Kommission zu übermitteln. Gleichzeitig erhält die Europäische Kommission die Befugnis, DORA um diese Standards zu ergänzen oder diese Standards zu erlassen.

Aufgrund der Harmonisierung der wichtigsten Anforderungen an die digitale operationale Resilienz durch den europäischen Gesetzgeber werden die nationalen sektoralen Anforderungen an die IT-Sicherheit im Finanzsektor in Deutschland aufgehoben. Dies betrifft sowohl die BAIT als auch die ZAIT.[10] Obwohl die Kompetenz zur Regulierung aller Elemente der digitalen operationalen Resilienz beim europäischen Gesetzgeber liegt, wirkt die deutsche Finanzaufsicht in den gemeinsamen Gremien der ESAs bei der Ausgestaltung von technischen Regulierungs- und Durchführungsstandards sowie in den Q&A Prozessen zu DORA mit.

DORA verstärkt die Anforderungen an die operative Resilienz, um die Stabilität bedeutender Finanzfunktionen zu gewährleisten. DORA verlangt von Finanzinstituten ein resilientes IKT-Risikomanagement. Es gibt im deutschen Finanzsektor bereits hohe aufsichtliche Erwartungen an die IT-Sicherheit gemäß MaRisk, BAIT und ZAIT. Indes führt DORA mit dem Fokus auf die digitale operationale Resilienz erweiterte Vorgaben und neue Schwerpunkte hinsichtlich der digitalen operationalen Widerstandsfähigkeit

9 European Banking Authority (EBA), European Securities and Markets Authority (ESMA), European Insurance and Occupational Pensions Authority (EIOPA).

10 Vgl.: „Machen Sie sich jetzt startklar für DORA“, bafin.de, letzter Abruf: 16. August 2024.

ein.[11)] Diese zielen darauf ab, nicht allein die potenziellen Schäden infolge von IKT-Störungen zu vermeiden oder auf ein tolerierbares Maß zu reduzieren, sondern insbesondere sicherzustellen, dass kritische und wichtige Funktionen des Finanzunternehmens auch in Krisensituationen fortgeführt oder zeitnah reaktiviert werden können. Damit sollen die Integrität und das ordnungsgemäße Funktionieren des Finanzmarktes unter allen Umständen gewährleistet werden.

2.3 Lernfelder für zukünftige DORA-Prüfungen

2.3.1 Governance und Organisation

Finanzinstitute sind dazu angehalten, eine wirksame Governance-Struktur und Organisationsform für das Management von IKT-Risiken zu implementieren. Der dafür erforderliche IKT-Risikomanagementrahmen muss zentrale Elemente der digitalen operationalen Resilienz abdecken, darunter Identifizierung, Schutz und Prävention, Erkennung, Reaktion, Wiederherstellung sowie Backup und Restoration. Diese Elemente sollten durch zuverlässige, widerstandsfähige IKT-Systeme sowie durch durchdachte Protokolle und Werkzeuge gestärkt werden. In Anbetracht der sich kontinuierlich wandelnden Cyberbedrohungen ist eine stetige Weiterbildung aller Mitarbeiterinnen und Mitarbeiter sowie eine permanente Weiterentwicklung des Risikomanagementansatzes notwendig. Im Fall eines Cyberangriffs oder IKT-Vorfalls ist eine klare und umfassende Kommunikation mit allen relevanten Interessengruppen, einschließlich Aufsichtsbehörden, Kunden und der breiten Öffentlichkeit, unabdingbar. Ergänzende technische Regulierungsstandards spezifizieren die Vorgaben für bestimmte Bereiche des IKT-Risikomanagements weiter.[12)]

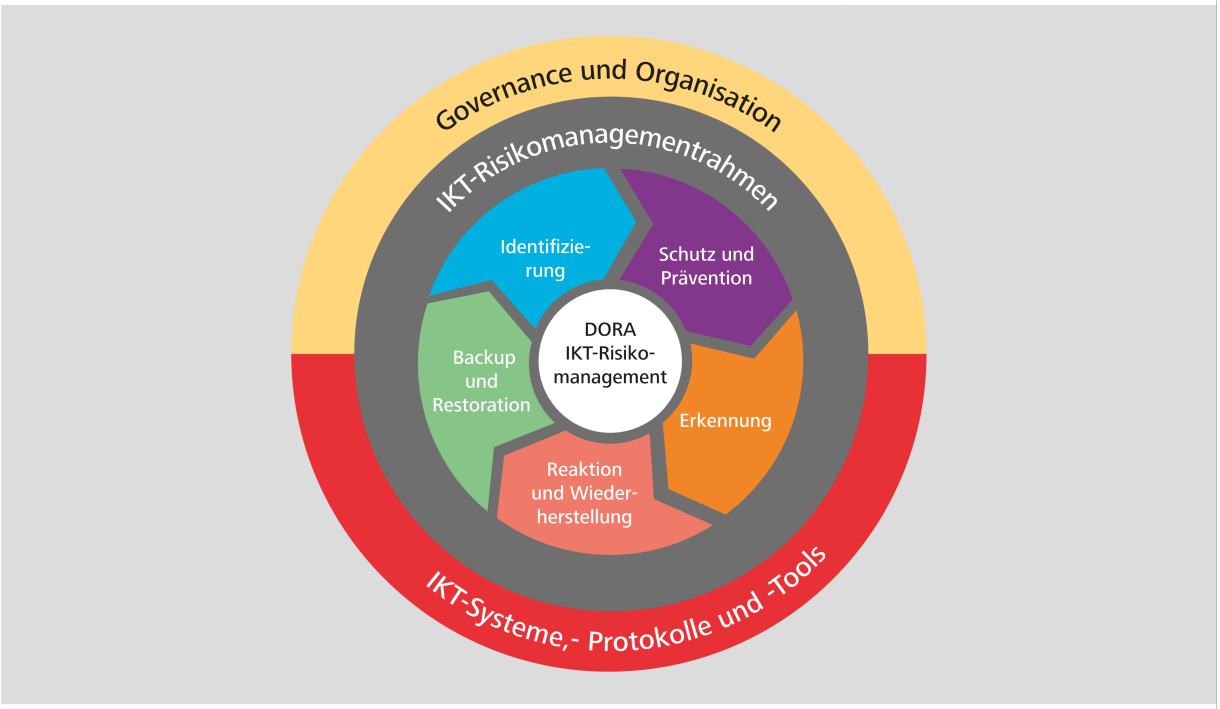
---

11 Vgl. Ergebnisse der Arbeitsgruppen der Industrie, der Deutschen Bundesbank und der BaFin in: Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, bafin.de, letzter Abruf 16. August 2024.

