Schwerwiegende IKT-Vorfälle unter DORA

Meldepflichten und Praxisanforderungen unter DORA: Wie DORA und die BaFin den Umgang mit IKT-Vorfällen neu definieren und welche neuen Anforderungen damit verbunden sind – insbesondere bei (Teil-)Ausfällen von IKT-Drittdienstleistern, Cyberangriffen, Systemausfällen oder internen Sicherheitsverletzungen.

Mit der DORA-Verordnung (Digital Operational Resilience Act – Verordnung (EU) 2022/2554) sowie den technischen Regulierungsstandards (RTS 2024/1774[1] und RTS 2025/301[2]) wird der Umgang mit sogenannten IKT-Vorfällen verbindlich geregelt. Gleichzeitig konkretisiert die BaFin mit ihren Leitlinien, welche Erwartungen sie an die Institute stellt. Dieser Beitrag beleuchtet die gesetzlichen Anforderungen, grenzt den Begriff des IKT-Vorfalls praxisnah ab und beschreibt, welche Schritte im Ereignisfall notwendig sind.

Gesetzliche Anforderungen

Der Art. 3 Abs. 8 DORA definiert IKT-Vorfälle als nicht geplante Ereignisse bzw. eine entsprechende Reihe von Ereignissen, die die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigen und negative Auswirkungen auf die Sicherheitsziele von Daten oder Diensten haben.

Art. 17 bis 23 DORA regeln den detaillierten Umgang mit IKT-Vorfällen und verpflichtet, Institute, Verfahren zur Erkennung, Klassifizierung, Behandlung und Meldung vorzuhalten.

Die Klassifizierung von Wesentlichkeitsschwellen und der Einzelheiten von Meldungen schwerwiegender Vorfälle ist im RTS 2024/1772 vorgegeben.

Die Meldefristen für schwerwiegende IKT-Vorfälle hat die BaFin im September 2024 präzisiert (BaFin – Veranstaltungen – Präsentation 4 – IKT-Vorfallsmeldewesen)[3].

Was ist ein IKT-Vorfall und wie ist er zu bewerten?

Nicht jede Störung ist ein meldepflichtiger IKT-Vorfall. Entscheidend ist die Auswirkung auf Funktionen oder Informationen. Abb. 1. gibt eine Orientierungshilfe, wie ein (potenzieller) IKT-Vorfall bewertet werden kann.

