ÖSTERREICHISCHE FMA·FINANZMARKTAUFSICHT

OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

FMA-OENB-DORA-DIALOG: DORA-INFORMATIONSREGISTER & AKTUELLE HINWEISE
23.10.2025

AGENDA

Begrüßung
Michael Hysek

Teil 1: DORA-Informationsregister

- FMA-Erfahrungen zur Übermittlung 2025
  Michael Mandelburger / Karl Machan / Alexander Kiennast
- Ausblick Informationsregister 2026
  Michael Mandelburger / Karl Machan / Alexander Kiennast

Teil 2: Aktuelle Hinweise

- Informationen zu IKT-bezogenen Vorfällen
  Alexander Mitter
- Update Generic Threat Landscape
  Georg Eilnberger
- Status Überwachungsrahmen
  Michael Mandelburger

Ausblick

MILESTONES & NÄCHSTE SCHRITTE

DORA-Anwendbarkeit ab 17.1.2025

Erste Informationsregister-Übermittlung an FMA im April 2025, danach jährlich bis zur jeweils vorgegebenen Frist

Designation kritischer IKT-Drittdienstleister & Start des neuen Überwachungsrahmens bis Ende 2025

Weitere Themen,
wie z.B. Meldung schwerwiegender IKT-bezogener Vorfälle

- FMA-OeNB-Erfahrungen
- FMA-OeNB-Hinweise
- Statistiken
- Ausblick

FMA-Erfahrungen zur Übermittlung 2025

EINMELDEPROZESS 2025

Erstellung eines XLSX-Templates

Kommunikation an Finanzunterneh-men über breite Informations-weitergabe (WKÖ), Videokonferenzen and direkte Aufforderung

Einmeldezeitraum vom 3.4. bis 14.4. mit direkter Rückmeldung

Überleitung an ESAs (EBA) mit weiteren Checks

Mehrstufiger Prozess

FMA beschloss, die Informationsregister gemäß DORA in zwei Hauptschritten zu sammeln. Zuerst musste die bereitgestellte XLSX-Vorlage auf konsolidierter Basis auf die ‚eingehende Plattform' der FMA hochgeladen werden. Durch das Hochladen startete die eingehende Plattform sofort Qualitätsprüfungen. Nachdem die gesammelten Dateien die internen Prüfungen bestanden hatten, wurden alle empfangenen Informationsregister auf einmal an die EBA übertragen. Neue Warnungen oder Ablehnungen wurden innerhalb der FMA analysiert und entweder direkt von der FMA korrigiert oder es wurde eine korrigierte Hochladung durch das Finanzinstitut angefordert.

VOR- UND NACHTEILE

Der mehrstufige Prozess hatte folgende Vorteile:

- „Die kurze Frist für die erste Sammlung (Mitte April) gab der FMA und den Finanzinstituten ausreichend Zeit für Analysen und Korrekturanfragen.
- Interne Prüfungen erleichterten die Kommunikation mit den Finanzinstituten durch die Beschreibung und die Art der Kommunikation.
- Probleme mit der EBA konnten von den Finanzinstituten ferngehalten werden.
- Häufige Warnungen/Ablehnungen konnten von der FMA effizient korrigiert werden.“

Der mehrstufige Prozess hatte folgende Nachteile:

- Der erste Upload zur EBA konnte erst starten, nachdem alle Informationsregister gesammelt worden waren.
- Neue Warnungen oder Ablehnungen traten auf, nachdem die Finanzinstitute die Mitteilung über einen erfolgreichen Upload erhalten hatten.

WIE NUTZT DIE FMA DIE DATEN DES INFORMATIONSREGISTERS?

Input für Aufsichtsmaßnahmen

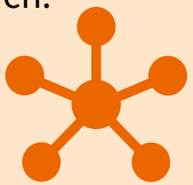
- Die Daten sind nützlich bei der Vorbereitung bzw. Auswahl von Prüfungen:
  - Vor-Ort-Prüfungen
  - Einsichtnahmen, Managementgespräche
  - Thematische Arbeiten
  - Trendanalysen

Identifizierung der Auswirkungen eines Vorfalls

- Viele gemeldete IKT-Vorfälle beziehen sich auf Dienstleister.
- Weitere potenziell betroffene Finanzunternehmen können identifiziert und kontaktiert werden.
- Beispielhaft wurde dies bei dem IKT-Vorfall von Colt im Sommer 2025 angewendet.

(Geplante) Analysen

- Die Informationsregister ermöglichen die Identifizierung von wichtigen IKT-Drittdienstleistern auf nationaler Ebene.
- Integration des IKT-Konzentrationsrisiko in das Risikoscoring von Beaufsichtigten möglich.
- Dienstleistungs-ketten



WIE NUTZEN DIE EUROPÄISCHEN AUFSICHTSBEHÖRDEN (ESA) DIE DATEN DES INFORMATIONSREGISTERS?

Kritische IKT-Drittdienstleister (CTPP)

- Bewertungsgrundlagen unter anderem:
  - Anzahl
  - Komplexität
  - Substituierbarkeit
  - Geographische Verteilung
  - Art der Dienst-leistung

(Vorbereitung von) Aufsichtsmaßnahmen bei CTPP

- Vor-Ort-Prüfungen bei CTPP
- Sonstige Aufsichtsmaßnahmen
- Thematische Arbeiten
- Konzentrationsrisiken

(Geplante / mögliche) Analysen

- Konzentrationsrisiken
- Regionale Unterschiede der Inanspruchnahme von IKT-Dienstleistungen
- Zusammenhänge
- Dienstleistungsketten

INFORMATIONSREGISTER: ERSTMALIGE ERSTELLUNG & VERWENDUNG 2025

Datensammlung & Übermittlung an ESAs

- April/Mai 2025 erfolgreich abgeschlossen
- Feedback ESAs: sehr gute Qualität der AT-Einmeldungen

Nutzung in der Aufsicht

- Datenbasis für umfassende Analysen
- Konzentrationsrisiken erkennbar (zentrale IKT-Dienstleister)
- Grundlage für die Planung von Aufsichtsmaßnahmen

Mehrwert für Beaufsichtigte & Aufsicht

- **Das Informationsregister liefert einen umfassenden Überblick über die IKT-Drittdienstleisterlandschaft in Österreich.**
- **Die daraus gewonnenen Daten ermöglichen eine gezieltere, effizientere und schnellere Aufsicht.**

Für Beaufsichtigte bedeutet das:

- Risiken und Konzentrationen bei Dienstleistern werden frühzeitig erkannt.
- Prüfungen und Aufsichtsmaßnahmen können besser vorbereitet und nachvollziehbar gestaltet werden.
- Die eigene Position im Markt und gegenüber Dienstleistern wird transparenter.
- Insgesamt profitieren Banken von einer erhöhten Sicherheit und einer datenbasierten, nachvollziehbaren Aufsicht.