12 CDR (EU) 2024/1774 on *RTS specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework* (OJ L, 25. Juni 2024) sowie CDR (EU) 2024/1773 on *RTS specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical o important functions provided by ICT third-party service providers* (OJ L, 25. Juni 2024).

Governance und Organisation

Schaubild 4.3



Deutsche Bundesbank

IKT-Kompetenz im Leitungsorgan wird unerlässlich. Das Leitungsorgan, welches für Kredit- und Zahlungsinstitute sowohl die Geschäftsleitung als auch den Aufsichtsrat umfasst, trägt die uneingeschränkte und letztliche Verantwortung für das angemessene Management des IKT-Risikos. Dies umfasst unter anderem die Definition der strategischen Ziele zur digitalen operationalen Resilienz des Instituts. Das Leitungsorgan hat hierzu selbst über ausreichende Kenntnisse und Fähigkeiten zu verfügen und muss diese regelmäßig auf dem aktuellen Stand halten, um die IKT-Risiken und deren Auswirkungen auf das Finanzinstitut ausreichend verstehen und bewerten zu können. Hierzu sind regelmäßig speziell auf den Bedarf zugeschnittene Schulungen zu absolvieren.

2.3.2 IKT-Risikomanagementrahmen

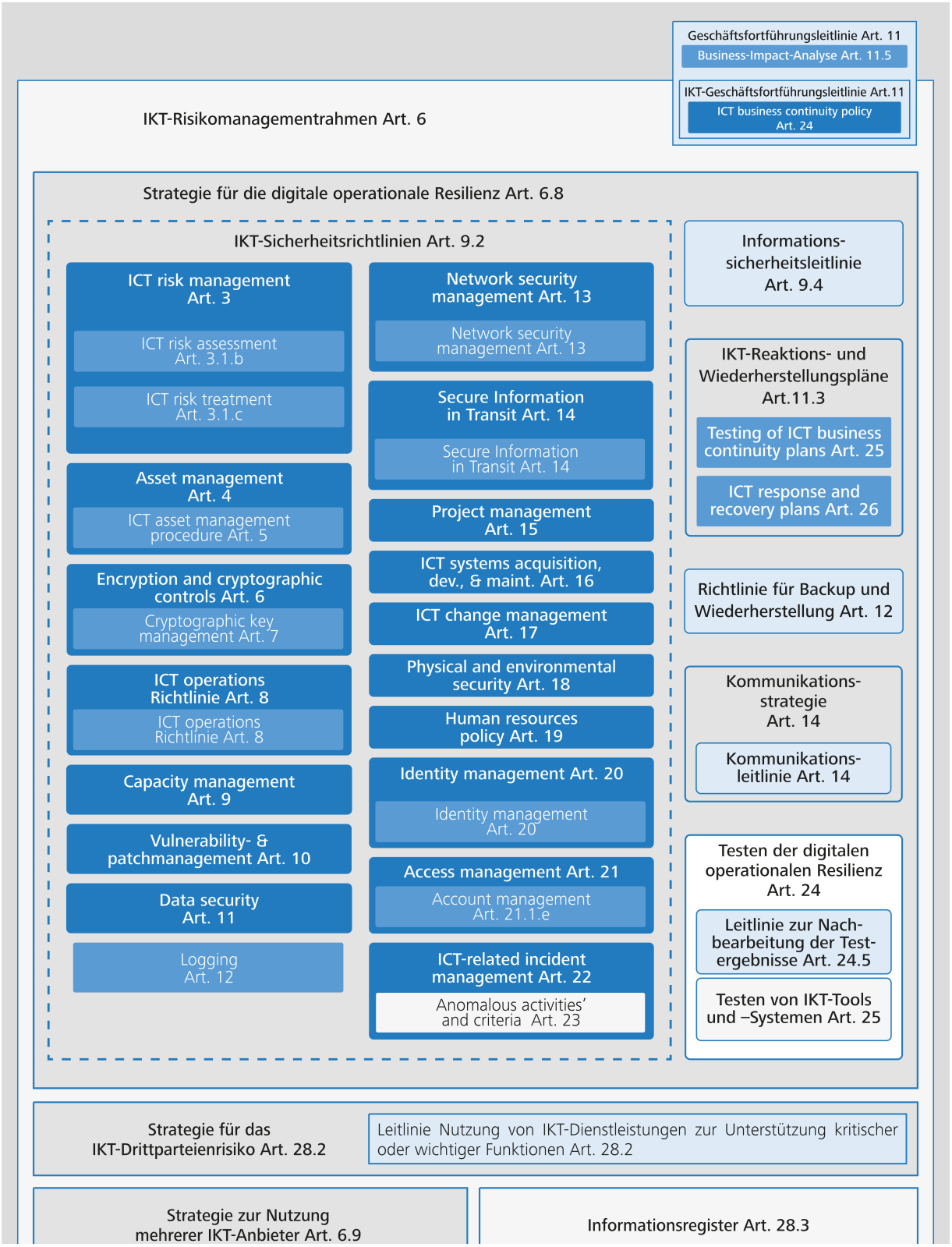
Governance- und Kontrollrahmen sind grundlegend für das ordnungsgemäße Management der IKT-Risiken. Nur ein umfassender, schriftlich fixierter IKT-Risikomanagementrahmen kann die strategischen Vorgaben des Leitungsorgans verlässlich transportieren und ein hohes Niveau digitaler operationaler Resilienz nach

