

MELDEPFLICHTEN IM BARGELD- LOSEN ZAHLUNGSVERKEHR

Entwurf neuer Empfehlungen der EBA im Kontext
PSD II

Holger Friedrich
Dr. Waldemar Grudzien

Key Facts

- » EBA veröffentlicht Dokument mit „Empfehlungen“ zu Anforderungen an ein Meldewesen im bargeldlosen Zahlungsverkehr für Zahlungsdiensteanbieter und Bankenaufsicht
- » EBA stellt ein Klassifizierungsschema basierend auf 7 Kriterien und Schwellwerten sowie ein detailliertes Meldeformular zur Verfügung
- » Zahlungsdiensteanbieter dürfen ihre Meldepflichten allein oder zusammen mit anderen Zahlungsdiensteanbietern an Dienstleister delegieren

1. Klassifizierung eines Vorfalls

Nach Artikel 96 der Payment Service Directive PSD II müssen Zahlungsdiensteanbieter bis zum 13. Januar 2018 ein Meldewesen für schwerwiegende Betriebs- und Sicherheitsvorfälle im bargeldlosen Zahlungsverkehr implementieren. Die EBA schlägt ein Klassifizierungsschema zum Entscheid über die Notwendigkeit der Meldung eines Vorfalls mit vier quantitativen und drei qualitativen Kriterien vor. Die Kriterien sind

- Anzahl betroffener Transaktionen
- Anzahl betroffener Kunden
- Dauer Ausfallzeit
- Wirtschaftliche Auswirkung
- Grad interne Eskalation
- Auswirkungen auf andere PSPs¹/ Infrastrukturen gegeben
- Auswirkung auf Reputation

Für vier Kriterien werden Schwellwerte (Zahlen) und für drei Entscheidungskriterien (Ja/ Nein) genannt, wobei sich die Schwellwerte in zwei Stufen unterteilen. Abhängig von der Anzahl der erfüllten Kriterien und ihrer Schwellwertstufe wird eine Klassifizierung des Vorfalls in schwerwiegend/ nicht schwerwiegend vorgenommen. Ein Vorfall

ist als schwerwiegend zu klassifizieren, wenn er mindestens einen Schwellwert der Stufe 2 oder mindestens drei Schwellwerte der Stufe 1 erreicht.

2. Meldeprozess

Für den Meldeprozess entlang eines Vorfalls erwartet die EBA drei Arten von Meldungen:

- Erstmeldung (initial report)
 - Was ist passiert?
 - Eingetretene/ mögliche Auswirkungen
 - Max. 2 Stunden nach Entdeckung des Vorfalls
- Zwischenmeldung(en) (intermediary report)
 - Bei signifikanter Änderung der Lage
 - Max. 3 Arbeitstage nach Erstmeldung
 - Letzte Zwischenmeldung nach Erreichen des Normalbetriebs
- Abschlussmeldung (end report)
 - Volle Information über vergangenen Vorfall
 - Auswirkungen und Lösung des Vorfalls
 - Max. 2 Wochen nach Bewältigung des Vorfalls