LESSONS LEARNED

- **Leere Tabellenblätter**

  Verpflichtend auszufüllende Tabellenblätter:

Nummer	Name
B_01.01	Unternehmen, das das Informationsregister führt
B_01.02	Liste der zum Konsolidierungskreis gehörenden Unternehmen
B_02.01	Vertragliche Vereinbarungen – Allgemeine Informationen
B_02.02	Vertragliche Vereinbarungen – Spezifische Informationen
B_03.01	Unternehmen, die die vertraglichen Vereinbarungen für den Erhalt der IKT-Dienstleistung(en) im Namen der Finanzunternehmen, die die IKT-Dienstleistung(en) in Anspruch nehmen, unterzeichnen
B_03.02	IKT-Drittdienstleister, die die vertraglichen Vereinbarungen für die Erbringung der IKT-Dienstleistung(en) unterzeichnen
B_04.01	Finanzunternehmen, die IKT-Dienstleistungen in Anspruch nehmen
B_05.01	IKT-Drittdienstleister
B_05.02	IKT-Dienstleistungsketten
B_06.01	Angabe der Funktionen
B_07.01	Bewertungen der IKT-Dienstleistungen

FEHLERMELDUNGEN

- **Fehlende bzw. nicht korrekte Verbindung der Tabellen**

  Primarykeys u. Foreignkeys:

B_01.01 - Unternehmen, das das Informationsregister führt			
B_01.01.0010	LEI des Finanzunternehmens, das das Informationsregister führt	Primary Key	Doppelte Werte nicht erlaubt
B_01.02 - Liste der zum Konsolidierungskreis gehörenden Unternehmen			
B_01.02.0010	LEI des Finanzunternehmens	Primary Key	Doppelte Werte nicht erlaubt
B_01.03 - Liste der Zweigniederlassungen			
B_01.03.0010	Identifikationscode der Zweigniederlassung	Primary Key	Doppelte Werte nicht erlaubt
B_01.03.0020	LEI des Hauptsitzes des Finanzunternehmens der Zweigniederlassung	Foreign-Key	Wert dieses Feldes muss in B_01.02.0010 vorhanden sein
B_02.01 - Vertragliche Vereinbarungen – Allgemeine Informationen			
B_02.01.0010	Kennnummer der vertraglichen Vereinbarung	Primary Key	Doppelte Werte nicht erlaubt
B_02.01.0030	Kennnummer der übergeordneten vertraglichen Vereinbarung	Foreign-Key	Wert dieses Feldes muss in B_02.01.0010 vorhanden sein
B_02.02 - Vertragliche Vereinbarungen – Spezifische Informationen			
B_02.02.0010 & B_02.02.0020 & B_02.02.0030 & B_02.02.0050 & B_02.02.0060	Kennnummer der vertraglichen Vereinbarung & LEI des Finanzunternehmens, das die IKT-Dienstleistung(en) in Anspruch nimmt & Identifikationscode des IKT-Drittdienstleisters & Funktionskennung & Art der IKT-Dienstleistungen	Primary Key	Doppelte Werte nicht erlaubt
B_02.02.0010 & B_02.02.0030	Kennnummer der vertraglichen Vereinbarung & Identifikationscode des IKT-Drittdienstleisters	Foreign-Key	Wert muss in den Feldern B_03.02.0010 & B_03.02.0020 vorhanden sein
B_02.02.0020 & B_02.02.0050	LEI des Finanzunter-nehmens, das die IKT-Dienstleistung(en) in Anspruch nimmt & Funktionskennung	Foreign-Key	Wert muss in den Feldern B_06.01.0010 & B_06.01.0040 vorhanden sein

FEHLERMELDUNGEN

- **Fehlende bzw. nicht korrekte Verbindung der Tabellen**

Primarykeys u. Foreignkeys:

B_02.03 - Liste der gruppeninternen vertraglichen Vereinbarungen			
B_02.03.0010 & B_02.03.0020	Kennnummer der vertraglichen Vereinbarung & Vertragliche Vereinbarung im Zusammenhang mit der in RT.02.03.0010 genannten vertraglichen Vereinbarung	Primary Key	Doppelte Werte nicht erlaubt
B_02.03.0010	Kennnummer der vertraglichen Vereinbarung	Foreign-Key	Wert muss im Feld B_02.01.0010 vorhanden sein
B_02.03.0020	Vertragliche Vereinbarung im Zusammenhang mit der in RT.02.03.0010 genannten vertraglichen Vereinbarung	Foreign-Key	Wert muss im Feld B_01.02.0010 vorhanden sein
B_03.01 - Unternehmen, die die vertraglichenVereinbarungen für den Erhalt der IKT-Dienstleistung(en) im Namen der Finanzunternehmen, die die IKT-Dienstleistung(en) in Anspruch nehmen, unterzeichnen			
B_03.01.0010 & B_03.01.0020	Kennnummer der vertraglichen Vereinbarung & LEI des Unternehmens, das die vertragliche Vereinbarung unterzeichnet	Primary Key	Doppelte Werte nicht erlaubt
B_03.01.0010	Kennnummer der vertraglichen Vereinbarung	Foreign-Key	Wert muss im Feld B_02.01.0010 vorhanden sein
B_03.01.0020	LEI des Unternehmens, das die vertragliche Vereinbarung unterzeichnet	Foreign-Key	Wert muss im Feld B_01.02.0010 vorhanden sein
B_03.02 - IKT-Drittdienstleister, die die vertraglichen Vereinbarungenfür die Erbringung der IKT-Dienstleistung(en) unterzeichnen			
B_03.02.0010 & B_03.02.0020	Kennnummer der vertraglichen Vereinbarung & Identifikationscode des IKT-Drittdienstleisters	Primary Key	Doppelte Werte nicht erlaubt
B_03.02.0010	Kennnummer der vertraglichen Vereinbarung	Foreign-Key	Wert muss im Feld B_02.01.0010 vorhanden sein
B_03.02.0020	Identifikationscode des IKT-Drittdienstleisters	Foreign-Key	Wert muss im Feld B_05.01.0010 vorhanden sein
B_03.03 - Finanzunternehmen, die die vertraglichen Vereinbarungen über die Erbringung der IKT-Dienstleistung(en) für andere Finanzunternehmen im Konsolidierungskreis unterzeichnen			
B_03.03.0010 & B_03.03.0020	Kennnummer der vertraglichen Vereinbarung & LEI des Finanzunternehmens, das IKT-Dienstleistungen erbringt	Primary Key	Doppelte Werte nicht erlaubt
B_03.03.0010	Kennnummer der vertraglichen Vereinbarung	Foreign-Key	Wert muss im Feld B_02.01.0010 vorhanden sein
B_03.03.0020	LEI des Finanzunternehmens, das IKT-Dienstleistungen erbringt	Foreign-Key	Wert muss im Feld B_01.02.0010 vorhanden sein

FEHLERMELDUNGEN

- **Fehlende bzw. nicht korrekte Verbindung der Tabellen**

Primarykeys u. Foreignkeys:

B_04.01 - Finanzunternehmen, die IKT-Dienstleistungen in Anspruch nehmen			
B_04.01.0010 & B_04.01.0020 & B_04.01.0040	Kennnummer der vertraglichen Vereinbarung & LEI des Finanzunternehmens, das die IKT-Dienstleistung(en) in Anspruch nimmt & Identifikationscode der Zweigniederlassung	Primary Key	Doppelte Werte nicht erlaubt
B_04.01.0010	Kennnummer der vertraglichen Vereinbarung	Foreign-Key	Wert muss im Feld B_02.01.0010 vorhanden sein
B_04.01.0020	LEI des Finanzunternehmens, das die IKT-Dienstleistung(en) in Anspruch nimmt	Foreign-Key	Wert muss im Feld B_01.02.0010 vorhanden sein
B_05.01 - IKT-Drittdienstleister			
B_05.01.0010	Identifikationscode des IKT-Drittdienstleisters	Primary Key	Doppelte Werte nicht erlaubt
B_05.01.0110	Identifikationscode des obersten Mutterunternehmens des IKT-Drittdienstleisters	Foreign-Key	Wert muss im Feld B_05.01.0010 vorhanden sein
B_05.02 - IKT-Dienstleistungsketten			
B_05.02.0010 & B_05.02.0020 & B_05.02.0030 & B_05.02.0050 & B_05.02.0060	Kennnummer der vertraglichen Vereinbarung & Art der IKT-Dienstleistungen & Identifikationscode des IKT-Drittdienstleisters & Rang & Identifikationscode des Empfängers von im Unterauftrag vergebenen IKT-Dienstleistungen &	Primary Key	Doppelte Werte nicht erlaubt
B_05.02.0010	Kennnummer der vertraglichen Vereinbarung	Foreign-Key	Wert muss im Feld B_02.01.0010 vorhanden sein
B_05.02.0030	Identifikationscode des IKT-Drittdienstleisters	Foreign-Key	Wert muss im Feld B_05.01.0010 vorhanden sein
B_05.02.0060	Identifikationscode des Empfängers von im Unterauftrag vergebenen IKT-Dienstleistungen	Foreign-Key	Wert muss im Feld B_05.01.0010 vorhanden sein

FEHLERMELDUNGEN

- **Fehlende bzw. nicht korrekte Verbindung der Tabellen**

  Primarykeys u. Foreignkeys:

B_06.01 - Angabe der Funktionen			
B_06.01.0010 & B_06.01.0040	Funktionskennung & LEI des Finanzunternehmens	Primary Key	Doppelte Werte nicht erlaubt
B_06.01.0040	LEI des Finanzunternehmens	Foreign-Key	Wert muss im Feld B_02.01.0010 vorhanden sein
B_07.01 - Bewertungen der IKT-Dienstleistungen			
B_07.01.0010 & B_07.01.0020 & B_07.01.0040	Kennnummer der vertraglichen Vereinbarung & Identifikationscode des IKT-Drittdienstleisters & Art der IKT-Dienstleistungen	Primary Key	Doppelte Werte nicht erlaubt
B_07.01.0010	Kennnummer der vertraglichen Vereinbarung	Foreign-Key	Wert muss im Feld B_02.01.0010 vorhanden sein
B_07.01.0020	Identifikationscode des IKT-Drittdienstleisters	Foreign-Key	Wert muss im Feld B_05.01.0010 vorhanden sein

  Primarykeys u. Foreignkeys stimmen nicht überein:

  Werte beinhalten Tabulator, Leerzeichen od. andere Sonderzeichen -> Wahrscheinlich meist Kopierfehler

FEHLERMELDUNGEN

- **Pflichtfelder nicht ausgefüllt**

  Eine Auflistung findet sich:

  Data Model for DORA RoI.pdf

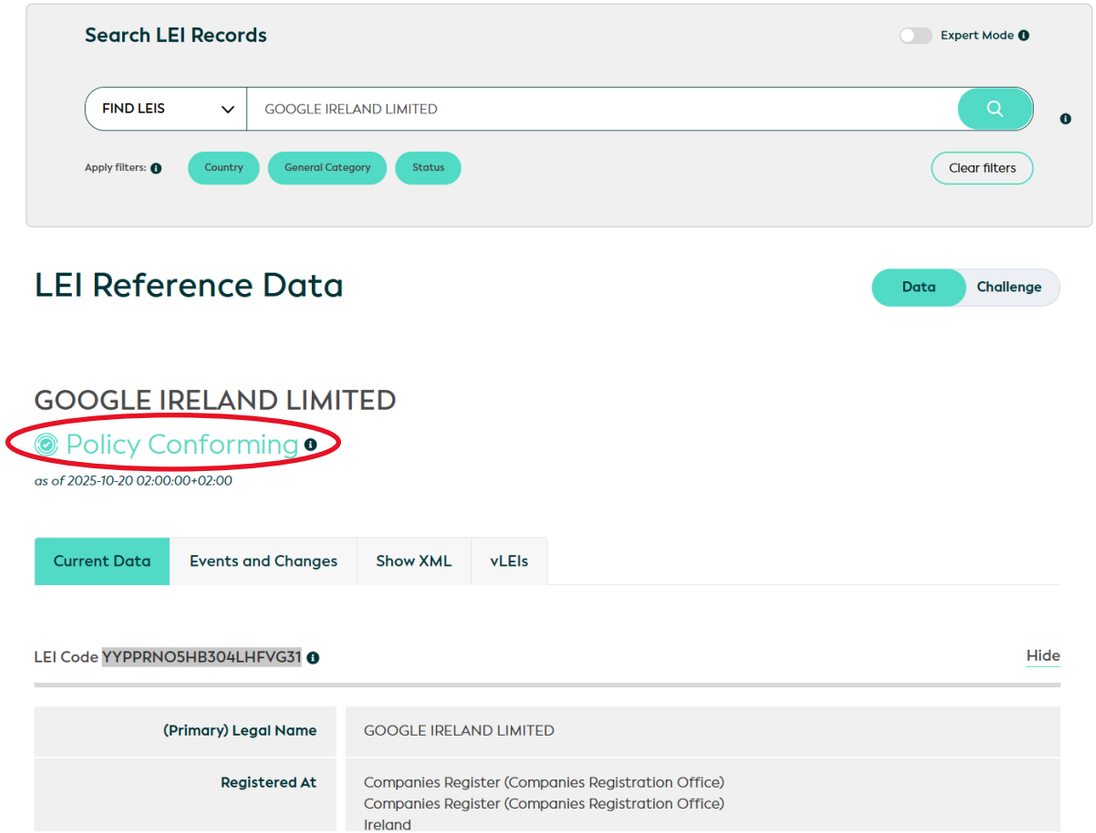
Table	Column	Type	Length	PrimaryKey	ForeignKey	Nullable
B.01.01 — Financial entity maintaining the register of information	**0010 - LEI of the entity maintaining the register of information**	char	20	Yes	No	No
	0020 - Name of the entity	varchar	255	No	No	No
	0030 - Country of the entity	char	2	No	No	No
	0040 - Type of entity	varchar	255	No	No	No
	0050 - Competent Authority	varchar	255	No	No	No
	0060 - Date of the reporting	date	0	No	No	No
B.01.02 — List of financial entities within the scope of the register of information	**0010 - LEI of the entity**	char	20	Yes	No	No
	0020 - Name of the entity	varchar	255	No	No	No
	0030 - Country of the entity	char	2	No	No	No
	0040 - Type of entity	varchar	255	No	No	No
	0050 - Hierarchy of the entity within the group (where applicable)	varchar	255	No	No	No
	0060 - LEI of the direct parent undertaking of the financial entity	char	20	No	Yes	Yes
	0070 - Date of last update	date	0	No	No	No
	0080 - Date of integration in the Register of information	date	0	No	No	No
	0090 - Date of deletion in the Register of information	date	0	No	No	No
	0100 - Currency	char	3	No	No	Yes
	0110 - Value of total assets - of the financial entity	money	0	No	No	Yes

FEHLERMELDUNGEN

- **Ungültige LEI**

  Global Legal Entity Identifier Foundation (GLEIF):