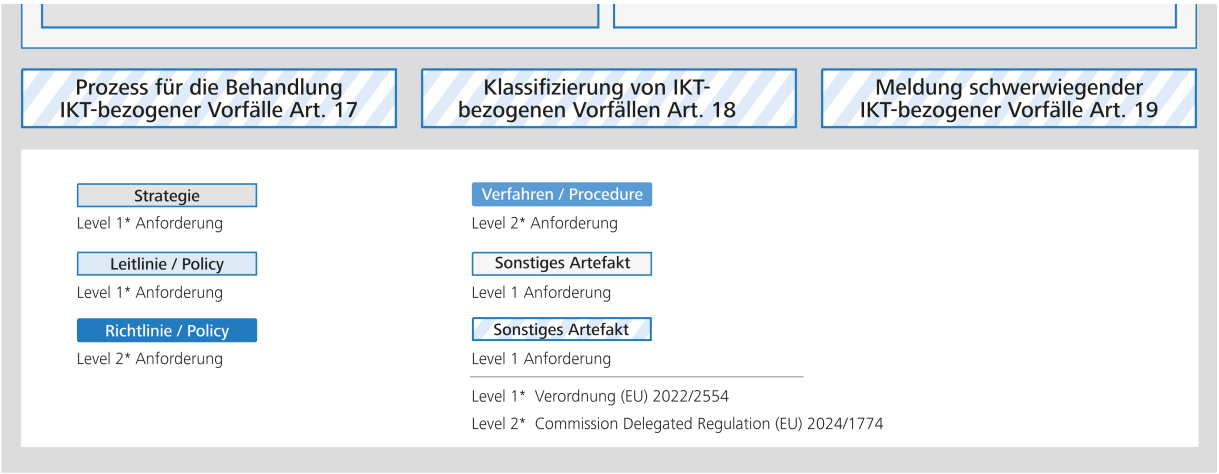
dem Stand der Technik gewährleisten. Dieser Rahmen muss detaillierte Strategien, Leitlinien, Richtlinien, Verfahren und Kontrollmechanismen umfassen, die speziell auf die Identifikation, Bewertung, Steuerung und Überwachung von spezifischen IKT-Risiken des Instituts abzielen. Um mit der sich laufend ändernden Bedrohungslandschaft Schritt zu halten, ist es unerlässlich, den Rahmen regelmäßig, mindestens jährlich zu überprüfen und zu aktualisieren. In den Finanzunternehmen sind zudem anlassbezogene Überprüfungen bei schwerwiegenden IKT-bezogenen Vorfällen oder aufgrund aufsichtsrechtlicher Anweisungen oder Feststellungen erforderlich. Nur so können die Sicherheitsstrategien des Unternehmens kontinuierlich optimiert und die digitale operationale Widerstandsfähigkeit weiter gestärkt werden.

Auf den IKT-Risikomanagementrahmen sollten die Finanzunternehmen besonderes Augenmerk legen. Nicht zuletzt haben aufsichtliche Prüfungen der MaRisk, BAIT und ZAIT der letzten Jahre diesbezüglich wiederholt Schwächen aufgedeckt, insbesondere hinsichtlich der Vollständigkeit, des Detaillierungsgrades und der Aktualität der schriftlich fixierten Ordnung. DORA-Finanzunternehmen sind künftig verpflichtet, den zuständigen Behörden auf Anfrage vollständige und aktuelle Informationen über ihre IKT-Risiken und ihren IKT-Risikomanagementrahmen vorzulegen.

IKT-Risikomanagement*

Schaubild 4.4





*Vereinfachte Darstellung der Mindestinhalte

Deutsche Bundesbank

2.3.3 IKT-Kontrollfunktion

Eine interne, unabhängige IKT-Kontrollfunktion ist entscheidend für die effektive Überwachung von IKT-Risiken und die Stärkung der digitalen operationalen Resilienz. Mit der Einführung von DORA ändern sich die regulatorischen Anforderungen. Die bisherigen Vorschriften in Deutschland, die gemäß BAIT grundsätzlich einen internen Informationssicherheitsbeauftragten (ISB) vorsahen, werden durch eine breiter gefasste IKT-Kontrollfunktion ersetzt, die für das Management und die Überwachung des IKT-Risikos zuständig ist. Die Implementierung einer unabhängigen IKT-Kontrollfunktion ist für eine effektive Überwachung von IKT-Risiken und zur Unterstützung des Leitungsorgans unerlässlich.

Zur Überwachung der institutseigenen IKT-Landschaft ist es unerlässlich, dass die zuständige Kontrollfunktion die implementierten Prozesse und Produkte sehr gut kennt. Daher ist es in der Regel. angebracht, diese IKT-Kontrollfunktion nicht auszulagern, sondern sie innerhalb des Instituts zu belassen, um Synergien zu maximieren und eine schnelle Reaktionsfähigkeit bei IKT-Vorfällen zu gewährleisten. Die interne Verankerung dieser Funktion fördert eine effektive Kontrolle über IKT-Risiken und trägt maßgeblich zur Stärkung der operationalen digitalen Resilienz des Finanzinstituts bei.

Die IKT-Kontrollfunktion soll im Einklang mit dem Modell der drei Verteidigungslinien[13] oder einem internen Modell für Risikomanagement und Kontrolle implementiert werden und ist speziell für die unabhängige Überwachung des IKT-Risikos verantwortlich. Indes hatte die deutsche Finanzaufsicht diese Anforderungen schon in den einschlägigen nationalen Rundschreiben verankert. Dennoch haben aufsichtliche Prüfungsergebnisse wiederholt Schwächen aufgezeigt, insbesondere hinsichtlich der erforderlichen Unabhängigkeit dieser Kontrollfunktion, der Angemessenheit der Berichtswege zum Leitungsorgan und der Verfügbarkeit der notwendigen Ressourcen für die effektive Aufgabenerfüllung.