¹ PSP: Payment Service Provider im Sinne der PSD II

Meldeprozess, Kriterien, Schwellwerte des EBA-Vorschlages

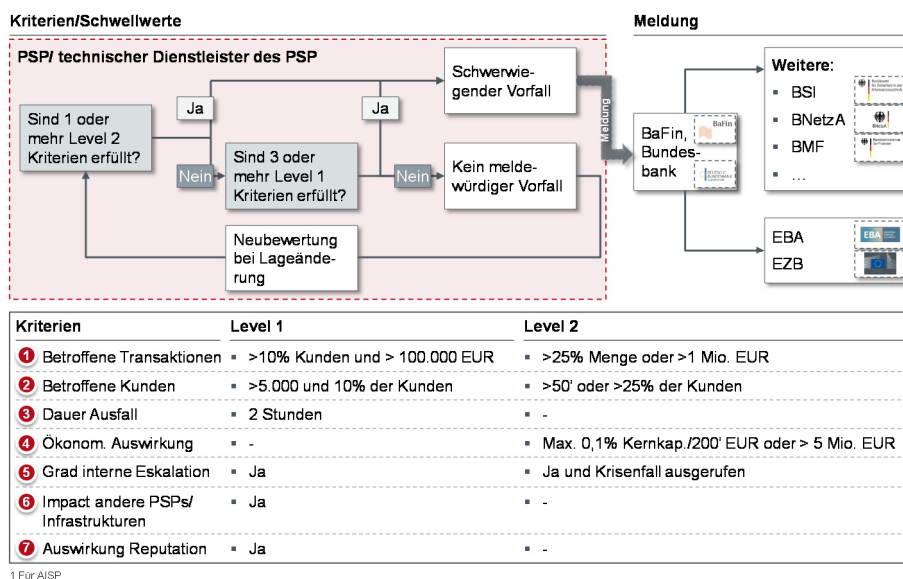


Abbildung 1: Mechanik der Klassifizierung von Betriebs- und Sicherheitsvorfällen
in Bezug auf die Schwere der Auswirkungen

Der Zahlungsdiensteanbieter kann seine Meldepflichten alleine oder im Verbund mit anderen Zahlungsdiensteanbietern an einen technischen Dienstleister auslagern, bleibt aber immer verantwortlich für die Meldung schwerwiegender Vorfälle. Ein Dienstleister muss seinen Sitz in der Europäischen Union haben. Sind mehrere seiner Kunden durch einen Vorfall betroffen, darf der Dienstleister eine einzige Meldung für diese Zahlungsdiensteanbieter an die Bankenaufsicht übermitteln. Neben den dargestellten detaillierten Vorgaben zum Meldeprozess vom Zahlungsdiensteanbieter zur Bankenaufsicht skizziert der Entwurf auch den Austausch von Informationen zum schwerwiegenden Vorfall zwischen der nationalen Bankenaufsicht und weiteren kompetenten nationalen Behörden (Section 5) und den Austausch zwischen nationalen Bankenaufsichten mit EBA und Europäischer Zentralbank (Section 6). Im ersten der zwei Fälle

kann zum Beispiel bei drohenden Gefahren für die Finanzmarktstabilität das Finanzministerium eingeschaltet werden oder weitere Stellen, wenn ein Vorfall bereits große mediale Aufmerksamkeit erfahren hat.

Gemäß Empfehlung 4 fordert die EBA Zahlungsdiensteanbieter auf, die Aufnahme aller Verantwortlichkeiten und Prozesse zur Bearbeitung schwerwiegender Vorfälle in ihre Betriebs- und Sicherheitspolicies sicherzustellen.

3. Vergleich mit MASl

Diese Guidelines werden in der finalen Fassung am 13. Januar 2018 die Meldevorschriften der MaSl (Mindestanforderungen an die Sicherheit von Internetzahlungen) ablösen. Ein erster Vergleich zeigt einige Gemeinsamkeiten und auch Unterschiede:

- **Meldungsarten:**
 - Beide Regelwerke schreiben drei Meldungsarten vor: Erst-, Zwischen-, Abschlussmeldung
 - EBA gibt konkrete Fristen im Verhältnis der drei Meldungsarten vor, BaFin ist flexibler bei Meldungsarten
- **Meldefrist:**
 - EBA erwartet die Erstmeldung zwei Stunden nach Bemerkung des Vorfalls
 - BaFin erwartet Erstmeldung „unverzüglich, also ohne schuldhaftes Zögern beim Ausfall oder Teilausfall von bankfachlichen Prozessen, wenn erkennbar ist, dass der Ausfall oder Teilausfall eine Stunde überschreiten wird“.
 - Die Meldefrist der BaFin bietet mehr Freiheitsgrade, schafft dadurch aber nach Auffassung der Verfasser mehr Entscheidungskomplexität in einer - mindestens wahrgenommenen - Krisenlage
- **Kriterien zu Meldeentscheid:**
 - EBA gibt konkretes Klassifizierungsschema mit 7 Kriterien mit Schwellwerten (Zahlen) und Entscheidungskriterien (Ja/Nein) und zwei Stufen vor
 - BaFin verwendet eine abstrakte Definition für zu meldende schwerwiegende Zahlungssicherheitsvorfälle vor - wenn Verfügbarkeit, Integrität, Vertraulichkeit oder Authentizität von IT-Systemen, Anwendungen oder Daten mit einem hohen oder sehr hohen Schutzbedarf verletzt oder beeinträchtigt wird.
 - Auch hier wieder mehr Freiheit gegen niedrigere Komplexität in einer schwierigen Entscheidungslage
- **Auslagerung der Meldepflicht:**
 - EBA und BaFin erlauben die Auslagerung der Meldepflicht an den externen IT-Dienstleister, an den die IT-Dienstleistung des PSP ausgelagert ist.
 - Aber die BaFin macht keine geographischen Einschränkungen der IT-Dienstleister.
- **Meldeformular:** EBA und BaFin bieten jeweils ein Meldeformular an.

