ÖSTERREICHISCHE FMA·FINANZMARKTAUFSICHT

OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

FMA-DORA-DIALOG: DORA-VORFÄLLE & FÖRDERUNG INFORMATIONSAUSTAUSCH 16.6.2025

AGENDA

Begrüßung
Michael Hysek

Teil 1: DORA-Vorfälle & Cyberbedrohungen

- Überblick zu aktuellen Vorfällen & Cyberbedrohungen
  Anna Muri, Ulrike Rhomberg
- Management und Meldung von Vorfällen & Cyberbedrohungen
  Ulrike Rhomberg
- FMA-Hinweise zur Meldung & Klassifizierung
  Daniel Kirnbauer

Teil 2: Förderung des Informationsaustausches zu Cyberbedrohungen

- Informationsaustauschmöglichkeiten & Förderungsinitiative (CERT.at)
  Wolfgang Rosenkranz
- Beiträge BMI, WKO, Watchlist Internet
  Andreas Wimmer, Aslan Tugce, Valentine Auer

Ausblick
Sabine Balogh-Preininger

Überblick zu aktuellen Vorfällen & Cyberbedrohungen

ÜBERBLICK – ANZAHL EINGELANGTER VORFÄLLE & URSACHEN

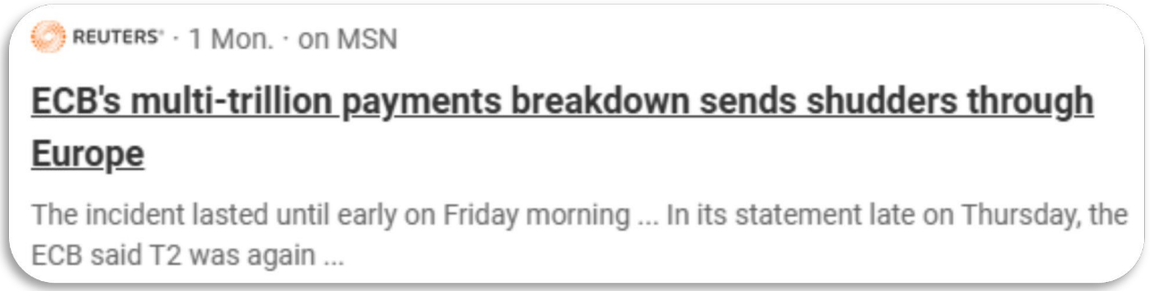
Erstmeldungen	Q1 2025	Q2 2025 (Stand 15.06.2025)
Anzahl gemeldete Vorfälle	17	25
davon als nicht schwerwiegend reklassifiziert	2	9
Gesamt	**15**	**16**

Ursprung IKT-Dienstleister	Q1 2025	Q2 2025 (Stand 15.06.2025)
	8	11

Ursachen lt. Zwischenmeldung (Mehrfachnennung möglich)	Q1 2025	Q2 2025 (Stand 15.06.2025)
System failure	6	11
Payment-related	5	1
External event	3	2
Process failure	1	-
Cybersecurity-related	2	2

Ursachen lt. Abschlussmeldung (Mehrfachnennung möglich)	Q1 2025	Q2 2025 (Stand 15.06.2025)
Malicious actions	2	2
Process failure	1	4
System failure / malfunction	9	7
Human error	1	2
External event	3	3

BEISPIEL: T2/T2S-VORFALL FEBRUAR 2025



- **TARGET2 (T2)** = Plattform des Eurosystems für die Abwicklung von Großbetragszahlungen

  TARGET2-Securities (T2S) = Plattform des Eurosystems für die Wertpapierabwicklung

- **Ursache der Störung:** Hardwarefehler, dadurch großer Backlog bei Großzahlungen und Wertpapier-Settlement

- Vielzahl an **Finanzunternehmen aus unterschiedlichen Sektoren** in der EU betroffen

➢ Mehrere **DORA Incidentmeldungen iZm T2/T2S** bei FMA eingegangen

Management & Meldung von Vorfällen & Cyberbedrohungen

RECHTLICHE VORGABEN

https://www.fma.gv.at/dora/ (Rubrik Rechtliche Grundlagen)		
DelVO 2024/1772: Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen (**RTS zu Incidentklassifizierung**)	Art. 18(3) DORA	**Delegierte Verordnung - EU - 2024/1772 - DE - EUR-Lex**
DelVO 2025/301: Festlegung Inhalt und Fristen für Meldungen schwerwiegender IKT-bezogener Vorfälle sowie der freiwilligen Meldung erheblicher Cyberbedrohungen (**RTS zu Incidentmeldungen**)	Art. 20(a) DORA	**Delegierte Verordnung - EU - 2025/301 - EN - EUR-Lex**
DurchführungsVO 2025/302: Berichtsdetails zu IKT-bezogenen Vorfällen (**ITS zu Incidentmeldungen**)	Art. 20(b) DORA	**Durchführungsverordnung - EU - 2025/302 - EN - EUR-Lex**
Leitlinien zur Kostenschätzung iZm schwerwiegenden Incidents	Art. 11(11) DORA	**Joint GL on the estimation of aggregated annual costs and losses caused by major ICT-related incidents**
Bericht zur Zentralisierung der Meldungen schwerwiegender IKT-bezogener Vorfälle	Art. 21 DORA	**Report on the feasibility for further centralisation of reporting of major ICT-related incidents**

INFORMATIONSQUELLEN BEI FRAGEN

https://www.fma.gv.at/dora/dora-ikt-bezogene-vorfaelle

(Rubrik Fragen und Antworten)

Fragen und Antworten

Welche Fristen gelten für die Prozessschritte?