2.3.4 IKT-Drittparteienrisikomanagement

Finanzunternehmen müssen die vollständige Kontrolle über ihr IKT-Risiko behalten. Das schließt die Kontrolle über solche Risiken mit ein, welche durch die Nutzung von IKT-Drittdienstleistungen entstehen, die von IKT-Drittdienstleistern oder deren Unterauftragnehmern bereitgestellt werden (IKT-Drittparteienrisiko). Das gilt auch in Bezug auf kritische IKT-Drittdienstleister, die dem europäischen Überwachungsrahmen unterliegen (siehe Exkurs EU-Überwachungsrahmenwerk). Die Einstufung als kritischer IKT-Drittdienstleister stützt sich auf die Informationsregister der Finanzunternehmen, die alle vertraglichen Vereinbarungen zu bereitgestellten IKT-Drittdienstleistungen enthalten. Im Fokus von DORA steht ein breites Spektrum von IKT-Drittdiensteistern, unter anderem Anbieter von Cloud-Computing, Software, Datenanalysen sowie Dienstleistungen aus Rechenzentren, aber auch Zahlungsdienste mit Zahlungsabwicklungstätigkeiten und den Betrieb von Zahlungsinfrastrukturen. Während sich durch den Bezug von IKT-Drittdienstleistungen von spezialisierten Anbietern manche Risiken anders oder besser steuern lassen, entstehen durch die zunehmenden Verflechtungen mit Abhängigkeiten von anderen Unternehmen zusätzliche Risiken für das Institut aber auch für den Finanzmarkt.

Die Abhängigkeiten der Finanzunternehmen von einzelnen IKT-Drittdienstleistern können zunehmen und gegebenenfalls auch in systemischen Abhängigkeiten des Finanzsektors resultieren. Das Angebot von IKT-Drittdienstleistungen entwickelt sich dynamisch in Breite und Tiefe weiter, und diese werden immer stärker in die Wertschöpfungskette von Finanzunternehmen integriert. Die Dynamik am Markt sorgt

13 Vgl.: European Banking Authority, Final Report on Guidelines on Internal Governance under Directive 2013/36/EU. Letzter Abruf: 26. August 2024. Die Geschäftsbereiche gehen im Rahmen der ersten Verteidigungslinie Risiken ein und sind für ihr operatives Management direkt und dauerhaft verantwortlich. Die zweite Verteidigungslinie bilden die Risikomanagementfunktion und die Compliance-Funktion. Die unabhängige interne Revision als dritte Verteidigungslinie führt risikobasierte und allgemeine Prüfungen durch und überprüft die internen Governance-Regelungen, -Prozesse und -Mechanismen, um sicherzustellen, dass sie solide und wirksam sind, umgesetzt und einheitlich angewendet werden.

zudem dafür, dass einige IKT-Drittdienstleister eine sehr große Marktmacht erlangen können, was es für die regulierten Finanzinstitute erschwert, bereits während der Vertragsverhandlungen beispielsweise die aufsichtlich geforderten Informations- und Prüfungsrechte in ausreichendem Maße zu implementieren und die Überwachung der IKT-Risiken angemessen wahrzunehmen zu können.

Um den regulatorischen Anforderungen in Bezug auf das IKT-Drittparteienrisikomanagement zu entsprechen, stehen die Finanzunternehmen vor enormen Herausforderungen. Denn in DORA werden insbesondere die Anforderungen an das Management des IKT-Drittparteienrisikos umfangreicher und detaillierter. Aber bereits in den Prüfungen gemäß nationalen sektorspezifischen Regelungen wurde häufig festgestellt, dass hinsichtlich der bestehenden aufsichtlichen Anforderungen unvollständige Verträge mit IKT-Drittdienstleistern abgeschlossen und die Risiken aus dem Drittbezug von den Finanzunternehmen unzureichend bewertet und gesteuert werden.

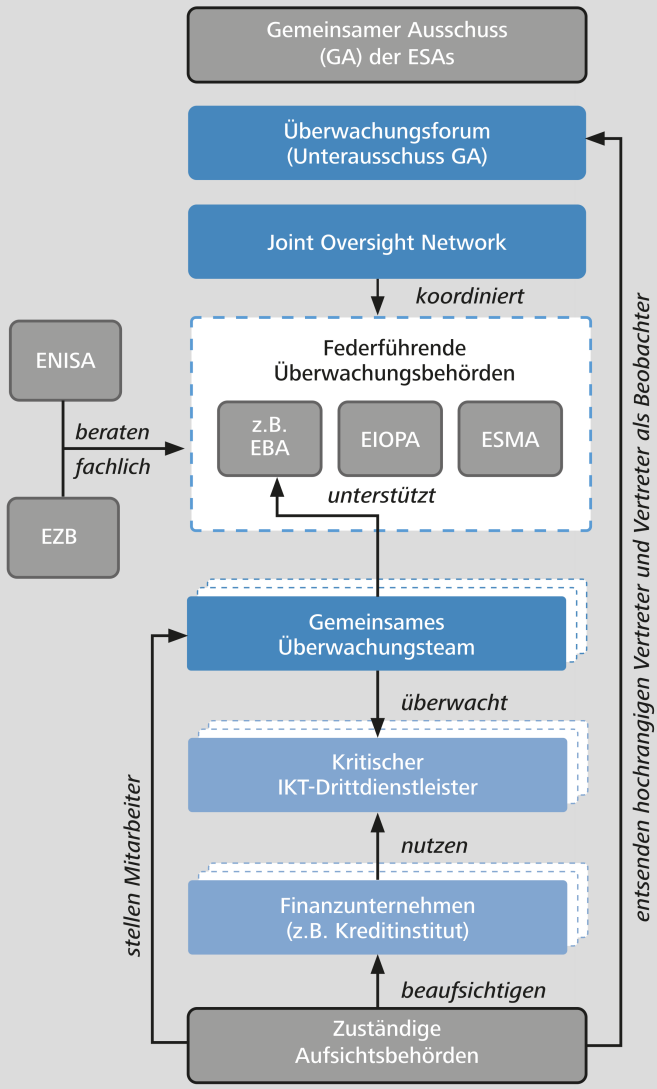
Exkurs

Das neue EU-Überwachungsrahmenwerk für kritische IKT-Drittdienstleister

Der gemeinsame Ausschuss der ESAs richtet das Überwachungsforum als Unterausschuss ein, der die Arbeit des gemeinsamen Ausschusses und der federführenden Überwachungsbehörden unterstützt. Kernelement des Überwachungsrahmens für kritische IKT-Drittdienstleister sind die federführenden Überwachungsbehörden, die entweder durch EBA, EIOPA oder ESMA (ESAs) gestellt werden. Eine kohärente operative Zusammenarbeit der federführenden Überwachungsbehörden wird durch das Joint Oversight Network sichergestellt, die hierfür ein gemeinsames Überwachungsprotokoll erstellen.