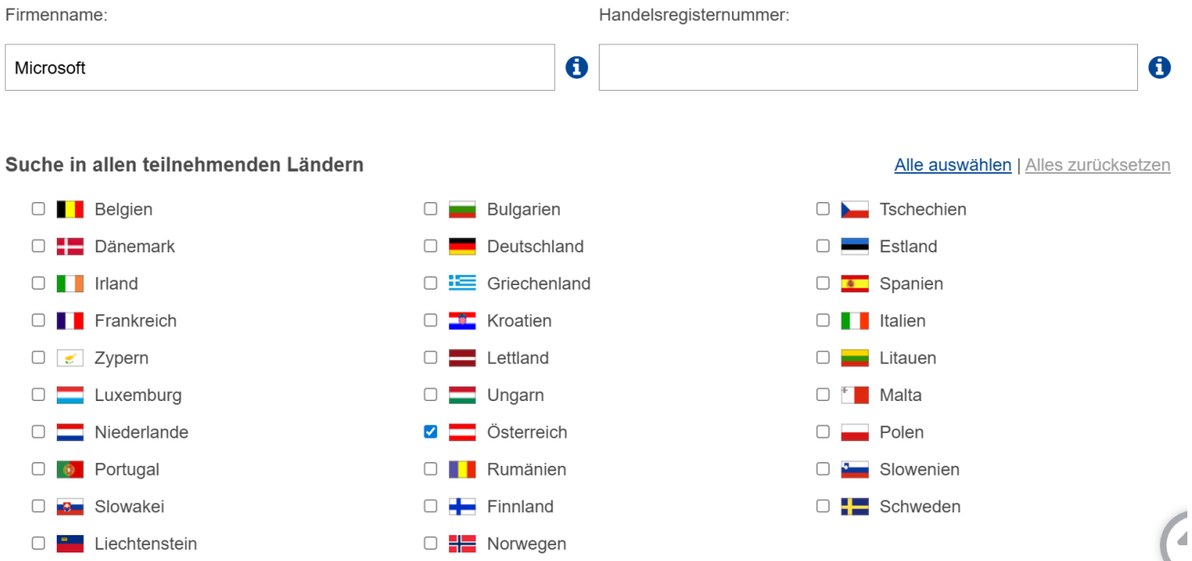
  LEI Search



FEHLERMELDUNGEN

- **Ungültige EuID**

Europäischen Justizportal:



FEHLERMELDUNGEN

- **Weitere häufige Fehler**

Tabelle B_01.02:

B_01.02 - Liste der zum Konsolidierungskreis gehörenden Unternehmen			
B_01.02.0010	LEI des Finanzunternehmens	Primary Key	Doppelte Werte nicht erlaubt
B_01.02.0060	LEI des direkten Mutterunternehmens des Finanzunternehmens	Foreign-Key	Wert dieses Feldes muss in B_01.02.0010 vorhanden sein

Sollte es kein direktes Mutterunternehmen geben, so ist hier die eigene LEI anzugeben

Tabelle B_05.01:

B_05.01 - IKT-Drittdienstleister			
B_05.01.0010	Identifikationscode des IKT-Drittdienstleisters	Primary Key	Doppelte Werte nicht erlaubt
B_05.01.0110	Identifikationscode des obersten Mutterunternehmens des IKT-Drittdienstleisters	Foreign-Key	Wert muss im Feld B_05.01.0010 vorhanden sein

Sollte es kein oberstes Mutterunternehmen geben, so ist hier die eigene LEI des IKT-Drittdienstleisters (B_05.01.0010) anzugeben

FEHLERMELDUNGEN

- **Weitere häufige Fehler**

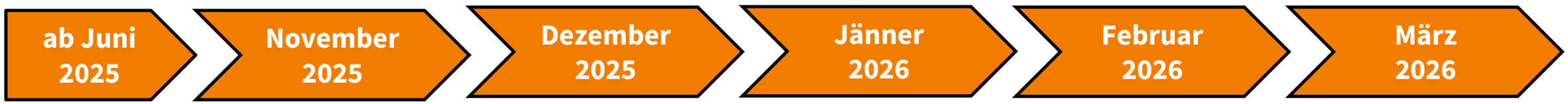
Tabelle B_05.02:

B_05.02 - IKT-Dienstleistungsketten			
B_05.02.0010 & B_05.02.0020 & B_05.02.0030 & B_05.02.0050 & B_05.02.0060	Kennnummer der vertraglichen Vereinbarung & Art der IKT-Dienstleistungen & Identifikationscode des IKT-Drittdienstleisters & Rang & Identifikationscode des Empfängers von im Unterauftrag vergebenen IKT-Dienstleistungen &	Primary Key	Doppelte Werte nicht erlaubt
B_05.02.0010	Kennnummer der vertraglichen Vereinbarung	Foreign-Key	Wert muss im Feld B_02.01.0010 vorhanden sein
B_05.02.0030	Identifikationscode des IKT-Drittdienstleisters	Foreign-Key	Wert muss im Feld B_05.01.0010 vorhanden sein
B_05.02.0060	Identifikationscode des Empfängers von im Unterauftrag vergebenen IKT-Dienstleistungen	Foreign-Key	Wert muss im Feld B_05.01.0010 vorhanden sein

Sollte der IKT-Dienstleister Rang 1 einnehmen, so ist hier die eigene LEI des IKT-Drittdienstleisters (B_05.02.0030) anzugeben

Ausblick Informationsregister 2026

TIMELINE INFORMATIONSREGISTERMELDUNG 2026



ESA-seitige Anpassungen des RoI-Formates werden bekannt gegeben

Start der Abgabe der Informationsregister an die FMA
Exaktes Datum: TBA

Ggf. Nachfragen der FMA zur Meldung
Weiterleitung an ESAs durch FMA: 31.03.2026

Erweiterte Checkregeln bei RoI-Abgabe umgesetzt

→ Testmöglichkeit vorhanden

Cutoff-Date für RoI-Meldung 2026:

<u>31.12.2025</u>

Deadline der Abgabe der Informationsregister an die FMA
Exaktes Datum: wird noch bekanntgegeben

Der Timeline zugrundeliegende ESA-Decision

TIMELINE INFORMATIONSREGISTERMELDUNG 2026

Timeline für Abgabe 2026, abhängig von ESA-Anpassungen des Abgabeformates:

- Sollen im November bekanntgegeben werden, dann Implementierung durch FMA.
- Cutoff-Date ist der 31.12.2025, Abgabestart für Jänner 2026, Deadline für Februar 2026 erwartet.
- Die Anpassungen sollen eher gering sein.

FMA zielt auf möglichst hohe Kompatibilität mit Abgabe 2025 ab:

- Bis auf Korrektur einzelner Typos keine nicht-ESA Änderungen am Template geplant.
- Starke Präferenz für Stabilität des Formates und der Check-Regeln an ESAs kommuniziert.