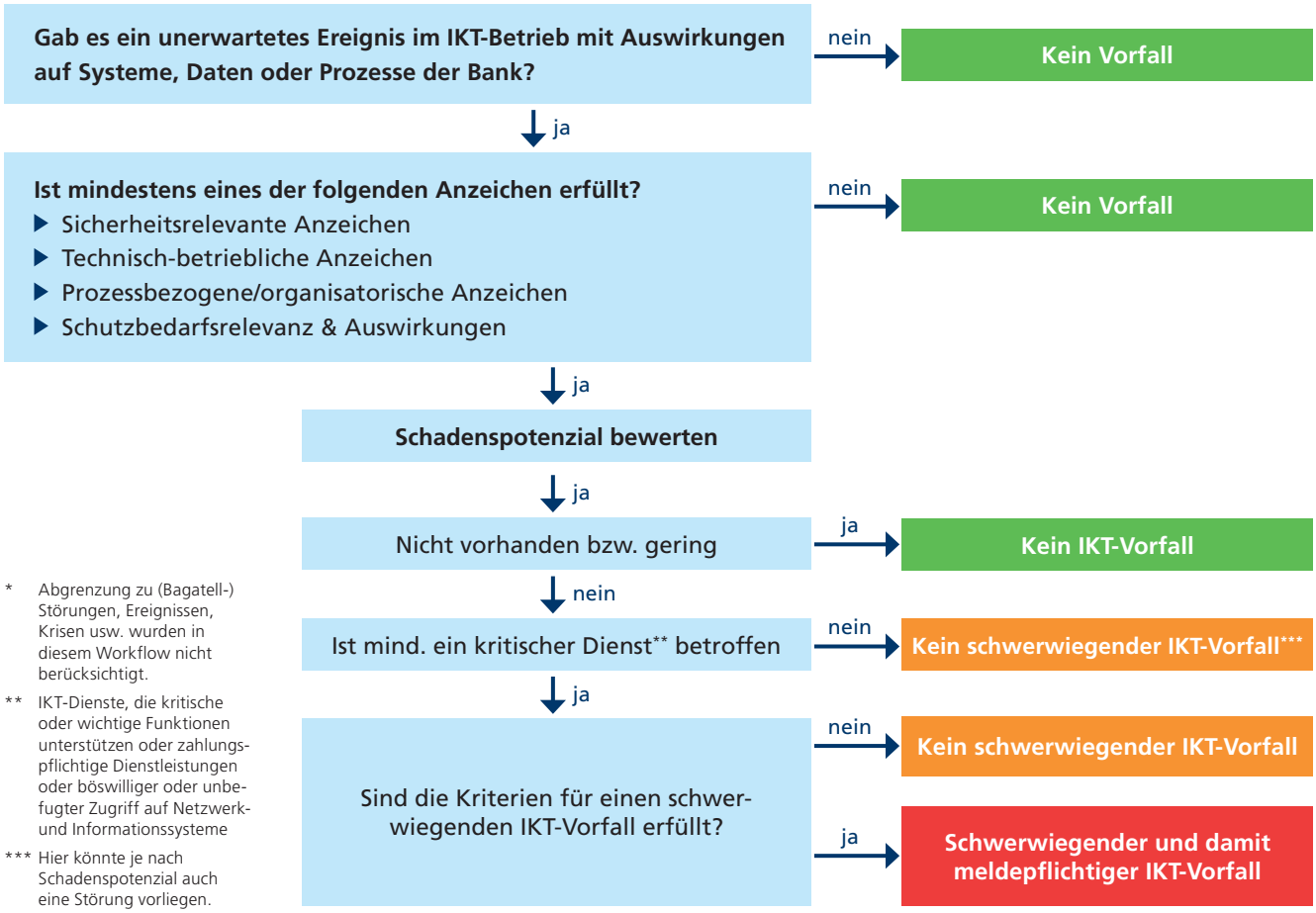
Sicherheitsrelevante Anzeichen

- Meldungen aus dem Security Information and Event Management (SIEM)
- Hinweise auf Malware, z. B. durch Virenscanner oder ungewöhnliche Prozesse
- Phishing-Angriffe oder kompromittierte Zugangsdaten
- Unautorisierter Datenabfluss (Data Leakage)
- Ungewöhnliche Anmeldezeiten oder -orte (z. B. Login aus Ländern, in denen keine Beschäftigten tätig sind)

Technisch-betriebliche Anzeichen

- Systemausfälle (z. B. relevante Anzahl an Clients, Server, Netzwerk, Storage) ohne erkennbare Ursache
- Unerwartet hohe Last auf Systemen oder Netzwerken
- Unerklärliche Veränderungen an Konfigurationen oder Datenbeständen
- Signifikanter Anstieg von Fehlermeldungen oder Support-Tickets

Abb. 1. **Einordnen von IKT-Vorfällen***



* Abgrenzung zu (Bagatell-) Störungen, Ereignissen, Krisen usw. wurden in diesem Workflow nicht berücksichtigt.

** IKT-Dienste, die kritische oder wichtige Funktionen unterstützen oder zahlungspflichtige Dienstleistungen oder böswilliger oder unbefugter Zugriff auf Netzwerk- und Informationssysteme

*** Hier könnte je nach Schadenspotenzial auch eine Störung vorliegen.

Prozessbezogene/organisatorische Anzeichen

- Schutzbedarf (Authentizität, Vertraulichkeit, Integrität, Nachvollziehbarkeit, kurz ACIN) von Geschäftsprozessen ist gestört oder kann nicht mehr gewährleistet werden.
- Kommunikation über zentrale Kanäle ist beeinträchtigt (z. B. E-Mail, Telefon).
- Mitarbeiter meldet Auffälligkeiten bei Systemnutzung oder IKT-Dienstleistungen.
- Verfügbarkeit von Funktionen ist eingeschränkt/nicht mehr vorhanden (z. B. Zahlungsverkehr, Ordersysteme, Limitsysteme, Onlinebanking etc.).

Schutzbedarfsrelevanz & Auswirkungen

- Reputationsschäden, rechtliche Konsequenzen oder finanzielle Verluste sind möglich.

Der IKT-Vorfall hat per Definition eine gewisse Reichweite, z. B. über mehrere Organisationseinheiten oder Institute hinweg. Die obige Aufzählung gibt eine Orientierung, was einen Vorfall ausmachen kann. Wesentlich ist die Frage, ob der Schutzbedarf (ACIN) der Prozesse eingehalten werden kann. Hier zeigt sich auch ein direkter Mehrwert aus der Einwertung der Funktionen im Informationsverbund durch die Prozessverantwortlichen.

Wir sehen, dass die Prozessverantwortlichen, die Beauftragten und der IT-Betrieb durch die Anforderungen immer enger und abgestimmter im Informationsverbund zusammenarbeiten.