Sind für die Einmeldung Formulare geplant?

https://www.eiopa.europa.eu/about/governance-structure/joint-committee/joint-qas_en

joint Q&A ID	Receiving ESA	Q&A ID at the ESA that received it	Date of publication of the final answer	Status	Legal act	Article	COM Delegated or Implementing Acts/RTS/ITS/GLs	Topic
DORA001	EIOPA	2622		Under review	DORA - Regulation (EU) 2022/2554	3(22)	N/A	Other DORA topics

Filters:

Legal act

DORA - Regu...

DORA - Regu...

KLASSIFIZIERUNGSANSATZ

Erkennung eines Vorfalls

Verpflichtendes Kriterium:
Kritikalität der betroffenen Dienste

I. Erfolgreicher, böswilliger und unbefugter Zugriff auf Netzwerk- und Informationssysteme, sofern dieser Zugriff zu Verlusten von Daten führen kann

II. Überschreitung der Schwellenwerte von zwei oder mehr der folgenden Kriterien:

- Kunden, finanzielle Gegenparteien und Transaktionen
- Reputationsschaden
- Dauer und Ausfallzeiten
- Geografische Ausbreitung
- Verluste von Daten (Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten)
- Wirtschaftliche Auswirkungen

Vorfall ist als schwerwiegender IKT-bezogener Vorfall an die FMA zu melden

KRITERIEN (1)

Kriterium DelVO (EU) 2024/1772	Schwellenwerte
Kritikalität der betroffenen Dienste	**Der Vorfall hat** a) IKT-Dienste oder Netzwerk- und Informationssysteme zur Unterstützung kritischer oder wichtiger Funktionen des Finanzunternehmens beeinträchtigt oder b) von dem Finanzunternehmen erbrachte Finanzdienstleistungen beeinträchtigt, die einer Zulassung oder Registrierung bedürfen oder von den zuständigen Behörden beaufsichtigt werden oder c) einen erfolgreichen, böswilligen und unbefugten Zugriff auf die Netzwerk- und Informationssysteme des Finanzunternehmens dargestellt.
Verluste von Daten	a) Jede **Auswirkung** auf die **Verfügbarkeit**, **Authentizität**, **Integrität** oder **Vertraulichkeit** von Daten, sofern dies negative Auswirkungen auf die Verwirklichung der Geschäftsziele des Finanzunternehmens oder auf dessen Fähigkeit, regulatorische Anforderungen zu erfüllen, hat oder haben wird b) Jeder **erfolgreiche, böswillige und unbefugte Zugriff auf Netz- und Informationssysteme**, welcher **nicht unter Punkt a)** fällt und zu einem **Datenverlust führen kann**

KRITERIEN (2)