Struktur des Oversight Frameworks

Schaubild 4.5



Deutsche Bundesbank

Die federführenden Überwachungsbehörden werden von einem gemeinsamen Überwachungsteam (sogenanntes Joint Examination Team, JET) unterstützt, das für jeden kritischen IKT-Drittdienstleister eingerichtet wird. Die JETs setzen sich aus Mitarbeitenden der ESAs sowie der zuständigen Behörden zusammen, die die Finanzunternehmen beaufsichtigen, für die der kritische IKT-Drittdienstleister IKT-

Dienstleistungen erbringt. Die federführende Überwachungsbehörde ist befugt, gegenüber einem kritischen IKT-Drittdienstleister Empfehlungen auszusprechen, und dieser ist verpflichtet, dazu Stellung zu nehmen und die Bedenken der federführenden Überwachungsbehörde auszuräumen. In erster Linie soll ein kritischer IKT-Drittdienstleister mit der federführenden Überwachungsbehörde nach Treu und Glauben zusammenarbeiten und diese bei ihrer Arbeit unterstützen, als Ultima Ratio sieht DORA aber die Verhängung von Zwangsgeldern durch die federführende Überwachungsbehörde vor. Zudem kann die federführende Überwachungsbehörde es grundsätzlich öffentlich machen, wenn der kritische IKT-Drittdienstleister sie nicht ausreichend oder fristgerecht über den Umgang mit Empfehlungen unterrichtet.

Festgestellt werden gegenseitige Abhängigkeiten und etwaige hohe kritische Konzentrationen bei IKT-Drittdienstleistern über die Auswertung der Register von Drittbezügen der beaufsichtigten Finanzunternehmen. Auf dieser Basis werden die kritischen IKT-Drittdienstleister bestimmt. Die Überwachung durch die federführende Überwachungsbehörde soll insbesondere über einen ständigen Dialog mit diesen IKT-Drittdienstleistern über deren IKT-Risikosituation erfolgen. Zur Wahrnehmung ihrer Aufgaben und Überwachungstätigkeiten ist die federführende Überwachungsbehörde zu Auskunftsersuchen, allgemeinen Untersuchungen sowie Vor-Ort-Inspektionen bei den kritischen IKT-Drittdienstleistern befugt. Dabei geht es um die Bewertung des Managements von IKT-Risiken, die vom kritischen IKT-Drittdienstleister auf die Finanzunternehmen übertragen werden können, weil sie IKT-Drittdienstleistungen berühren, die kritische oder wichtige Funktionen von Finanzunternehmen unterstützen.

In DORA wird festgelegt, auf welche Bereiche des IKT-Risikomanagements sich die Bewertung bei kritischen IKT-Drittdienstleistern erstrecken soll. Die Bewertung des IKT-Risikomanagements des kritischen IKT-Drittdienstleisters erfolgt auf der Grundlage eines Überwachungsplans, und soll

- die Sicherheit, Verfügbarkeit, Kontinuität, Skalierbarkeit und Qualität der Dienste berücksichtigen,
- die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der Daten einbeziehen,
- die IKT-Risikomanagementstrategie, die IKT-Geschäftsfortführungsleitlinie sowie die IKT-Reaktions- und Wiederherstellungspläne umfassen und die Governance-Regelungen betrachten,
- die Prozesse für IKT-bezogene Vorfälle, die Ermittlung, Überwachung, Meldung an Finanzunternehmen, Behandlung und Lösung einbeziehen,

- die Mechanismen zur wirksamen Wahrnehmung der Kündigungsrechte durch die Finanzunternehmen beinhalten, welche die Datenübertragbarkeit, Übertragbarkeit von Anwendungen und Interoperabilität sicherstellen sollen,
- das Testen von IKT-Systemen und Infrastrukturen sowie die Kontrollen umfassen und
- die IKT-Audits sowie die Übernahme einschlägiger Normen berücksichtigen.

Die kritischen IKT-Drittdienstleister unterliegen jedoch nicht den Anforderungen, die DORA an das IKT-Risikomanagement der Finanzunternehmen richtet.

2.3.5 Identifizierung

Ein effektives IKT-Risikomanagement benötigt vollständige und aktuelle Informationen über IKT-Assets. [14)] Ein effektives IKT-Risikomanagement kann nur betrieben werden, wenn die zugrunde liegenden Informationen aktuell und korrekt sind. Nur wer seine Funktionen und Assets kennt, kann diese zielgerichtet vor Risiken schützen. Daher ist es grundlegend, die spezifischen IKT-Risiken und kritischen und wichtigen Funktionen präzise zu bestimmen. Dabei sind die strategischen Vorgaben und das spezifische Geschäftsmodell zu berücksichtigen. IKT-Systeme und Daten, die diese kritischen und wichtigen Funktionen unterstützen, müssen ein hohes Maß an digitaler operationaler Resilienz aufweisen. Um hohe Standards bezüglich Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit zu gewährleisten, sind klare Kriterien für die Bewertung der Kritikalität der Daten und IKT-Systeme zu etablieren. Dies setzt voraus, dass umfassende und aktuelle Informationen über Daten und IKT-Assets sowie über deren Interdependenzen vorliegen. Prüfungen der Bundesbank haben wiederholt Defizite hinsichtlich des Umfangs und der Vollständigkeit der Auswirkungs- und Kritikalitätsanalysen (sogenannte Schutzbedarfsanalyse) sowie der Aktualität der Informationen zu IKT-Assets festgestellt. Künftig müssen Finanzunternehmen die entsprechenden Inventare ihrer IKT-Assets und Risiken vorhalten und regelmäßig sowie bei wesentlichen Änderungen aktualisieren.