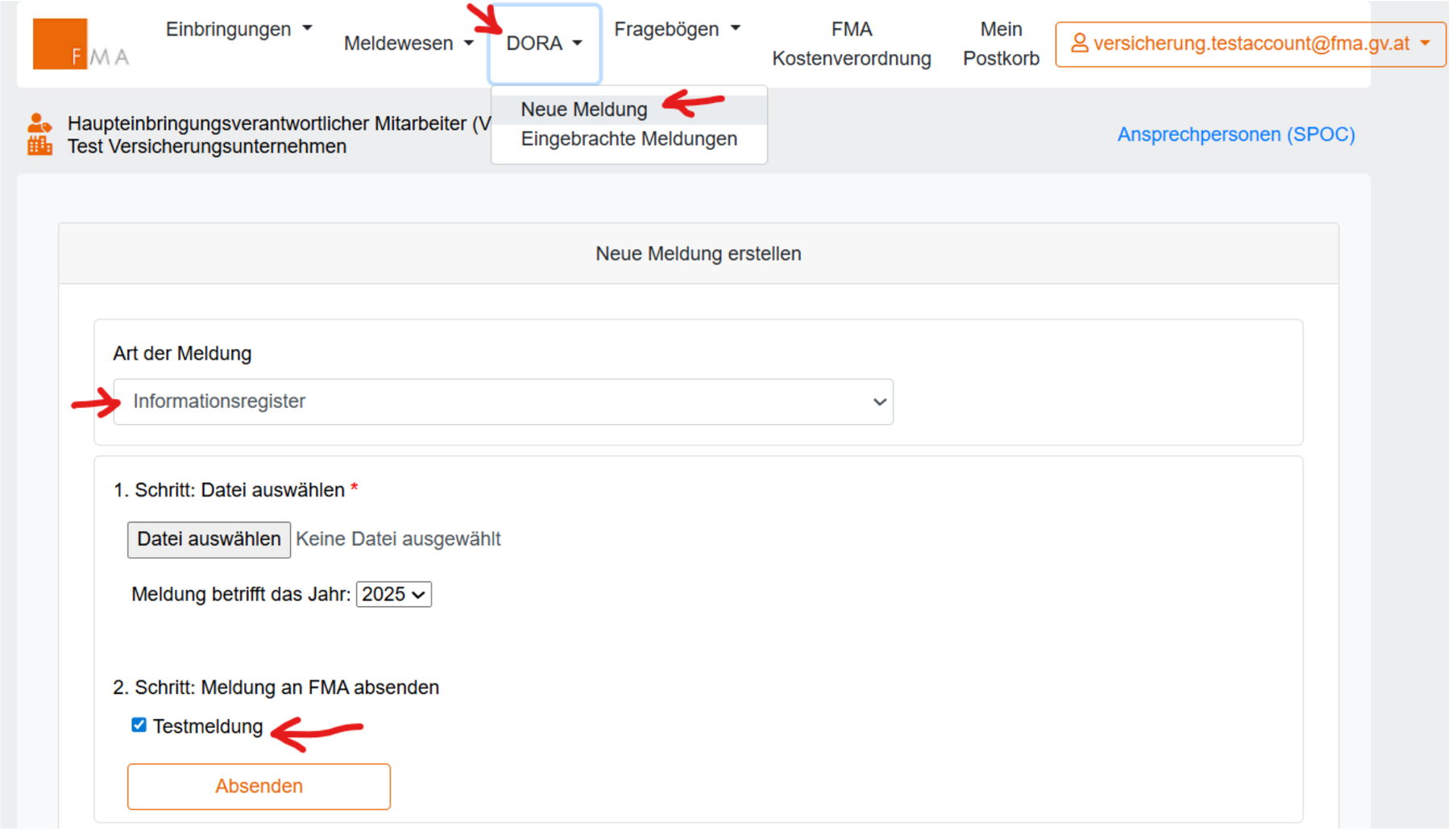
Die FMA wird das aktualisierte Excel-Template frühestmöglich zur Verfügung stellen:

- In Abhängigkeit von den europäischen Vorgaben werden weitere Möglichkeiten (z.B. csv) evaluiert.

TIMELINE INFORMATIONSREGISTERMELDUNG 2026

Testmöglichkeit

- Bereits offen
  (Siehe Screenshot)
- Status der Checks:
  Mai 2025



FAQ: ABBILDUNG INTERNER IKT-SERVICEANBIETER IM ROI

- **VARIANTE I**
  - Eine gruppeninterne Servicegesellschaft erbringt IKT-Dienstleistungen
  - Diese werden **teilweise selbst erbracht** und ggf. teilweise von Dritten außerhalb der Gruppe erbracht

- **VARIANTE II**
  - Die IT wird vertraglich an eine gruppeninterne Gesellschaft (meist die Muttergesellschaft) übertragen
  - Diese Gesellschaft hat **selbst kein IT-Personal**, sondern zeichnet weiterführende IKT-Dienstleistungsverträge mit externen/internen Drittparteien

- **Erfassung der Servicegesellschaft als Dienstleister**
  - Erfassung der Beziehung mit der Servicegesellschaft wie üblich als direkte IKT-Dienstleistung (dh. in B.02.01, B.02.02, B.05.01, etc.)
  - Zusätzlich Beschreibung der internen Dienstleistungskette in Template B.02.03
  - Weitere Drittparteien werden wie üblich bei kritischen/wichtigen DL in B.05.02 als Sub-Dienstleister erfasst (Achtung! Der erste externe DL einer Kette auch bei nicht kritisch/wichtigen DL!)

- **Erfassung der Zwischengesellschaft als ‚Entitiy signing'**
  - Erfassung der Zeichnung von Verträgen in B.03.01 und B.03.03
  - Die Zwischengesellschaft selbst wird NICHT als IKT-Dienstleister erfasst, wenn keine DORA IKT-DL selbst erbracht werden
  - Die externen/internen Drittparteien werden als DIREKTE Dienstleister erfasst (dh. in B.02.01, B.02.02, B.05.01, etc.)

FAQ: KRITISCHE ODER WICHTIGE FUNKTIONEN

- **Was sind kritische oder wichtige Funktionen?**
  - **Art. 3 Z 22 DORA:**
    „kritische oder wichtige Funktion“ eine Funktion, deren Ausfall 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;
  - D.h.: Dies sind sämtliche Funktionen, die man im Rahmen einer Business Impact Analyse (BIA) identifiziert und als kritische oder wichtige Funktion definiert hat. Die Einstufung hat grundsätzlich anhand der unter Art. 3 Z 22 DORA genannten Kriterien zu erfolgen.
  - Die Einstufung der Kritikalität erfolgt nicht nach den gesetzten Maßnahmen, die die Ausfallswahrscheinlichkeit der Funktionen reduziert.
    D.h.: Auch wenn Vorkehrungen getroffen wurden, die einen Ausfall einer kritischen oder wichtigen Funktion nahezu verhindern, bleibt es trotzdem eine wichtige oder kritische Funktion!
- **Sind nur IKT-Dienstleister im RoI anzuführen, welche ausschließlich kritische oder wichtige Funktionen unterstützen?**
  - Nein, es sind sämtliche IKT-Dienstleister im ROI anzuführen.

UNTERSCHEIDUNG FINANZDIENSTLEISTUNG UND IKT-DIENSTLEISTUNG

Wichtigste Grundlagen zur Einstufung

Art 4 Zi 21 DORA: Begriff IKT-Dienstleistung

digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste

Erwägungsgrund 63 DORA

Der Erwägungsgrund zeigt den Grundgedanken der Gesetzgebung zur Einstufung und Breite des Begriffs „IKT-Dienstleistung“. Ausnahme: von Zentralbanken, die Zahlungs- oder Wertpapierliefer- und -abrechnungssysteme betreiben, und von staatlichen Behörden, die IKT-bezogene Dienste im Zusammenhang mit Funktionen des Staates bereitstellen.

Q&A DORA030 – 2999: Einstufung IKT-Dienstleistung

Die Q&A bestätigt die breite Auslegung von IKT-Dienstleistung. Darüber hinaus gibt sie weitere Hinweise zur Einstufung und bietet 2 Fragestellungen, die einer Zuordnung zur Art der Dienstleistung dienen.