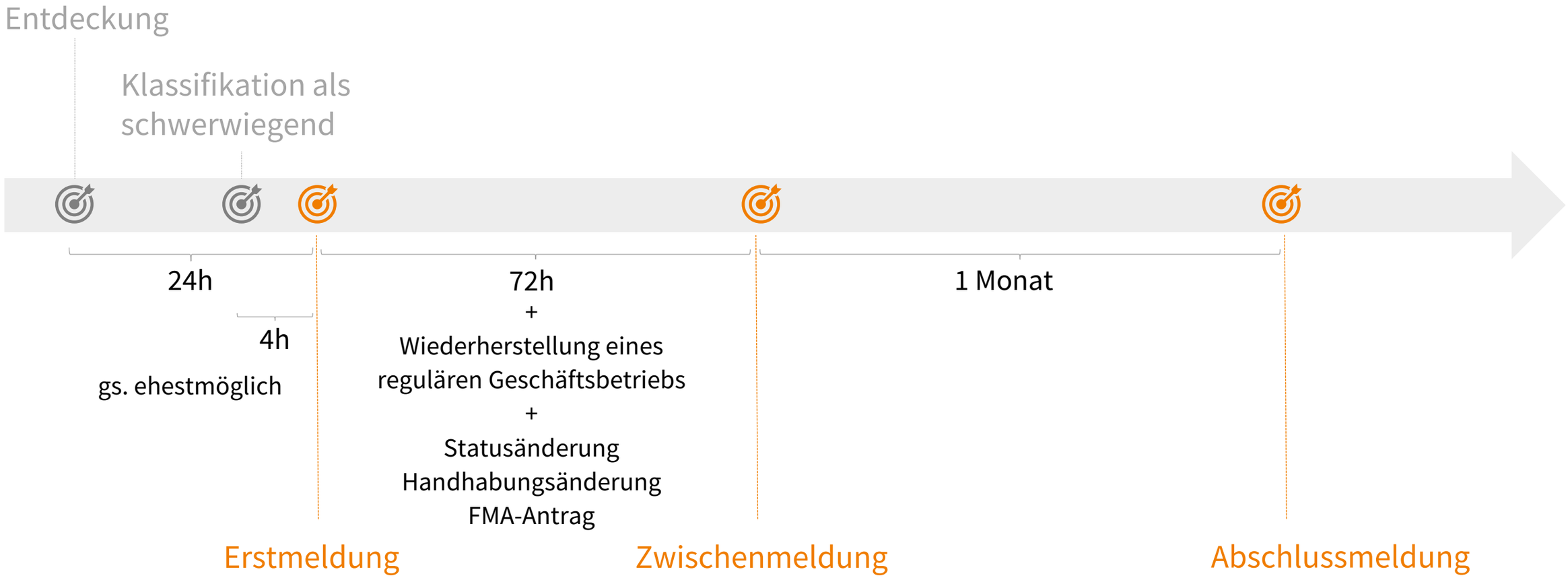
Kriterium DelVO (EU) 2024/1772	Schwellenwerte
Kunden, finanzielle Gegenparteien und Transaktionen	a) > 10 % aller Kunden, welche die betroffene Dienstleistung nutzen b) > 100.000 Kunden, welche die betroffene Dienstleistung nutzen c) > 30 % aller zentralen Gegenparteien, die Tätigkeiten im Zusammenhang mit der Bereitstellung der betroffenen Dienstleistung ausüben d) > 10% der üblichen durchschnittlichen Anzahl an Transaktionen, die das Finanzunternehmen im Zusammenhang mit der betroffenen Dienstleistung durchführt e) > 10% des täglichen Durchschnittswerts der Transaktionen, die das Finanzunternehmen im Zusammenhang mit der betroffenen Dienstleistung durchführt f) Betroffenheit von Kunden oder finanzielle Gegenparteien, die als relevant eingestuft wurden
Dauer und Ausfallzeiten	➢ Vorfall dauert mehr als 24 Stunden ➢ die Ausfallzeiten bei IKT-Diensten zur Unterstützung kritischer oder wichtiger Funktionen betragen mehr als zwei Stunden
Wirtschaftliche Auswirkungen	➢ die direkten und indirekten Bruttokosten und -verluste überschreiten **EUR 100 000** oder werden voraussichtlich **EUR 100 000** überschreiten

KRITERIEN (3)

Kriterium DelVO (EU) 2024/1772	Schwellenwerte
Geografische Ausbreitung	➢ Betroffenheit von mindestens zwei Mitgliedstaaten
Reputationsschäden	Grad der Bekanntheit des Vorfalls, beispielsweise durch: a) Medienaufmerksamkeit b) Wiederholte Beschwerden verschiedener Kunden oder finanzieller Gegenparteien c) Nichterfüllung der aufsichtlichen Anforderungen d) Kundenverlust, mit Auswirkungen auf das Geschäft
Wiederholte Vorfälle *Kein Kriterium ieS.*	➢ Sofern einzelne Vorfälle nicht als kritisch eingestuft werden, jedoch im Zeitraum der letzten **sechs Monate mindestens zwei Mal** aufgetreten sind, die **gleiche Grundursache** aufweisen und **zusammengenommen die Kriterien** für die Betrachtung als **schwerwiegender Vorfall erfüllen** ➢ Vorliegen muss monatlich bewertet werden ➢ Kleinstunternehmen sind ausgenommen

FRISTEN

Schwerwiegende IKT-bezogene Vorfälle



+ Wochenend- und Feiertagsbestimmung:
bis 12:00 Uhr des nächsten Werktages

➔ Gilt nicht für wesentliche Einrichtungen gem. NIS2-RL, also nicht für NIS2-Kreditinstitute, zentrale Gegenparteien und Betreiber von Handelsplätzen

MELDEWEG

Einbringung grundsätzlich über die FMA-Incoming-Plattform

➔ siehe FMA-Schreiben vom 17. Jänner 2025:
„DORA: Neue Anzeigen, Meldungen und ihre Einbringungsart auf der Incoming Plattform“

https://www.fma.gv.at/querschnittsthemen/dora/

(Rubrik FMA-Aktivitäten / FMA-Schreiben zu DORA: Anzeigen und Meldungen)

Im Falle von technischen Problemen mit der FMA-Incoming-Plattform wenden Sie sich bzgl. Versicherungsunternehmen, Pensionskassen und Betrieblicher Vorsorgekassen bitte an +43-1-24-959 DW 2103 oder 2107 bzw. bzgl. sonstiger Finanzunternehmen bitte an Ihren FMA-SPOC **zwecks alternativen Meldewegs**

Im Anschluss erfolgt die Meldung – soweit technisch möglich – über eine **sichere Datentransferapplikation**:

FTAPI

WEITERLEITUNGEN DER MELDUNGEN DURCH FMA

Die FMA leitet jede eingebrachte Meldung automatisch weiter an ….