4. Erste Fragen und Anregungen

Die Anforderungen der EBA an ein Meldewesen im bargeldlosen Zahlungsverkehr werden die Zahlungsdiensteanbieter zwingen, ihre IT- und Datenbanken-Infrastruktur anzupassen. Wie in Abbildung 2 dargestellt gibt es derzeit mehrere nationale und europäische Initiativen zu Meldepflichten. Die Verfasser schätzen, dass die Herausforderung darin besteht, die verschiedenen Anforderungen in möglichst einer singulären Melde-Engine zusammenzuführen und nicht im ungünstigen Fall je Regelung spezifische Meldeprozesse zu implementieren; wie in der Vergangenheit jedoch oftmals geschehen.

Durch die Erlaubnis der Delegation der Meldepflichten an den technischen Dienstleister, der für den PSP die IT-Dienstleistung erbringt, erkennt die EBA an, dass externe Dienstleister nicht nur die erbrachte IT-Dienstleistung besser ausführen, sondern auch einen Vorfall besser verstehen und verarbeiten können, als ein Zahlungsdiensteanbieter. Diese Entscheidung wird sich mit hoher Wahrscheinlichkeit als richtungsweisend

Meldepflichten aus nationalen und europäischen regulatorischen wie gesetzlichen Vorgaben

Organisation	Regulierung	Stelle	Definition Meldung	Ab wann	Meldung an
BaFin (BMF)	MaSi Wird abgelöst durch	Titel I Ziffer 12, Nr. 3.2	Schwerwiegender Zahlungssicherheitsvorfall, Meldebogen	Bereits in Kraft	BaFin, Bundesbank, Datenschutzbb.
EU KOM	PSD II Meldeanforderungen detailliert durch	Artikel 96	„schwerwiegender Betriebs- oder Sicherheitsvorfall“, wird definiert durch EBA RTS Incident Mgt. bis 13.01.2018	13.01.2018	BaFin → EBA
EBA	RTS Incident Management	Consultation Draft am 07.12.2016	schwerwiegender Betriebs- und Sicherheitsvorfall im bargeldlosen Zahlungsverkehr	13.01.2018	BaFin → EBA
	RTS SCA & CSC	Definition und Guideline 3	„Major payment security incident“	Frühestens Okt. 2018	BaFin, Datenschutzbb.
EU KOM	NIS-RL Ist bereits umgesetzt durch	Artikel 14 Abs. 3, 4, 5, 6	Meldung „erheblicher Störung“	10.05.2018	Bundesamt für Sicherheit in der Informationstechnik
BSI (BfSI)	IT-SIG	Artikel 1 Nr. 7 §8b	„Erhebliche Störungen“, Konkretisierung durch Änderungsverordnung (erwartet im Dez. 2016)	01.07.2017	Bundesamt für Sicherheit in der Informationstechnik

Abbildung 2: Nationale und europäische Meldevorgaben

für weitere PSP-Dienstleister-Beziehungen außerhalb des aktuell betrachteten Fokus erweisen; beispielhaft sind hier Cloud Computing, Identitäts-, Authentizitäts- und Autorisierungsdienstleister mit massiv skalierenden Echtzeit-Anforderungen genannt.

Die EBA beschränkt die technischen Dienstleister auf die Europäische Union. Zahlungsdiensteanbieter dürfen keinen Dienstleister aus Norwegen, der Schweiz oder den USA wählen. Mindestens die Erweiterung auf den Europäischen Wirtschaftsraum (EWR) scheint geboten. Zudem sollte die EBA den bevorstehenden Austritt Großbritanniens in ihre Erwägungen einbeziehen. Auch schreibt die EBA den Dienstleistern vor, eine Meldung für mehrere Zahlungsdienstleister nur dann anfertigen zu dürfen, wenn diese Zahlungsdienstleister in einem Land angesiedelt sind. Hier sollte bedacht werden, dass Angriffe oft multinational wirken und bei Zahlungsdienstleistern aus mehr als einem Land zum gleichen Vorfall führen können. Eine

Meldung aus einem möglichst großen Einwirkungsraum des Angriffs böte auch der Bankenaufsicht ein umfassenderes Bild, als wenn sie vergleichsweise die Meldung aus ihrem Land erhielte.

