Aus der DORA-Werkstatt:

Klassifizierungsschema für IKT-bezogene Vorfälle gemäß Artikel 18 (1) DORA-VO

**Verwendungshinweis:** Das nachstehende Schema dient der Klassifizierung von IKT-bezogenen Vorfällen gemäß Artikel 18 (1) DORA-VO und der Ermittlung der meldepflichtigen „schwerwiegenden IKT-bezogenen Vorfällen“ gemäß Artikel 19 (1) DORA-VO.

.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Kriterium | Kriterienbeschreibung |  |  |
| **1) Kritikalität der betroffenen Dienste** | Nein | Ja |
| 1.1 | KWF-relevanter IKT-Vorfall  | Der Vorfall beeinträchtigt (wahrscheinlich) IKT-Assets, die kritische oder wichtige Funktionen unterstützen. |  |  |
| 1.2 | Lizenzierungsrelevanter Vorfall | Der Vorfall beeinträchtigt (wahrscheinlich), zulassungs- oder registrierungspflichtige Finanzdienstleistungen. Eine Liste der lizenzierten Tätigkeiten wird bereitgestellt durch die EBA im Kontext des Informationsregister, abzurufen unter folgendem [Link](https://www.eba.europa.eu/sites/default/files/2024-06/ef5f4b3f-f81d-4c3f-b799-06058e28d67e/ITS%20on%20RoI%20-%20Annex%202%20list%20of%20licensed%20activities%20for%20data%20point%20model.xlsx). |  |  |
| 1.3 | Cybersicherheits-Angriff | Der Vorfall stellt (wahrscheinlich) einen erfolgreichen, böswilligen Cyber-Angriff dar und beeinträchtigt die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität von Daten. |  |  |
| 1.4 | Störung oder sonstiger IKT-Vorfall  | Der Vorfall stellt **keinen** Cyber-Angriff dar **und** betrifft auch **keine** * IKT-Assets, die kritische oder wichtige Funktionen unterstützen,
* zulassungs- oder registrierungspflichtige Finanzdienstleistungen
 |  |  |
| **2) Kunden, finanzielle Gegenparteien und Transaktionen** |
| 2.1 | Kundenwirksamer Vorfall | Der Vorfall betrifft (wahrscheinlich) eine relevante Anzahl von Kunden des Unternehmens. | ≤10%≤ 100.000 | > 10%> 100.000 |
| 2.2 | Vorfall mit Relevanz für finanzielle Gegenparteien | Der Vorfall betrifft (wahrscheinlich) eine relevante Anzahl von finanziellen Gegenparteien des Unternehmens. | ≤ 30%  | > 30% |
| 2.3 | Transaktionswirksamer Vorfall | Der Vorfall betrifft (wahrscheinlich), bezogen auf den täglichen Durchschnittswert, eine relevante Anzahl bzw. einen relevanten Wert von Transaktionen.  | ≤ 10%  | > 10% |
| 2.4 | Vorfall mit Auswirkung auf Geschäftsziele & Effizienz | Der Vorfall betrifft (wahrscheinlich) bedeutende Kunden & finanzielle Gegenparteien, die für Erreichung der Geschäftsziele oder Markteffizienz relevant sind. | nein | ja |
| **3) Reputationsschaden** | Nein | Ja |
| 3.1 | Medienwirksamer Vorfall | Über den Vorfall wird (wahrscheinlich) in den Medien berichtet. |  |  |