Umsetzung

Grundsätzlich gilt, dass Finanzunternehmen gemäß DORA in jedem **Einzelfall prüfen** (Vertragsinhalte) müssen, ob es sich um eine IKT-Dienstleistung gemäß DORA handelt. Der **Begriff der IKT-Dienstleistung** gemäß DORA ist **sehr breit** zu sehen. Eine Einstufung als **Finanzdienstleistung** ist nur zulässig, **wenn die gesamthafte Finanzdienstleistung bezogen wird**, nicht nur Teilbereiche einer Finanzdienstleistung (z.B. Verification of Payee als IKT-Dienstleistung).

Informationen zu IKT-bezogenen Vorfällen

WARUM IST IT-SECURITY & ZUSAMMENARBEIT WICHTIG?

Beispiel aus aktuellem Anlass: GlassWorm – aktuell aktiv!

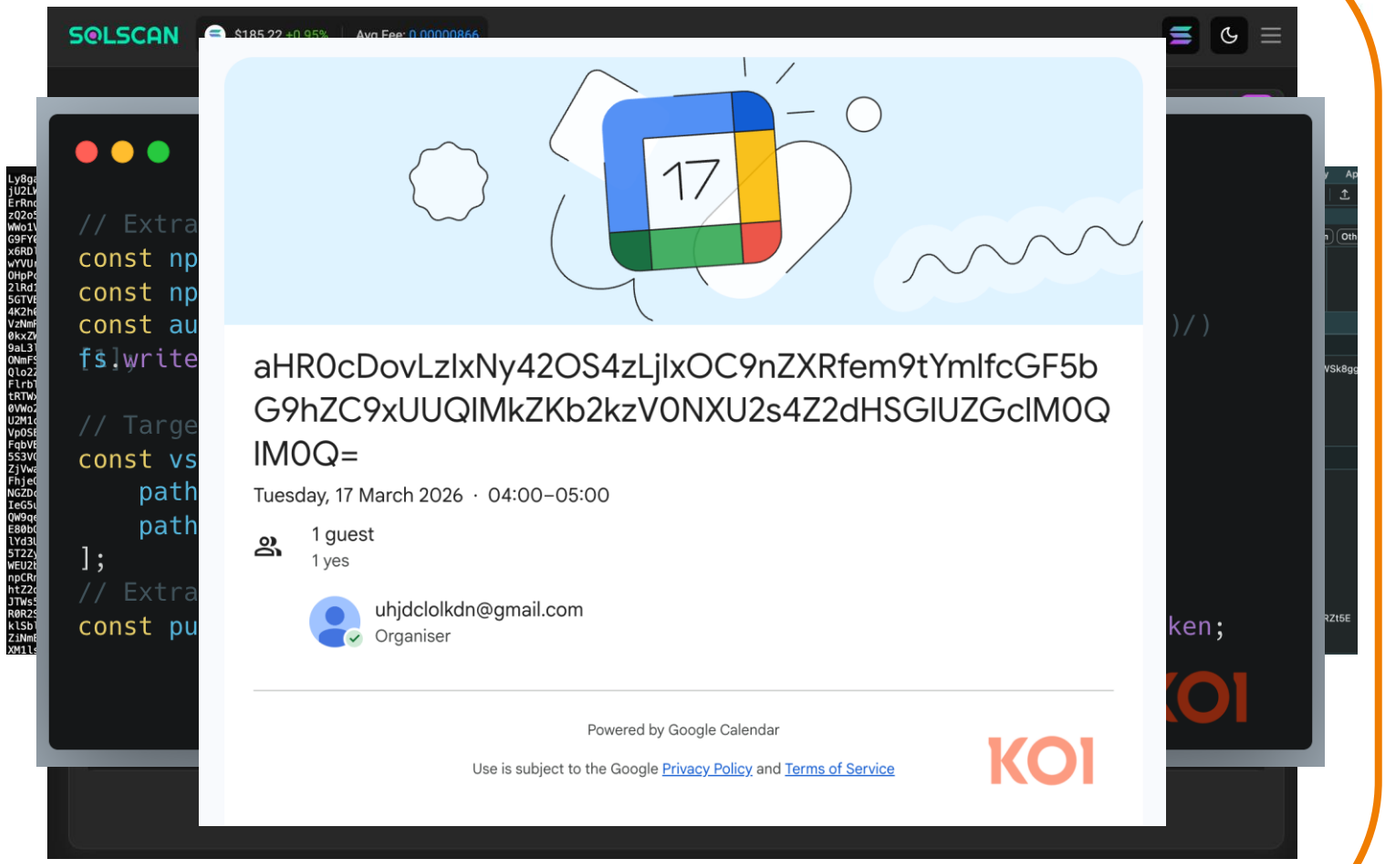
- Kostenlose Erweiterungen für beliebtes Entwicklertool (VS-Code) werden genutzt, um Rechner von Softwareentwicklern zu infizieren.
- Technisch hoch entwickelt: Nutzung von Blockchain, um Befehle an die Schadsoftware zu verteilen, Selbstständige Weiterverbreitung durch Infektion von Softwarepaketen, auf die der betroffene Entwickler selbst Zugriff hat.

https://www.heise.de/news/Gefaehrlicher-und-unsichtbarer-Wurm-in-Visual-Studio-Code-Extensions-gefunden-10789320.html
https://www.koi.ai/blog/glassworm-first-self-propagating-worm-using-invisible-code-hits-openvsx-marketplace

WARUM IST IT-SECURITY & ZUSAMMENARBEIT WICHTIG?

B

1. Download einer kostenlosen Erweiterung für VS.Code aus Open VSX
2. Code darin versteckt mit nicht darstellbaren Unicode Schriftzeichen
3. Nachladen von aktueller C&C Serveradresse aus der Solana Blockchain
4. Nachladen von Schadcode vom C&C Server, verschlüsselt, Key im HTTP-Response Header
5. Malware versucht Crypto Wallets und Zugänge zu Quellcodeablagen zu kopieren
6. Holt über Google Calender weitere C&C Server Adresse und lädt Remote Access Toolkit (RAT) herunter, um Rechner langfristig komplett zu übernehmen und zu nutzen. C&C über BitTorrent DHT



https://ww

https://www.koi.ai/blog/glassworm-first-self-propagating-worm-using-invisible-code-hits-openvsx-marketplace

WARUM IST IT-SECURITY & ZUSAMMENARBEIT WICHTIG?

Beispiel aus aktuellem Anlass: GlassWorm – aktuell aktiv!

- Kostenlose Erweiterungen für beliebtes Entwicklertool (VS-Code) werden genutzt, um Rechner von Softwareentwicklern zu infizieren.
- Technisch hoch entwickelt: Nutzung von Blockchain, um Befehle an die Schadsoftware zu verteilen, Selbstständige Weiterverbreitung durch Infektion von Softwarepaketen, auf die der betroffene Entwickler selbst Zugriff hat.

C&C Anweisungen in der Blockchain?

Nicht dargestellte UniCode Zeichen?

Command & Control Server?

Open VSX Repository?