- **ESAs**
  (sektorspezifisch)
- **EZB**
  (bei SI)
- **NIS-Behörde**
  (bei wesentlichen Einrichtungen)
- **OeNB**
  (soweit anwendbar)

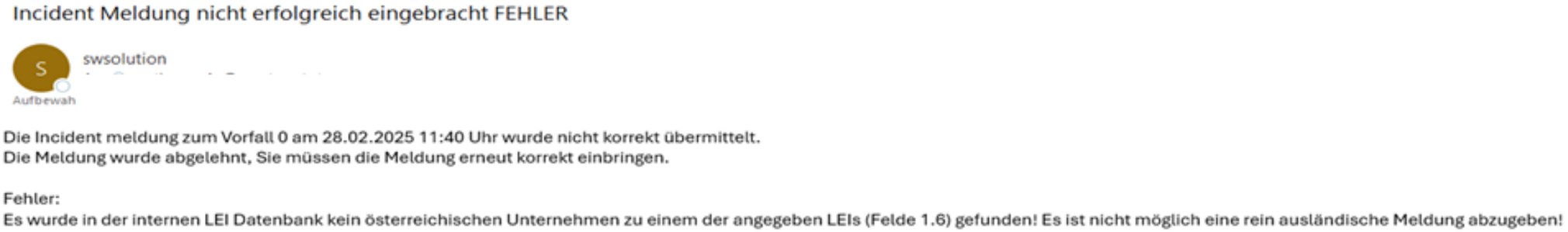
FMA-Hinweise zur Meldung & Klassifizierung

MELDEHINWEISE ZU SCHWERWIEGENDEN IKT-BEZOGENEN VORFÄLLEN (1)

- **E-Mail-Rückmeldungen zu den Einmeldungen**

  Fehlermeldungen:

  → <u>erneute Einmeldung!</u>



Incident Meldung nicht erfolgreich eingebracht FEHLER

S swsolution

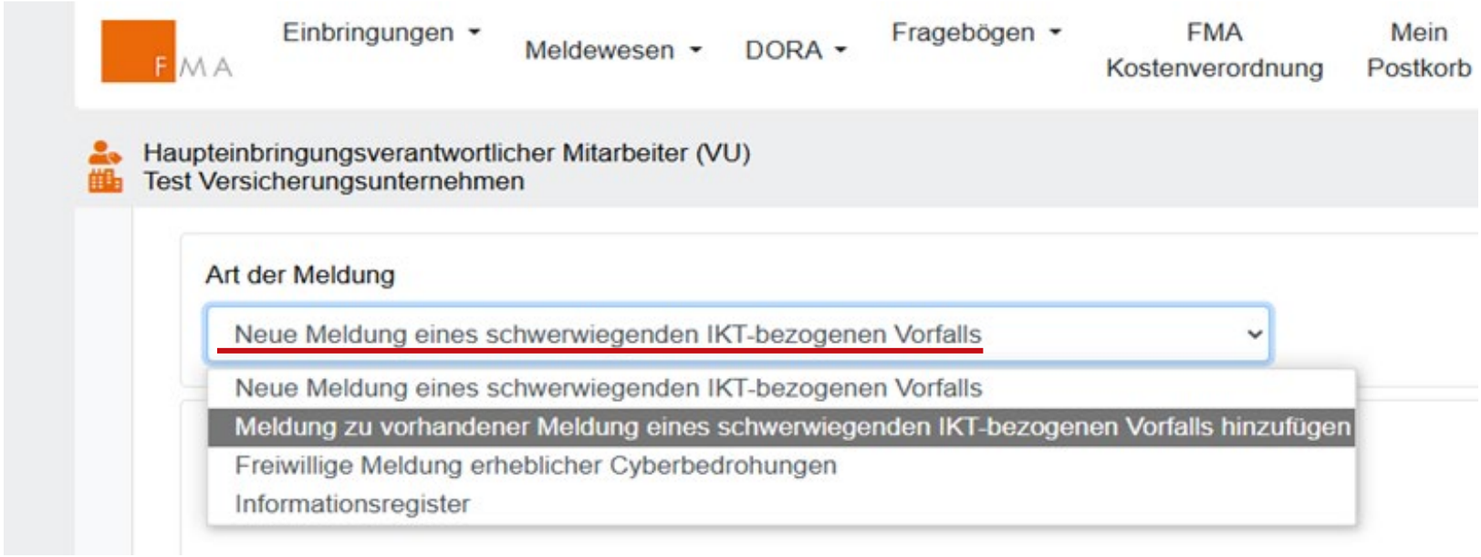
Aufbewah

Die Incident meldung zum Vorfall 0 am 28.02.2025 11:40 Uhr wurde nicht korrekt übermittelt.
Die Meldung wurde abgelehnt, Sie müssen die Meldung erneut korrekt einbringen.

Fehler:
Es wurde in der internen LEI Datenbank kein österreichischen Unternehmen zu einem der angegeben LEIs (Felde 1.6) gefunden! Es ist nicht möglich eine rein ausländische Meldung abzugeben!