| 3.2 | Beschwerdewirksamer Vorfall | Der Vorfall führt (wahrscheinlich) zu wiederholten Beschwerden durch Kunden oder finanzielle Gegenparteien. |  |  |
| 3.3 | Compliance-relevanter Vorfall | Der Vorfall ist (wahrscheinlich) mit einem Verstoß gegen regulatorische Vorgaben verbunden. |  |  |
| 3.4 | Vorfälle mit Auswirkung auf den Kundenbestand | Vorfall führt (wahrscheinlich) zu einem bedeutenden Verlust von Kunden oder finanziellen Gegenparteien. |  |  |
| **4) Dauer und Ausfallzeiten** |
| 4.1 | 24h+ Vorfälle | Der Vorfall dauert (wahrscheinlich) mehr als 24 Stunden. | ≤ 24 h | > 24 h |
| 4.2 | KWF-relevante IKT-Ausfälle 2h+ | Der Vorfall betrifft IKT-Assets, die kritische oder wichtige Funktionen unterstützen und dauert (wahrscheinlich) mehr als 2 Stunden. | ≤ 2 h | > 2 h |
| **5) Geografische Ausbreitung** | Nein | Ja |
| 5.1 | Kunden & Partner in Mitgliedstaaten | Der Vorfall hat (wahrscheinlich) Auswirkungen auf Kunden und finanzielle Gegenparteien in anderen Mitgliedstaaten. |  |  |
| 5.2 | Niederlassungen oder Gruppenunternehmen in  | Der Vorfall hat (wahrscheinlich) Auswirkungen auf Zweigniederlassungen oder Finanzunternehmen innerhalb der, die in anderen Mitgliedstaaten tätig sind. |  |  |
| 5.3 | Finanzmarktinfrastrukturen oder Drittdienstleister  | Der Vorfall hat (wahrscheinlich) Auswirkungen auf Finanzmarktinfrastrukturen oder Drittdienstleister, die in anderen Mitgliedstaaten tätig sind. |  |  |
| **6) Verluste von Daten[[1]](#footnote-1)** | Nein | Ja |
| 6.1 | Auswirkung auf Verfügbarkeit von Daten | Der Vorfall verursacht (wahrscheinlich), dass benötigte Daten vorübergehend oder dauerhaft unzugänglich sind **und** dies negative Auswirkungen hat. |  |  |
| 6.2 | Auswirkung auf Vertraulichkeit von Daten | Der Vorfall verursacht (wahrscheinlich), dass Unbefugte Zugang zu oder Kenntnis von Daten erhalten **und** dies negative Auswirkungen hat. |  |  |
| 6.3 | Auswirkung auf Integrität von Daten | Der Vorfall hat (wahrscheinlich) zu einer nicht autorisierten Veränderung der Daten geführt **und** ist mit negativen Auswirkungen verbunden. |  |  |
| 6.4 | Auswirkung auf Authentizität von Daten | Der Vorfall hat (wahrscheinlich) die Vertrauenswürdigkeit der Datenquelle kompromittiert **und** ist mit negativen Auswirkungen verbunden. |  |  |
| *6.5* | *Cybersicherheits-Angriff* | *Siehe Punkt 1.3.* |
| **7) Wirtschaftliche Auswirkungen** |
| 7.1 | Vorfälle mit wirtschaftlichen Auswirkungen[[2]](#footnote-2) | Der Vorfall verursacht (wahrscheinlich) spürbare Kosten und Verluste für das Finanzunternehmen | ≤ 100 T€ | > 100 T€ |