Striktere Überwachung der Risiken von IKT-Altsystemen. IKT-Systeme veralten, denn ab einem gewissen Zeitpunkt werden keine Ersatzteile für die Hardware oder Sicherheitsupdates für die Software mehr bereitgestellt. Werden IKT-Altsysteme dennoch weiterbetrieben, bedürfen diese einer besonderen Aufmerksamkeit, da die fehlenden Sicherheitsupdates die Verwundbarkeit für Cyberangriffe erhöhen. Daher ist es zwingend erforderlich, den Lebenszyklus von IKT-Systemen zu überwachen und zu steuern. Obwohl diese Problemstellung in der BAIT-Novelle 2021 hervorgehoben wurde, haben Prüfungen häufig gezeigt, dass diese Systeme unzureichend überwacht und gesteuert werden. DORA verpflichtet zu einer gründlichen Risikobewertung bei der Integration von IKT-Systemen sowie zu einer mindestens jährlichen Neubewertung.

2.3.6 Schutz und Prävention sowie Erkennung

Nach der Identifikation kritischer Daten und IKT-Systeme sind durchgehend Schutzmaßnahmen zu implementieren, die in allen Verarbeitungsstadien – Speicherung, Übertragung und Verarbeitung – wirksam sind. Regelmäßige Tests zur Wirksamkeit der implementierten Schutzmaßnahmen werden notwendig. Das

14 IKT Assets bezeichnen "eine Software oder Hardware in den Netzwerk- und Informationssystemen, die das Finanzunternehmen nutzt", vgl.: DORA, Artikel 3, Nummer 7.

Leitungsorgan hat die Aufgabe, eine Informationssicherheitsleitlinie zu verabschieden, die die grundlegenden Schutzanforderungen für Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit verbindlich vorschreibt. Auf dieser Basis müssen IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -tools entwickelt werden, um die einzelnen Sicherheitsmaßnahmen weiter zu präzisieren. Beispielsweise sollen Netzwerksegmente und Geräte im Falle eines Cyberangriffs möglichst automatisch isoliert werden können und automatische Schwachstellenscans für IKT-Systeme, die kritische oder wichtige Funktionen unterstützen, mindestens wöchentlich durchgeführt werden.

Neben diesen technischen und prozessualen Vorgaben ist dem Faktor Mensch Rechnung zu tragen und die notwendige Sensibilisierung für IKT-Risiken zu schaffen. So hat eine Studie von Gartner 2022 ergeben, dass mehr als zwei Drittel aller Angestellten wissentlich gegen die Sicherheitsvorschriften verstoßen, um komfortabel arbeiten zu können.[15)] Es ist also wichtig, dass die Sicherheitsmaßnahmen in die IKT-Systeme integriert und dabei gleichzeitig möglichst einfach und praktikabel sind. Prüfungen haben wiederholt gezeigt, dass wichtige Sicherheitsmaßnahmen fehlten oder nicht effektiv umgesetzt wurden. Lücken in den Schutzmaßnahmen wurden aufgrund eines unzureichenden Schwachstellenmanagements nicht aufgedeckt und folglich nicht behoben, was Institute anfälliger für Cyberangriffe machte. Mit DORA müssen Schutzmaßnahmen nun regelmäßig und unabhängig im Rahmen eines umfassenden Testprogramms überprüft werden.

15 Vgl.: 2022 Gartner Drivers of Secure Behavior Survey, gartner.com, letzter Abruf: 16. August 2024.

Exkurs

Bedrohungsgeleitete Penetrationstests (Threat-led Penetration Testing)

Mit dem Inkrafttreten von DORA im Januar 2025 werden die bisher freiwilligen TIBER-Tests, nun als Threat-led Penetration Testing (TLPT) bezeichnet, für bestimmte Finanzunternehmen in der EU verpflichtend. TLPT wird somit ein Instrument der Finanzaufsicht, das aber nicht primär auf die Erfüllung regulatorischer Anforderungen gerichtet ist, sondern durch dessen besonderen Lerncharakter den Unternehmen Potenzial für die Verbesserung der eigenen Widerstandsfähigkeit gegen Cyberangriffe aufzeigen soll.

Die allgemeinen Anforderungen an die Durchführung von TLPT sind im technischen Regulierungsstandard (RTS on TLPT [1]) festgelegt. Dieser orientiert sich eng an dem in der EU weitverbreiteten TIBER-Rahmenwerk [2], das als eine „Durchführungsanleitung" für das konkrete Vorgehen bei einzelnen Tests dient. TIBER, kurz für „Threat Intelligence-Based Ethical Red Teaming", beinhaltet die Simulation realistischer Cyberangriffe auf kritische IKT-Systeme von Finanzunternehmen durch „ethische Hacker" (Red Team Tester), basierend auf einer Bedrohungsanalyse. Dies ermöglicht eine realitätsnahe Erprobung des unternehmensspezifischen Sicherheitsniveaus. In Deutschland unterstützt das TIBER-Kompetenzzentrum der Bundesbank und das TIBER Cyber Team Deutschland (TCT-DE) bereits seit 2020 die Durchführung von TIBER-Tests nach diesem Rahmenwerk. Die in fünf Jahren gesammelten Erfahrungen des TCT-DE fließen nahtlos in die Umsetzung von TLPT unter DORA ein.

Gemäß DORA kommen verschiedene Arten von Finanzunternehmen für die verpflichtende Durchführung von TLPT infrage, darunter Kreditinstitute, Versicherungen und Finanzmarktinfrastrukturen. Da TLPT ein fortgeschrittenes Instrument zur Stärkung der operationalen Resilienz ist, setzt es ein Mindestmaß an Reife des IKT-Sicherheitsniveaus voraus. Nur so kann der Test effektiv durchgeführt werden und Nutzen stiften. Nicht alle genannten Finanzunternehmen müssen daher TLPT durchführen. Artikel 26 (8) DORA legt drei Auswahlkriterien fest: (1)

1 Vgl. beispielsweise: eba.europa.eu, letzter Abruf: 16. August 2024.
2 Für weitere Informationen zu TIBER, siehe: bundesbank.de.

wirkungsbezogene Faktoren (Auswirkungen der Tätigkeiten des Finanzunternehmens auf den Finanzsektor), (2) Finanzstabilität und (3) IKT-Risikoprofil und IKT-Reifegrad. Der RTS on TLPT detailliert diese Auswahlkriterien weiter aus und führt eine Unterscheidung in quantitative institutsbezogene und qualitative risikobezogene Kriterien ein.