MELDEHINWEISE ZU SCHWERWIEGENDEN IKT-BEZOGENEN VORFÄLLEN (2)

- **Meldungen zu einem bereits gemeldeten Vorfall hinzufügen**



Zwischenmeldungen, **Abschlussmeldung** oder **Reklassifizierungs-meldungen** zu einem bereits an die FMA gemeldeten Vorfall sind unter Auswahl des Feldes “Meldung zu vorhandener Meldung eines schwerwiegenden IKT-bezogenen Vorfalls hinzufügen” einzumelden. Dort ist die DORA-Incident ID der Erstmeldung auszuwählen.

MELDEHINWEISE ZU SCHWERWIEGENDEN IKT-BEZOGENEN VORFÄLLEN (3)

- **Initial notification – Feld 2.5**

2.5	2.6	2.7	2.8	2.9
Classification criteria that triggered the incident report	Materiality thresholds for the classification criterion 'Geographical spread'	Discovery of the major ICT-related incident	Indication whether the incident originates from a third party provider or another financial entity	Activation of business continuity plan, if activated
Critical services affected				

Die Beeinträchtigung kritischer Dienste ist jedenfalls anzugeben. Dies stellt gem. Art 8 Delegierte Verordnung (EU) 2024/1772 eine Grundvoraussetzung für die Klassifizierung als ‚schwerwiegend' dar.

Die EBA hat klargestellt, dass es sich bei Artikel 6 Delegierte Verordnung (EU) 2024/1772 um eine ODER-Bestimmung handelt (siehe Critical services (eine Oder-Bestimmung)).

MELDEHINWEISE ZU SCHWERWIEGENDEN IKT-BEZOGENEN VORFÄLLEN (4)

- **Aktualisierung der Klassifizierungskriterien in der Initial notification – Feld 2.5**

2.4	2.5	2.6
Description of the ICT-related incident	Classification criteria that triggered the incident report	Materiality thresholds for the classification criterion 'Geographical spread'
Beispieltext	Clients, financial counterparts and transactions affected	
	Duration and service downtime	
	Critical services affected	

Sollten im Zuge der Zwischenmeldung oder der Abschlussmeldung andere Klassifizierungskriterien erfüllt sein als in der Erstmeldung angegeben, so ist das Feld 2.5 der Erstmeldung ebenso anzupassen. Gemäß Artikel 1 Absatz 4 DelVO (EU) 2025/302 sind bereits übermittelte Informationen im Zuge der Zwischen- oder Abschlussmeldung zu aktualisieren.

MELDEHINWEISE ZU SCHWERWIEGENDEN IKT-BEZOGENEN VORFÄLLEN (5)

- **Richtige Angaben – „Clients, financial counterparts and transactions“**

3.4	3.5	3.6	3.7	3.8	3.9	3.10	3.11
Number of clients affected	Percentage of clients affected	Number of financial counterparts affected	Percentage of financial counterparts affected	Impact on relevant clients or financial counterparts	Number of affected transactions	Percentage of affected transactions	Value of affected transactions
2798	0,0	0	0,0	No	47	0,0	348000

Achtung bei Angaben zu Kriterium „Clients, financial counterparts and transactions“ in der Zwischenmeldung:

✓ **Number of clients affected**: 2798 ≠ **Percentage of clients affected**: 0%

✓ **Value of affected transactions**: in T EUR anzugeben

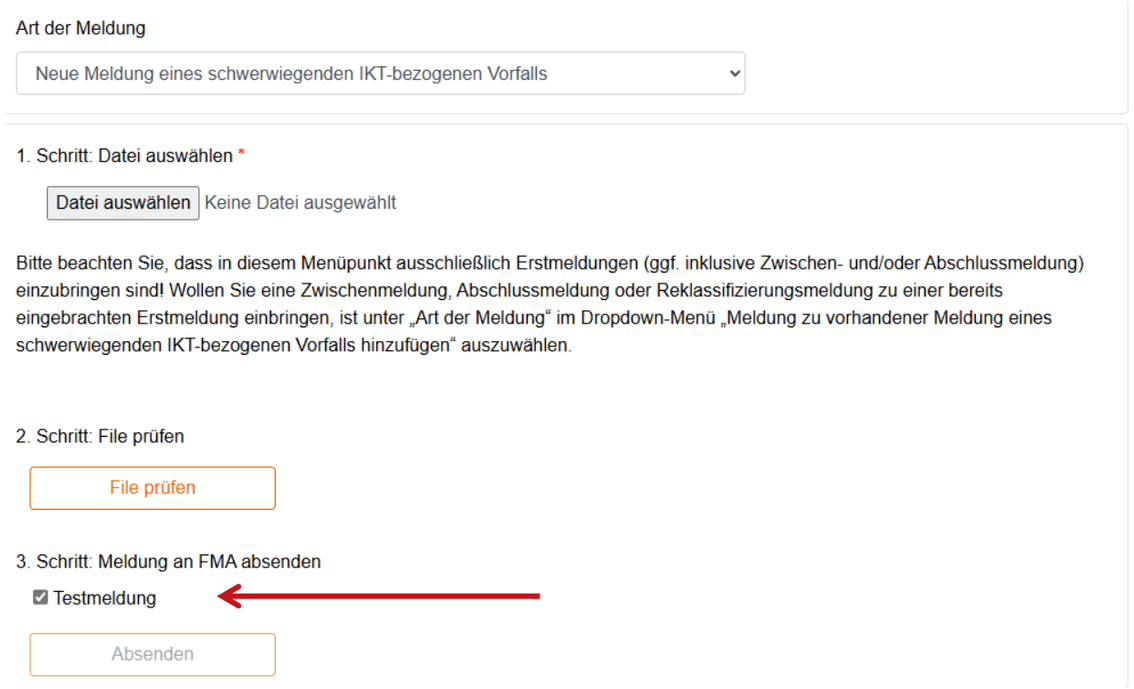
✓ **Number** und **Value of affected transactions**: gegebenenfalls mittels Schätzungen auf Basis verfügbarer Daten aus vergleichbaren Referenzzeiträumen zu befüllen