Was ist zu tun, wenn ein IKT-Vorfall vorliegt?

Sobald ein IKT-Vorfall identifiziert ist, muss dessen Wesentlichkeit (RTS 2024/1772) eingestuft werden. Das Ergebnis zeigt auf, ob der IKT-Vorfall der BaFin gemeldet

werden muss (schwerwiegender IKT-Vorfall, vgl. Abb. 1). Die Klassifizierungskriterien werden in sieben Kategorien geclustert:

- Kunden, finanzielle Gegenparteien und Transaktionen
- Reputationsschaden
- Dauer und Ausfallzeit
- Geografische Ausbreitung
- Verlust von Daten
- Kritikalität der betroffenen Dienste
- wirtschaftliche Auswirkung

Im Rahmen der Anforderungen des RTS 2024/1772 haben wir als DZ CompliancePartner unseren Mandanten ein Tool bereitgestellt, mit dem sich die relevanten Kriterien systematisch abfragen lassen. Das Tool liefert eine klare Auswertung darüber, ob ein schwerwiegender und somit meldepflichtiger IKT-Vorfall vorliegt.

Im Falle einer Einstufung als schwerwiegender Vorfall leitet die Bank unverzüglich geeignete Gegenmaßnahmen ein, um die Auswirkungen einzugrenzen. Parallel dazu werden die vorgesehenen Kommunikationspläne aktiviert. Der Beauftragte IKT-Risikomanagement und Informationssicherheit bewertet gemeinsam mit dem zuständigen Fachverantwortlichen das Risiko für die Bank.

Die Erstmeldung eines schwerwiegenden IKT-Vorfalls an die BaFin erfolgt innerhalb der gesetzlich vorgegebenen Fristen über das Meldeportal der BaFin. Sollte sich der Sachstand der Erstmeldung wesentlich ändern oder sollten neue Erkenntnisse eine Neubewertung erfordern, wird eine Zwischenmeldung abgegeben. Zudem kann die BaFin jederzeit eine Zwischenmeldung anfordern. Nach Abschluss der Ursachenanalyse und der Ermittlung der tatsächlichen Auswirkungen wird eine Abschlussmeldung erstellt.

Grundsätzlich besteht die Möglichkeit, die Pflichten zur Meldung schwerwiegender IKT-Vorfälle auszulagern. Hierbei sind jedoch weitere aufsichtsrechtliche Anforderungen zu beachten. Kunden der ATRUVIA AG können diese Meldepflichten über das Produkt DORA-MIR auslagern. DORA-MIR umfasst eine 24/7-Überwachung von Störungen anhand der Kriterien gemäß Art. 18 und 23 DORA sowie die fristgerechte Übermittlung der erforderlichen Meldungen an die BaFin. Für Rückfragen der Aufsicht steht ebenfalls die ATRUVIA AG als primärer Ansprechpartner zur Verfügung.

Fazit

DORA regelt den Umgang mit IKT-Vorfällen neu. Ob tatsächlich ein meldepflichtiger IKT-Vorfall vorliegt entscheidet sich über die Frage nach den Auswirkungen der Störung. Wesentlich ist die Frage, ob der Schutzbedarf eingehalten werden kann oder eben nicht. Wenn es sich um einen schwerwiegenden Vorfall handelt, müssen einerseits unmittelbar Gegenmaßnahmen ergriffen werden und andererseits entsprechende Kommunikationspläne aktiviert werden.

Insgesamt ist mit DORA der Prozess um die Identifizierung schwerwiegender IKT-Vorfälle nachvollziehbarer und transparenter, leider aber auch aufwendiger geworden. ▬

[1] RTS 2024/1774 (https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401772, abgerufen am 25.04.2025)

[2] RTS 2025/301 (https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202500301, abgerufen am 25.04.2025)

[3] https://www.bafin.de/SharedDocs/Downloads/DE/Veranstaltung/dl_IT_Aufsicht_2024_4.html und https://www.bafin.de/DE/Aufsicht/DORA/Meldewesen_IKT_Vorfaelle/Meldung_schwerwiegender_IKT_bezogener_Vorfaelle_und_erheblicher_Cyberbedrohungen/Meldung_schwerwiegender_IKT_bezogener_Vorfaelle_und_erheblicher_Cyberbedrohungen_artikel.html

Frank Lutter
Beauftragter IKT-Risikokontrolle und Informationssicherheit,
E-Mail: frank-lutter@dz-cp.de

Benjamin Wellnitz
Bereichsleiter IKT-Risikokontrolle, Informationssicherheit & Datenschutz,
E-Mail: benjamin.wellnitz@dz-cp.de