5. Fazit

Die EBA hatte diese Guidelines über mehrere Jahre hinweg jeweils für das Jahresende angekündigt. Die Verfasser begrüßen die nunmehr erfolgte Veröffentlichung, obwohl die feststellbar erhebliche Verzögerung zu weiteren immensen Herausforderungen in den Planungsprozessen der Deutschen Kreditwirtschaft für das Geschäftsjahr 2017 führen wird. Zumal in der verstrichenen Zeit die allumfassende, tiefgehende Vernetzung des Großteils der Geschäftsmodelle fortgeschritten ist oder mit höherer Dynamik vorangetrieben wird. Daher ist von einer deutlich anschwellenden Proliferation von Technologie im Banken- wie auch im Kundeneinsatz auszugehen, was auf eine gestiegene Anzahl

von Vorfällen und wohl auch vereinzelt auf eine Zunahme von Schweregraden in Vorfällen schließen lässt.

Deswegen wird es begrüßt, wenn eine Branche, die ihre Geschäftsmodelle im Besonderen auf Vertrauen aufbaut, mit gutem Beispiel vorangeht und Chancen im Vergleich zu Risiken aus neuen regulatorischen Anforderungen und zugrundeliegenden Technologien höher gewichtet, als es in der Vergangenheit in den Gremien der Institute erfolgte.

Mit der Veröffentlichung wurde jedoch ein Aspekt – die sich auch in diesem Segment zeigende regulatorische Überforderung der Kreditwirtschaft – nicht angegangen. Strukturell positiv hätte gewirkt, eine einzige Meldevorschrift verbindlich zu stellen; dies hätte jedoch einer nationalen sowie europäischen Harmonisierung im Vorfeld bedurft. Nun wird diese Harmonisierung im Markt durch die Zahlungsdiensteanbieter nachgeholt werden müssen. Hier werden Anstrengungen nötig sein, die umfänglichen Meldeanforderungen mit möglichst einem Ansatz zu erfüllen.

Ein angemessenes Meldewesen wird eine Bank keine neuen Kunden, auch keine neuen Erträge ermöglichen, aber bankaufsichtliche Anforderungen erfüllen und bei fokussierter Vorbereitung der IT ermöglichen, anstehende Konsolidierungsleistungen mit einem höheren Servicegrad für Fachseiten wie auch später effizientere Betriebsstrukturen zu kombinieren.

Sources

INTERNET:

<https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2>

VORAUSGEHENDE POSTS DER SERIE

COREinstitute 2016

<http://www.coretechmonitor.com/de/public-hearing-der-eba-zu-starker-authentifizierung-und-sicherer-kommunikation-im-rahmen-der-psd-ii/>

<http://www.coretechmonitor.com/de/auswirkungen-rtts-psd-ii/>

<http://www.coretechmonitor.com/de/it-sicherheitsgesetz-neue-anforderungen-an-kritische-betreiber/>



Holger Friedrich verantwortet seit 2010 die Beratungseinheit von CORE. Er ist seit über 25 Jahren in der Softwareindustrie tätig. Vor der Gründung von CORE hat er ein Technologieunternehmen aufgebaut, wirkte in leitender Position bei marktführenden Technologieanbietern und war u.a. Partner in einer führenden internationalen Strategieberatung.

Mail: holger.friedrich@coretransform.com



Dr. Waldemar Grudzien setzt sich als Transformation Engineer mit den aktuellen regulatorischen Anforderungen und deren technischer Realisierung auseinander. Als promovierter Elektrotechniker war er als Leiter in einem nationalen Bankenverband für die Bereiche Retailbanking und Banktechnologien zuständig.

Mail: waldemar.grudzien@coretransform.com

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
www.coreinstitute.org
Phone: +49 30 26344 020
office@coreinstitute.org

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
www.coretransform.de
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
www.coretransform.ch
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
www.coretransform.co.uk
Phone: +44 203 319 0356
office@coretransform.co.uk