➔ Reportinganweisungen des Meldetemplates sowie die DelVO (EU) 2024/1772 (RTS zu Klassifizierungskriterien) beachten!

➔ siehe insbesondere auch DurchführungsVO (EU) 2025/302 (ITS zu Incidentmeldungen), hierin Anhang II: **Datenglossar und Anleitung für die Meldung schwerwiegender Sicherheitsvorfälle**

MELDEHINWEISE ZU SCHWERWIEGENDEN IKT-BEZOGENEN VORFÄLLEN (6)

- **Kästchen “Testmeldung”**



Das Häkchen bei „Testmeldung“ ist nur anzukreuzen, wenn Sie das Einbringen einer Meldung testen wollen.
Es erfolgt keine Verarbeitung seitens FMA!

MELDEHINWEISE ZU SCHWERWIEGENDEN IKT-BEZOGENEN VORFÄLLEN (7)

- **Technisch aggregierte Meldungen**
  Gemäß DelVO (EU) 2025/302 ist eine aggregierte (konsolidierte) Meldung bei signifikanten Kreditinstituten, Betreibern von Handelsplätzen und zentralen Gegenparteien nicht möglich (Art 7 Abs 2 DelVO (EU) 2025/302).

  Die FMA ermöglicht jedoch eine technisch aggregierte Meldung, wofür ein eigenes Template von der FMA zur Verfügung gestellt wird. Bitte kontaktieren Sie diesbezüglich Ihren FMA-SPOC.

- **Auslagerung der Meldeverpflichtung schwerwiegender IKT-bezogener Vorfälle**
  Sollten Sie die Meldeverpflichtung von schwerwiegenden IKT-bezogenen Vorfällen an einen Drittdienstleister ausgelagert haben, so ist dies der FMA als wesentliche Auslagerung gem. Art 28 Abs 3 letzter Satz DORA per Incoming Plattform anzuzeigen. Die Anzeige soll so bald wie möglich, jedoch nicht später als 30. September 2025 bei der FMA eingebracht werden.

  Signifikante Institute haben eine Auslagerungsanzeige gem. Art 28 Abs 3 DORA nicht bei der FMA, sondern bei der EZB einzubringen.

MELDEHINWEISE ZU SCHWERWIEGENDEN IKT-BEZOGENEN VORFÄLLEN (8)

- **Reklassifizierungsmeldung**

  Stellt sich nach Übermittlung der Erstmeldung heraus, dass die Schwellenwerte der Kriterien für eine Meldung nach Art. 19 DORA doch nicht vorliegen, so ist eine Reklassifizierungsmeldung bei der FMA einzubringen (eigener Punkt im Tabellenblatt „Type of submission“ im Excel-Template).

- **Einbringung Erst-, Zwischen- und Abschlussmeldung**

  Es ist möglich, Erst-, Zwischen- und Abschlussmeldung in einem einzubringen (sofern bereits alle Daten zum Vorfall vorliegen). Siehe Artikel 2 DelVO (EU) 2025/302.

  Sollten Sie ausschließlich eine Erstmeldung einbringen wollen, stellen Sie sicher, dass keine Felder in der Zwischen- und Abschlussmeldung befüllt sind.

- **Einbringung von mehr als einer Zwischenmeldung (Vorfall dauert mehr als 72 Stunden)**

  Die ESMA hat klargestellt, dass mehr als eine Zwischenmeldung zu einem schwerwiegenden IKT-bezogenen Vorfall einzubringen ist, wenn die reguläre Tätigkeit nicht innerhalb von 72 Stunden wieder aufgenommen werden konnte (siehe Timelimits intermediate report).

Informationsaustauschmöglichkeiten & Förderungsinitiative

RECHTLICHE MÖGLICHKEIT & ZIELE

- **DORA-Verordnung**

Artikel 45

Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen

(1) Finanzunternehmen können Informationen und Erkenntnisse über Cyberbedrohungen untereinander austauschen, einschließlich Indikatoren für Beeinträchtigungen, Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools, soweit dieser Austausch von Informationen und Erkenntnissen

a) darauf abzielt, die digitale operationale Resilienz von Finanzunternehmen zu stärken, insbesondere indem für Cyberbedrohungen sensibilisiert, die Verbreitung von Cyberbedrohungen eingeschränkt oder verhindert wird und die Verteidigungsfähigkeiten, Techniken zur Erkennung von Bedrohungen, Abmilderungsstrategien oder Phasen der Reaktion und Wiederherstellung unterstützt werden;

b) innerhalb vertrauenswürdiger Gemeinschaften von Finanzunternehmen erfolgt;

c) durch Vereinbarungen über den Austausch von Informationen umgesetzt wird, die den potenziell sensiblen Charakter der ausgetauschten Informationen schützen und Verhaltensregeln unterliegen, in deren Rahmen die Wahrung des Geschäftsgeheimnisses, der Schutz personenbezogener Daten im Einklang mit der Verordnung (EU) 2016/679 und Leitlinien für die Wettbewerbspolitik vollumfänglich befolgt werden.