Ermittlung der „schwerwiegenden IKT-bezogenen Vorfälle“

gemäß Artikel 19 (1) DORA-VO

Zur Ermittlung der meldepflichtigen Vorfälle sind auf Basis der Vorfallsklassifikation die „schwerwiegenden IKT-bezogenen Vorfälle“ zu bestimmen. Die detaillierten Vorgaben dazu finden sich im RTS zur Klassifizierung von IKT-bezogenen Vorfällen ([DELEGIERTE VERORDNUNG (EU) 2024/1772 DER KOMMISSION](https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401772)).

Potenziell meldepflichtig sind alle IKT-bezogenen Vorfälle, die das Primär-Kriterium „**Kritikalität der betroffenen Dienste**“ erfüllen. Die Meldepflicht ist an folgende konkretisierende Bestimmungen gekoppelt:

1. **Cybersicherheits-Angriffe:** Vorfälle, die gemäß Artikel 6 (c) des RTS einen „erfolgreichen, böswilligen und unbefugten Zugriff auf die Netzwerk- und Informationssysteme des Finanzunternehmens“ darstellen und damit das Kriterium „Kritikalität der betroffenen Dienste“ erfüllen, gelten unmittelbar als meldepflichtige „schwerwiegende IKT-bezogene Vorfälle“, unabhängig von der Bewertung der sekundären Vorfallskriterien.
2. **KWF-relevante IKT-Vorfälle und Vorfälle mit Bezug zu lizenzierten Tätigkeiten:** Vorfälle, die gemäß Artikel 6 (a) „IKT-Dienste oder Netzwerk- und Informationssysteme zur Unterstützung kritischer oder wichtiger Funktionen“ betreffen oder die gemäß Artikel 6 (b) zulassungs- oder registrierungspflichtige Tätigkeiten betreffen, gelten als „schwerwiegende IKT-bezogene Vorfälle“, wenn
* mindestens zwei sekundäre Vorfallskriterien als wesentlich eingestuft werden.
* sie mindestens zwei Mal innerhalb von 6 Monaten auftreten
* wenn sie wiederholt auftreten und dieselbe Ursache haben
* wenn sie wiederholt auftreten und zusammen mindestens zwei sekundäre Vorfallskriterien als wesentlich eingestuft werden.

**Das Vorliegen von wiederholten Vorfällen ist monatlich zu überprüfen.**



**Anhang 1: Hilfestellung zur Ermittlung von Kosten und Verlusten** nach Artikel 7 (1) des RTS zur Klassifizierung von IKT-bezogenen Vorfällen (DELEGIERTE VERORDNUNG (EU) 2024/1772)

|  |  |  |  |
| --- | --- | --- | --- |
| # | Kosten-/ Verlustart | Erläuterungen | Kosten in EUR (geschätzt) |
| a) | **Verluste durch gestohlene Vermögenswerte** | Beispielsweise gestohlene Gelder, Krypto-Vermögenswerte, Kundendaten, Geschäftsinformationen, Hardware, Verträge, Akte, etc.  |  |
| b) | **Kosten für neue Technik** | Ersatz oder Umzug von Software, Hardware oder Infrastruktur. |  |
| c) | **Personalkosten** | Kosten für zusätzliches Personal, Überstunden oder das Ersetzen von Teammitgliedern. |  |
| d) | **Vertragsstrafen** | Gebühren wegen nicht erfüllter Verträge. |  |
| e) | **Entschädigungen** | Zahlungen an betroffene Kunden. |  |
| f) | **Verluste durch fehlende Einnahmen** | Umsatzausfälle während des Vorfalls. |  |
| g) | **Kommunikationskosten** | Kosten für interne und externe Informationen, z. B. an Kunden oder Medien. |  |
| h) | **Beratungskosten** | Ausgaben für Rechtsanwälte, IT-Forensik und externe Experten, um das Problem zu lösen |  |
|  |  | **Summe:** |  |

Folgende Kosten sollen bei der Ermittlung der Wirtschaftlichen Auswirkungen **nicht** berücksichtigt werden:

1. Keine Wartungs- und Schulungskosten, d.h. keine regelmäßigen Ausgaben für die Instandhaltung von Infrastruktur, Geräten, Hardware und Software und auch keine Weiterbildungskosten
2. Keine Kosten für betriebliche Verbesserungen, d.h. keine Kosten für Upgrades, Verbesserungen oder Investitionen nach einem Vorfall
3. Keine regelmäßigen Beiträge für Versicherungen
1. Die Ursache des Vorfalls ist unerheblich, d.h. es sind auch technisch bedingte oder unbeabsichtigte Vorfälle zu bewerten. [↑](#footnote-ref-1)
2. Eine Hilfestellung zur Ermittlung der Kosten findet sich in Anhang 1 [↑](#footnote-ref-2)