Insbesondere fallen systemisch relevante Kreditinstitute (G-SIIs und O-SIIs gemäß Artikel 131 der Richtlinie 2013/36/EU) in den Anwendungsbereich des RTS und müssen TLPT durchführen. In Deutschland betrifft dies hauptsächlich Kreditinstitute, die direkt von der EZB beaufsichtigt werden. Der RTS benennt Zentralverwahrer (Central Security Depository, CSD), zentrale Gegenparteien (Central Counterparty, CCP) und die größten Handelsplätze (Börsen) eines Mitgliedstaates sowie Versicherungen, Zahlungsinstitute und E-Geld-Institute, wenn sie bestimmte quantitative Kriterien erfüllen.

Letztlich entscheidet die zuständige Aufsichtsbehörde, welche Finanzunternehmen die Kriterien erfüllen, und benachrichtigt diese im Vorfeld der Tests. Für bedeutende Kreditinstitute sind dies die EZB, für Börsen die Börsenaufsichtsbehörden der Länder und für alle anderen Finanzunternehmen in Deutschland die BaFin. Die Anforderungen zu TLPT richten sich mehrheitlich an große, systemrelevante Finanzunternehmen. In der Regel haben diese Finanzunternehmen in der Vergangenheit bereits einen TIBER-Test durchgeführt und stehen bereits mit dem TCT der Bundesbank in Kontakt.

Die operative Begleitung der TLPT wird nach heutigem Stand weiterhin durch das TCT der Bundesbank erfolgen, das als erster Ansprechpartner für die Unternehmen fungieren und für die laufende Kommunikation während des TLPT verantwortlich sein soll. Um die Realitätsnähe der Tests zu wahren, muss die Durchführung im streng vertraulichen Rahmen stattfinden, und nur ein begrenzter Personenkreis im Unternehmen darf Kenntnis vom TLPT haben. Das TCT unterstützt die Unternehmen mit seiner Expertise sowie Erfahrungen aus anderen Tests, um einen reibungslosen Ablauf der TLPT zu gewährleisten und die Lernerfahrung für die Unternehmen zu maximieren.

Die Aufsichtsbehörden auf europäischer und auf nationaler Ebene werden aber künftig stärker in die Vorbereitung und Nachbereitung von TLPT eingebunden sein. Ebenso wird die Zusammenarbeit mit den bestehenden nationalen TCTs in den jeweiligen EU-Ländern intensiviert. Die Aufsichtsbehörden sind insbesondere bei der Identifikation, Planung und Anordnung der Tests sowie bei der Validierung des Testumfangs involviert. Nach Abschluss des TLPT erstellt das getestete Unternehmen einen Abschlussbericht und einen Behebungsplan, die an die Aufsichtsbehörden übermittelt werden, die die identifizierten Schwächen nachverfolgen.

Die konkreten Aufklärungs- und Angriffsschritte bei TLPT werden von spezialisierten Dienstleistern, den Threat-Intelligence- und den Red-Teaming -Dienstleistern, durchgeführt. Der Threat-Intelligence-Dienstleister führt die Bedrohungsanalyse durch und erstellt realitätsnahe Angriffsszenarien. Der Red-Teaming-Dienstleister setzt diese Szenarien anschließend durch simulierte Cyberangriffe um. Der RTS on TLPT definiert Mindestkriterien für deren Erfahrung und Expertise, die sich an den Anforderungen des TIBER-Rahmenwerks orientieren, diese konkretisieren sowie in einigen Aspekten erweitern. Damit wird sichergestellt, dass TLPT mit den höchsten Qualitätsstandards durchgeführt werden. Während der Threat Intelligence-Dienstleister in jedem Fall extern beauftragt sein muss, kann das Red Teaming unter bestimmten Bedingungen durch interne Tester erfolgen; allerdings muss jeder dritte TLPT durch externe Tester durchgeführt werden. Für von der EZB direkt beaufsichtigte Kreditinstitute ist der Einsatz interner Tester gemäß Artikel 26 (8) DORA nicht gestattet.

Die rechtzeitige Erkennung von anomalen Aktivitäten und Verhalten ist ein unverzichtbarer Bestandteil einer proaktiven Verteidigung. In Anbetracht der komplexen und sich stetig weiterentwickelnden Bedrohungslandschaft ist es unumgänglich, Mechanismen zu implementieren, die es ermöglichen, ungewöhnliche Aktivitäten und Verhaltensweisen in IKT-Systemen sowie bei den Nutzern schnell zu identifizieren und effektiv darauf zu reagieren. Es ist daher erforderlich, alle relevanten Informationen der IKT-Systeme fortlaufend zu erfassen, sicher zu speichern und sorgfältig zu analysieren. Werden Muster identifiziert, die Angreifer häufig verwenden oder die vom Normalzustand abweichen, muss ein automatisierter Alarm ausgelöst und von spezialisiertem Personal umgehend auf potenzielle IKT-Vorfälle hin überprüft werden.

In der Vergangenheit wurde bei BAIT-Prüfungen festgestellt, dass nicht alle notwendigen Informationen erfasst wurden oder dass die gesammelten Daten nicht in angemessener Weise und ohne die nötige Zeitnähe analysiert wurden. DORA fordert künftig ein, dass genügend Ressourcen und passende IKT-Tools vorgehalten sowie klare Zuständigkeiten und Verantwortlichkeiten festgelegt werden.

2.3.7 Reaktion und Wiederherstellung sowie Backups

Umfassende Notfallpläne und regelmäßige Tests der Pläne halten Institute funktionsfähig. Trotz umfassender präventiver Schutzmaßnahmen und proaktiver Strategien zur Erkennung von IKT-Störungen und Cyberangriffen muss die Möglichkeit einer Beeinträchtigung der IKT-Systeme in Betracht gezogen werden. Deshalb müssen effektive Notfallpläne vorgehalten werden, um kritische oder wichtige Funktionen im Falle von IKT-Störungen und Angriffen aufrechtzuerhalten, Schäden zu begrenzen und den Betrieb schnell wiederherzustellen. Die Pläne haben sofortige Eindämmungsmaßnahmen sowie auf alle relevanten Situationen angepasste Reaktions- und Wiederherstellungsverfahren inklusive der dafür notwendigen Ressourcen zu beinhalten. Hierfür sind effektive Kommunikationsstrategien für interne und externe Stakeholder sowie Behörden zu etablieren. Die ausreichend detaillierten Notfallpläne sind regelmäßig auf ihre Wirksamkeit zu testen; ein Bereich, in dem die Aufsicht noch Verbesserungspotenzial bei den beaufsichtigten Instituten sieht. Mit DORA werden die notwendigen Szenarien nun nochmals deutlich detaillierter vorgegeben und die Tests der Pläne verbindlich eingefordert.