(2) Für die Zwecke von Absatz 1 Buchstabe c werden in den Vereinbarungen über den Austausch von Informationen die Voraussetzungen für die Teilnahme und gegebenenfalls die Einzelheiten zur Einbindung staatlicher Behörden und der Eigenschaft, in der diese in die Vereinbarungen über den Austausch von Informationen eingebunden werden können, zur Einbindung von IKT-Drittdienstleistern sowie zu operativen Aspekten, einschließlich der Nutzung spezieller IT-Plattformen, festgelegt.

(3) Finanzunternehmen teilen zuständigen Behörden ihre Einbindung in die in Absatz 1 genannten Vereinbarungen über den Austausch von Informationen mit, sobald ihre Mitwirkung bestätigt wurde bzw. endet und diese Beendigung in Kraft ist.

- **Ziele**
  - FMA-Unterstützung der Nutzung der in Art. 45 DORA-VO vorgesehenen Möglichkeit
  - Einbeziehung auch ‚kleinerer' Finanzunternehmen
  - Schutz insb. der Vertraulichkeit der Informationen
  - Feeds aus verschiedenen, verlässlichen Quellen
  - Nutzung auch für Koordination und Kommunikation bei systemischen Cyberkrisen

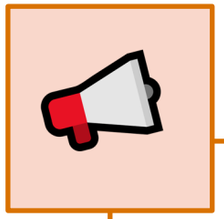
  ⇨ Stärkung Finanzmarktstabilität

- **Hinweis**

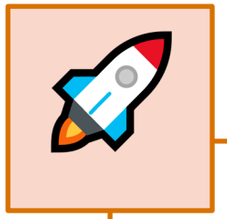
  Meldeerfordernis an FMA

OPTIONEN FÜR FINANZUNTERNEHMEN

- Zielgerichtete Teilnahme an vorhandenen Möglichkeiten



- Mitwirkung an neu entstehenden Angeboten: zB evtl CERT.at-Mailingliste



- Aktive Mitgestaltung der Finanzunternehmen & Weiterentwicklung, zB in Richtung Dashboard

Beitrag CERT.at

INFORMATIONSAUSTAUSCHMÖGLICHKEITEN (1)

NATIONALE FORMATE IN ÖSTERREICH

- **CERT.AT**
  - Nationales Computernotfallteam nach NISG
  - CERT.at ist damit auch das nationale CERT des Finanzsektors, da es in Österreich kein eigenes FinCERT gibt
  - Fachlicher Austausch über „discuss“-Mailingliste und Austrian Trust Circle
  - Mailingslisten zum Versand von Warnungen und Bedrohungen

- **AUSTRIAN TRUST CIRCLE (ATC)**
  - Zielgruppe: technische Entscheider, CISOs, IT/Cybersecurity-Verantwortliche – Invitation only
  - Ziel der Veranstalter: Teilnehmer sollen in ruhigen Zeiten voneinander lernen und bei Cyberangriffen in den anderen Organisationen jemanden kennen, zu dem sie rasch und unkompliziert Kontakt aufnehmen können
  - Kein Verein, sondern eine Veranstaltungsreihe
  - Aktives Teilen von Vorfällen und Erfahrungen ist Voraussetzung
  - Keine vertrieblichen Aktivitäten, keine Consultants oder „Dienstleister“, keine Regulatoren/Aufseher

INFORMATIONSAUSTAUSCHMÖGLICHKEITEN (2)

NATIONALE FORMATE IN ÖSTERREICH

- **CISO-ERFAHRUNGSAUSTAUSCH**
  - Lokale Gruppen für CISOs in den Bundesländern

INTERNATIONALE FORMATE MIT ÖSTERREICHISCHER BETEILIGUNG

- **ISAC – INFORMATION SHARING AND ANALYSIS CENTER**
  - FI-ISAC
    - Non-profit Organisation der ENISA
    - Regelmäßige Treffen zum Erfahrungsaustausch
    - Teilnehmer CERTs, Europol, EZB, Kommission, etc.
  - FS-ISAC
    - Non-profit Organisation mit US-Schwerpunkt
    - Ca. 5000 teilnehmende Organisationen in 75 Ländern
    - Teilnehmer: u.a. österr. Finanzinstitute, keine aktive Teilnahme durch CERT.at

INFORMATIONSAUSTAUSCHMÖGLICHKEITEN (3)