Distributed Hash Table & Bittorrent?

https://www.heise.de/news/Gefaehrlicher-und-unsichtbarer-Wurm-in-Visual-Studio-Code-Extensions-gefunden-10789320.html
https://www.koi.ai/blog/glassworm-first-self-propagating-worm-using-invisible-code-hits-openvsx-marketplace

WARUM IST IT-SECURITY & ZUSAMMENARBEIT WICHTIG?

Beispiel aus aktuellem Anlass: GlassWorm – aktuell aktiv!

- Kostenlose Erweiterungen für beliebtes Entwicklertool (VS-Code) werden genutzt, um Rechner von Softwareentwicklern zu infizieren.
- Technisch hoch entwickelt: Nutzung von Blockchain, um Befehle an die Schadsoftware zu verteilen, Selbstständige Weiterverbreitung durch Infektion von Softwarepaketen, auf die der betroffene Entwickler selbst Zugriff hat.

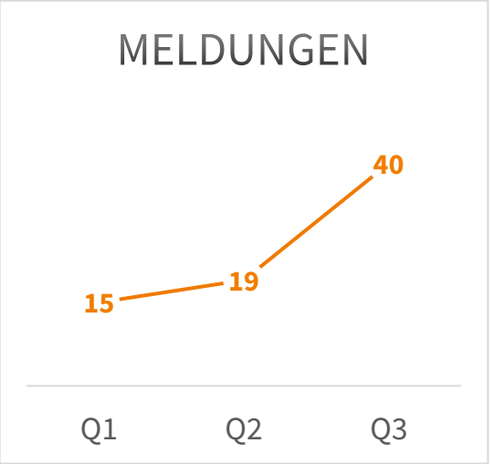
Erkenntnisse und Erwartungen der Aufsicht

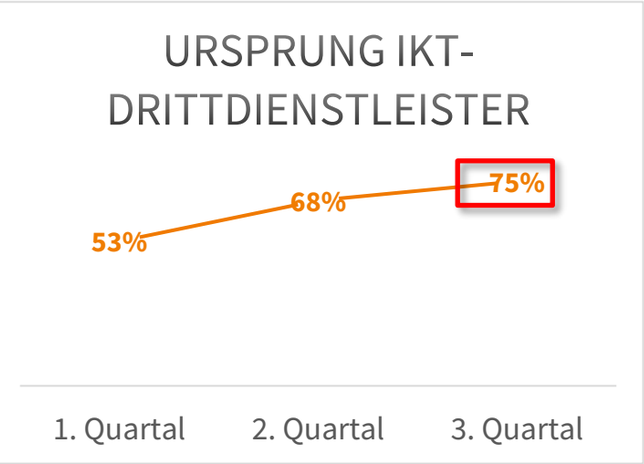
- Staatliche Akteure nutzen aktuell alle technischen Möglichkeiten, um Schutzmechanismen zu umgehen und maximalen Schaden zu erzeugen.
- Die Software Supply Chain wird genutzt um Schadcode an Entwickler sowie deren Kunden zu verteilen und bereitet weiterführende Angriffe durch Installation von Hintertüren vor.
- Speziell der Finanzsektor ist ein attraktives Ziel – wir müssen die Bedrohungen im Detail verstehen und systematisch dagegen vorsorgen – DORA gibt uns den Rechtsrahmen dafür.

https://www.heise.de/news/Gefaehrlicher-und-unsichtbarer-Wurm-in-Visual-Studio-Code-Extensions-gefunden-10789320.html
https://www.koi.ai/blog/glassworm-first-self-propagating-worm-using-invisible-code-hits-openvsx-marketplace

ÜBERBLICK – ANZAHL EINGELANGTER VORFÄLLE & URSACHEN 2025

Meldungen	Q1	Q2	Q3
Anzahl gemeldete Vorfälle	17	28	51
davon als nicht schwerwiegend reklassifiziert	2	9	11
Gesamt	**15**	**19**	**40**





Ursprung IKT-Dienstleister	Q1	Q2	Q3
Gesamt	8	13	30

Ursachen lt. Abschlussmeldung (Mehrfachnennung von Ursachen möglich)	Q1	Q2	Q3* *noch nicht alle Abschlussmeldungen erhalten
Malicious actions	2	2	16
Process failure	1	4	2
System failure / malfunction	9	9	13
Human error	1	3	3
External event	3	3	7

ÜBERBLICK – ANZAHL EINGELANGTER VORFÄLLE & URSACHEN 2025

Beispiel: Ransomware-Angriff bei einem IKT-Drittanbieter

- DORA verlangt eine **vertragliche Verpflichtung von IKT-Drittanbietern**, dass diese Sicherheitsvorfälle an Kunden melden und mit der Aufsicht kooperieren – in der Praxis ist die Umsetzung oft uneinheitlich.
- Ransomware-Vorfälle bei IKT-Drittanbietern bergen ein erhöhtes Risiko für viele Finanzunternehmen.
- Ziel ist, zu verhindern, dass Angreifer über einen Dienstleister mehrere Kunden gleichzeitig kompromittieren (z.B. SolarWinds 2019).

Erkenntnisse und Erwartungen der Aufsicht

- Auch Vorfälle, die durch IKT-Drittanbieter verursacht werden, müssen gemeldet werden. FMA kann analysieren, inwieweit andere Finanzunternehmen von dem Vorfall betroffen sind.
- FMA kann Informationen direkt von Drittanbietern anfordern und mit Kundeninformationen abgleichen.
- Updates von kompromittierten Drittanbietern sollten kritisch geprüft werden!
- Sichern Sie auch Ihre eigenen DevOps. (→ NPM Angriffe im September 2025)

Beispiel: Agentic AI

- KI-Systeme werden gegenwärtig sehr schnell in zahlreiche bestehende IT-Infrastrukturen integriert.
- Insbesondere Agentic-AI und Retrieval-Augmented Generation (RAG)-Systeme benötigen Zugriff auf Bestandsdaten.
- Sicherheitslücken in (bleeding-edge) KI-Software dürfen keinesfalls als Einfallstor für Angriffe dienen.
- Praxisbeispiel:
  Salesloft Drift → Salesforce → Zscaler, Palo Alto, Tenable, Cloudflare, etc.:
  https://www.driftbreach.com/

Erkenntnisse und Erwartungen der Aufsicht

- Stellen Sie sicher, dass auch bei Innovationsprojekten die in DORA geforderten Tests durchgeführt werden.
- Beziehen Sie Angriffe auf KI-Anwendungen ggf. in Resilienztests mit ein.

FÖRDERUNG INFORMATIONSAUSTAUSCH ZU CYBERBEDROHUNGEN

Hinweis auf Dialog ‚DORA-Vorfälle & Förderung Informationsaustausch' vom 16.6.2025:

Unterstützung durch

- CERT.at
- BMI
- WKO
- Watchlist Internet

Nutzen Sie unsere Webseite: FMA-DORA-Querschnittsthemen
Lesen Sie in den Unterlagen des DORA-Dialogs vom 16.6.2025 nach, auch im Beitrag der Watchlist Internet.

Melden Sie sich zu den Newslettern von CERT.at an: https://www.cert.at/de/services/mailinglisten/.

Update Generic Threat Landscape

Was ist die Generic Threat Landscape (GTL)?

Die GTL erfasst die **generelle Bedrohungslage im Cyberraum** des österreichischen Finanzsektors

Die GTL dient primär als **Ausgangspunkt für TIBER-Tests** und wird darüber hinaus an **interessierte Finanzunternehmen** zur Information übermittelt.