Robuste Backups und Wiederherstellungstools sind für Finanzinstitute fundamental, um katastrophale Schäden zu minimieren. Angesichts der zunehmenden Bedrohung durch Ransomware, bei der die Angreifer sowohl operative Daten als auch Backups von Unternehmen verschlüsseln und ein Lösegeld für die Entschlüsselung verlangen, ist es von größter Wichtigkeit, sich mit robusten Backup-Strategien, abgestimmten Backup-Zyklen und wirksamen Methoden zur

Datenwiederherstellung und Systemreparatur zu wappnen. Diese, in bankaufsichtlichen Prüfungen teilweise vermissten, Maßnahmen sind entscheidend, um im Falle eines Angriffs die Betriebsunterbrechungen zu verkürzen und potenziell katastrophale Datenverluste und die damit einhergehenden Schäden zu minimieren. DORA geht die die Gefahr von Ransomware an, indem unter anderem. die Backups durch physische und logische Trennung von den Produktionssystemen besser vor Angreifern geschützt werden müssen.

2.3.8 Bedrohungsinformationen und Kommunikation

Aktiver Informationsaustausch über Cyberbedrohungen und Lessons Learned aus Vorfällen verbessern die eigene Sicherheitslage. Die sich ständig wandelnde Cyber-Bedrohungslandschaft erfordert von Unternehmen mehr, als einmalig ihren IKT-Risikomanagementrahmen zu entwickeln und diesen zu aktualisieren. Vielmehr ist eine kontinuierliche Informationsbeschaffung über Schwachstellen und Bedrohungen notwendig, um die eigene Resilienz zu stärken. Darüber hinaus muss das Risikomanagementrahmenwerk regelmäßig, insbesondere nach gravierenden IKT-bezogenen Vorfällen oder bei der Aufdeckung von Defiziten, auf Verbesserungsmöglichkeiten hin evaluiert und daraufhin unter Umständen adjustiert werden. Vergangene Prüfungen haben häufig aufgezeigt, dass Finanzinstitute externe Bedrohungsinformationen unzureichend nutzen und somit kein akkurates Bild der individuellen Sicherheitslage besitzen. DORA empfiehlt nun, dass sich Institute aktiv in Netzwerken zum Austausch von Informationen und Erkenntnissen über Cyberbedrohungen engagieren.

Kommunikationspläne und klare Zuständigkeiten bei IKT-Störungen vermindern Reputationsrisiken. IKT-Störungen und Cyberangriffe können neben finanziellen Schäden erheblichen Reputationsverlust verursachen. In der Vergangenheit wurde nicht immer angemessen auf IKT-Vorfälle reagiert, indem verspätet oder uneinheitlich mit relevanten Stakeholdern kommuniziert wurde. DORA schreibt nun vor, dass spezifische Kommunikationspläne für alle relevanten Interessensgruppen, einschließlich Kunden, andere Finanzunternehmen und die Öffentlichkeit, bereitgehalten werden. Zudem ist eine eindeutige Verantwortlichkeit für die Kommunikation im Falle von IKT-Vorfällen zu definieren.

3 Ausblick

Wir befinden uns im digitalen Zeitalter, in der Informations- und Kommunikationstechnologien essenziell für Finanzunternehmen sind, die hochgradig miteinander vernetzt und voneinander abhängig sind. Es ist daher unerlässlich, den damit einhergehenden Risiken durch digitale operationale Resilienz zu begegnen. Mit DORA wird ein bedeutender Meilenstein hinsichtlich des Managements von IKT-Risiken im Finanzsektor gesetzt.

Unternehmen profitieren von einem harmonisierten Risikomanagementansatz, der die Risiken aus IKT-Drittdienstleistungen einbezieht, wodurch der Finanzsektor im Umgang mit IKT-Drittdienstleistern gestärkt wird. Gleichzeitig ist es unerlässlich, dass in den beaufsichtigten Instituten das Verständnis weiterwächst, dass die Implementierung und Aufrechterhaltung eines robusten IKT-Risikomanagementrahmens nicht ausschließlich eine Frage der Erfüllung regulatorischer Vorgaben darstellt. Vielmehr liegt es im eigenen fundamentalen Interesse der Institute, solche soliden Risikomanagementpraktiken zu etablieren und zu pflegen.

Die deutsche Aufsicht hat sich in der Vergangenheit immer aktiv für ein effektives und praxisorientiertes IKT-Risikomanagement der Institute eingesetzt. Insbesondere die Erkenntnisse aus Prüfungen und aus Dialogen mit Finanzunternehmen und IKT-Drittdienstleistern sind wertvolle Grundlagen, um die zukünftigen Herausforderungen im Umgang mit IKT-Risiken zu identifizieren und die Weiterentwicklung regulatorischer Vorgaben praxisnah voranzubringen.

DORA trägt zur Sicherung der Integrität, Verfügbarkeit und Vertraulichkeit der Informations- und Kommunikationssysteme der beaufsichtigten Finanzunternehmen bei und schützt somit vor potenziellen finanziellen Verlusten, Reputationsrisiken und anderen operationellen Risiken, die aus IKT-bezogenen Bedrohungen resultieren können. Angesichts der dynamischen Entwicklung durch die Digitalisierung und der sich ständig verändernden Bedrohungslage ist jedoch absehbar, dass zukünftige Anpassungen an der Regulierung erforderlich sein werden. Der europäische Gesetzgeber plant daher, DORA bis zum Jahr 2028 zu überprüfen und einen Bericht darüber sowie gegebenenfalls einen Gesetzgebungsvorschlag vorzulegen.

Literaturverzeichnis

Tremmel, S. (2024), Vermeidbares Übel – Hergang und Folgen des CrowdStrike-Vorfalls, c´t, Nr. 18/2024, S. 14 f.