FÖRDERUNG DES INFORMATIONSAUSTAUSCHES

- **RAHMENBEDINGUNGEN**
  - Einbindung aller Organisationen, die DORA umsetzen müssen
  - Freier vs. moderierter Informationsaustausch - Verhaltensregeln
  - Vertraulichkeit
- **UMSETZUNGSOPTIONEN**
  - **CERT.at-Mailingliste**: Nachrichten an die Liste werden an alle Teilnehmer:innen weitergeleitet
    - Regelmäßiger Versand branchenrelevanter Informationen z.B. durch CERT.at, BMI, Wachtlist Internet, etc.
    - Freie Austauschmöglichkeit oder Nachrichtenverteilung erst nach Freigabe durch einen Moderator
    - Teilnehmer sind nur die der FMA genannten Kontakte – oder: Selbstverwaltung der Liste durch die Finanzinstitute
  - **CERT.at-Mattermost-Chat**: Chat-Kanäle für alle Institute gemeinsam und direkte Kontaktaufnahme möglich
    - Am sinnvollsten bei aktiver Beteiligung am Informationsaustausch

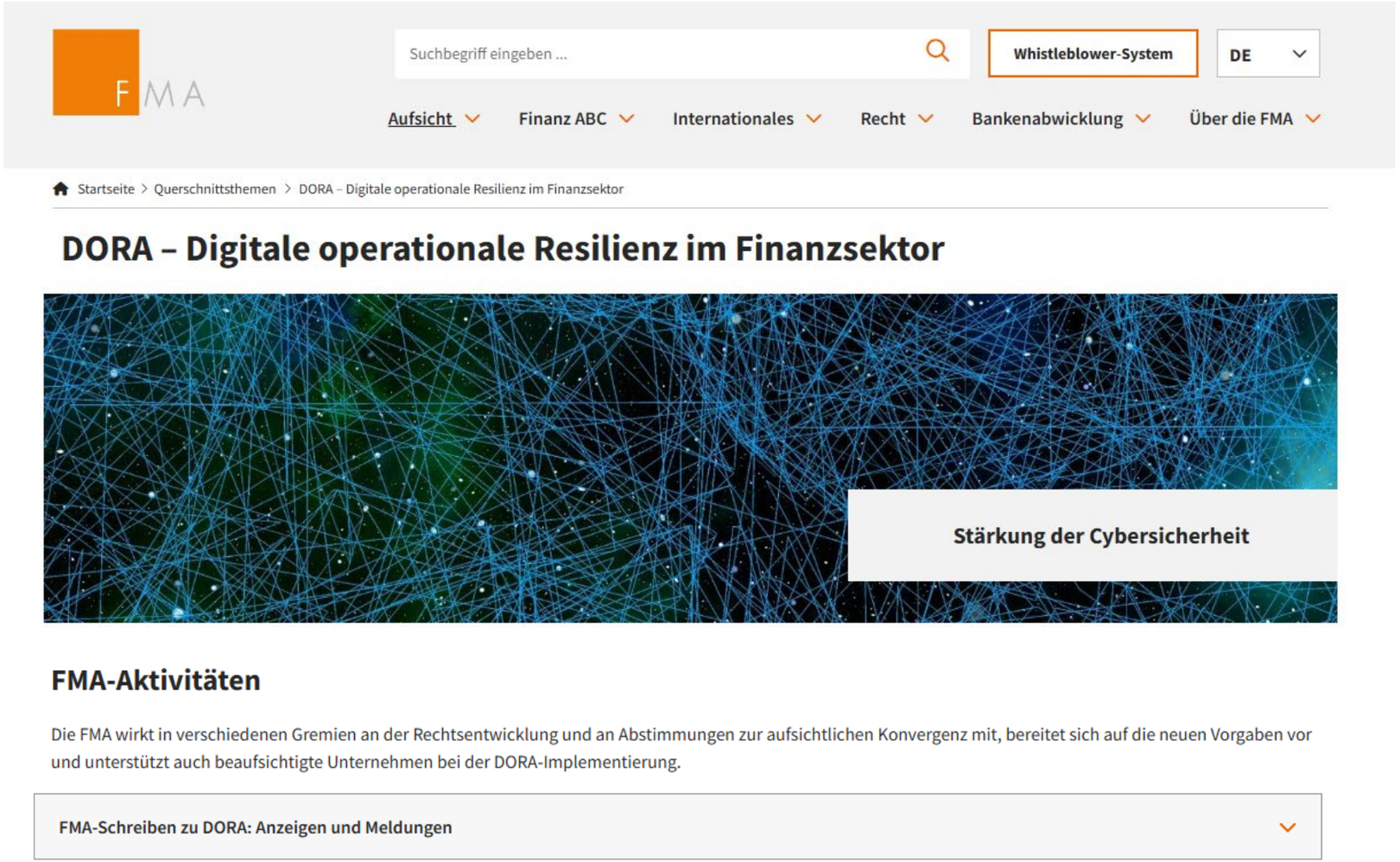
Beitrag BMI

Beitrag WKO

Beitrag Watchlist Internet

Ausblick

FMA-DORA-WEBSITE



⇦ Updates folgen

Sie können Fragen an dora@fma.gv.at richten.

FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz

OESTERREICHISCHE NATIONALBANK

EUROSYSTEM