Wird **halbjährig** von einem externen Dienstleister **erstellt**

Erfasst relevante **Bedrohungsakteure, Taktiken, Techniken** und globale sowie lokale **Trends** im österreichischen Finanzsektor

GTL | Aktuelle Bedrohungen im österreichischen Cyberraum

Staatlich motivierter Akteure

Die wichtigsten Akteure:

Russland ändert aktuell sein Verhalten:

- **Zunehmend destruktives Vorgehen** – auch gegen Energie- und andere kritische Infrastrukturen
- **Primärfokus auf der Ukraine**, begrenzte Ressourcen im Westen
- **Hacktivistische Aktivität** im Westen **rückläufig**, vermutlich durch Fokusverlagerung
- **Network-Prepositioning-Aktivitäten** gewinnen an Bedeutung und sind eine **realistische Bedrohung**

Organisierte Cyberkriminalität (OCGs)

- **Ransomware, Datendiebstahl** und **Erpressung** bleiben dominierende Bedrohungen
- Finanzsektor weiterhin **attraktives Ziel** für OCGs
- **Datendiebstahl** finanzkritischer Informationen durch verschiedene Akteure
- „**Access-as-a-Service**“ boomt:
  - Ausnutzung neuer Schwachstellen durch wenig versierte Angreifer
  - Weiterverkauf erlangter Netzwerkzugänge oder Credentials an RaaS-Anbieter

GTL | Einflussfaktoren auf die aktuelle Cyberbedrohungslage

Politische Faktoren

- **US-Wahl / Trump-Faktor**: mögliche Veränderungen in internationaler Sicherheits- und Handelspolitik
- **Gestiegene geopolitische Spannungen** zwischen Russland und dem Westen, begleitet von erhöhter militärischer und cyberoperativer Aktivität

Technologische Faktoren

- **AI-gestützte Phishing-Kampagnen** und automatisierte Exploits erhöhen Angriffseffizienz
- **US-Zölle** und Exportbeschränkungen hemmen technologische Entwicklung und führen zu erhöhter Motivation für den **Diebstahl geistigen Eigentums**

Regulatorische Faktoren

- **DORA** und **NIS2** werden dazu beitragen, die Cyber-Resilienz innerhalb der Europäischen Union insgesamt zu stärken

Status Überwachungsrahmen

STATUS IM ÜBERWACHUNGSRAHMEN

Designierung

- Seit Sommer 2025 läuft auf Basis der Informations-register-Daten die Auswahl der kritischen IKT-Drittdienstleister (CTPP).
- Auswahl Prozess sollte im November 2025 abgeschlossen sein.

Aufsetzen der Aufsichtsteams (JET)

- In den 3 ESAs (EBA, ESMA, EIOPA) werden gemeinsame Aufsichtsteams (Joint Eximination Teams, kurz JET) aufgesetzt.
- Zuteilung zu ESAs erfolgt themenabhängig.

Laufende Aufsicht kritischer IKT-Drittdienstleistern (CTPP)

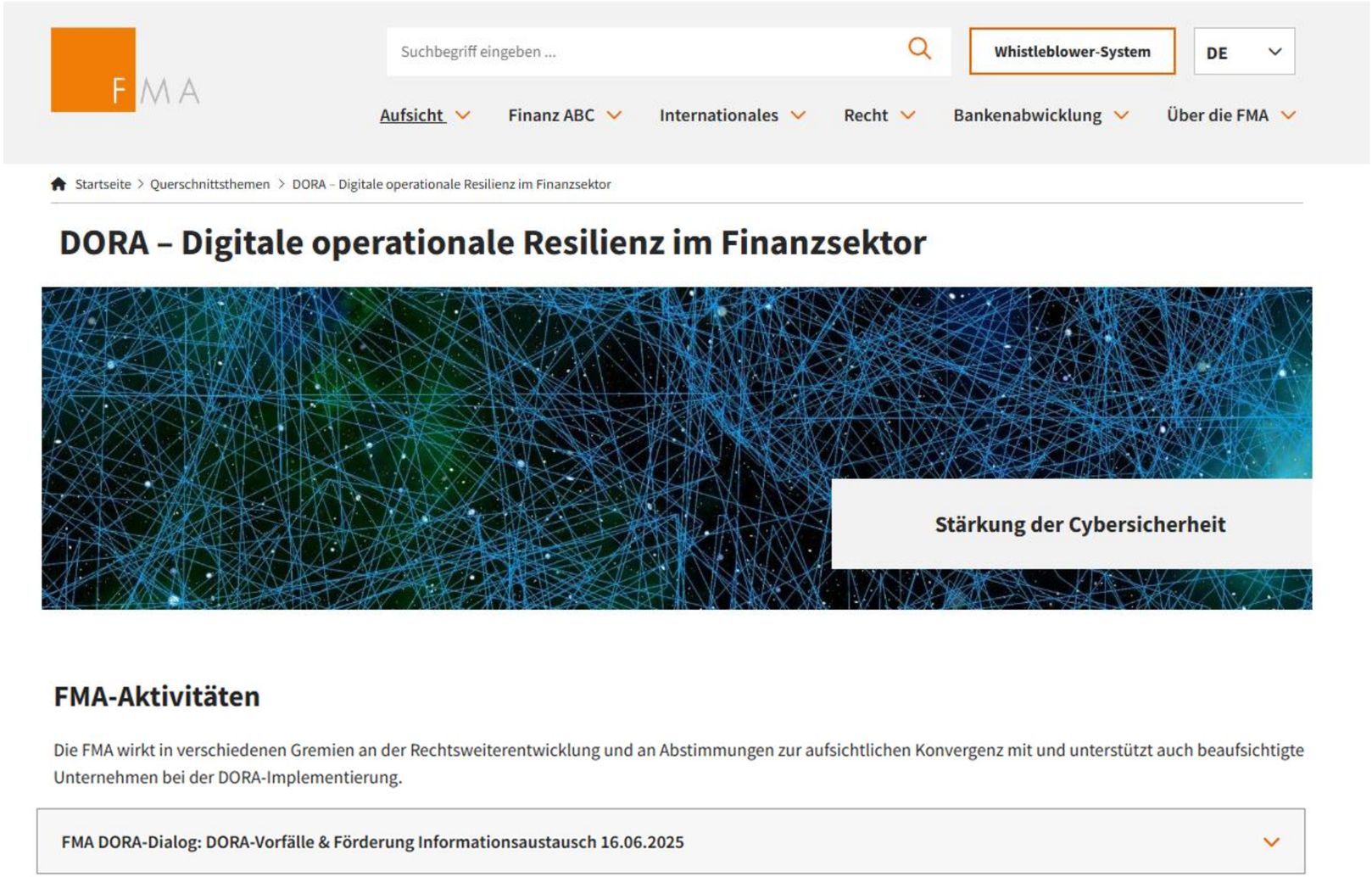
- Vor-Ort-Prüfungen
- Sonstige Aufsichtsmaßnahmen
- Thematisch Arbeiten

Über das Oversight Forum der ESAs und den gemeinsamen Aufsichtsteams werden kritische IKT-Drittdienstleister auf europäischer Ebene geprüft.

Ein Überwachungsrahmen zum Informationsaustausch wird aufgesetzt, damit nationale Behörden auf Feststellungen der JETs reagieren können.

Ausblick

FMA-DORA-WEBSITE



⇦ **Updates folgen**

FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz

OESTERREICHISCHE NATIONALBANK

EUROSYSTEM