FINALE EMPFEHLUNGEN DER EBA ZU MELDEPFLICHTEN IM BARGELD-LOSEN ZAHLUNGSVERKEHR IM KONTEXT PSD II

Christian Everts
Holger Friedrich
Dr. Waldemar Grudzien

Juli 2017
COREtechmonitor | Blogpost

Key Facts

- EBA veröffentlicht finales Dokument mit Empfehlungen zu Anforderungen an ein Meldewesen im bargeldlosen Zahlungsverkehr für Zahlungsdiensteanbieter und Bankenaufsicht
- Finale Empfehlungen nahezu unverändert im Vergleich zu Entwurf der Empfehlungen aus dem Dezember 2016
- EBA erhielt 43 Kommentare zum Entwurf der Empfehlungen
- Signifikante Änderungen betreffen die Verlängerung einer Meldefrist, die Erhöhung einer Schadensschwelle, die neue Einteilung der drei Meldearten sowie die Delegation der Meldepflichten
- Weitere Änderungen wurden zur Klarstellung von Definitionen und zur Präzisierung bislang verkürzt gefasster Begrifflichkeiten vorgenommen

Report

1. Änderungen zum Entwurf

Signifikant verlängert wurde die Frist bei der Erstmeldung von 2 auf 4 Stunden ab Identifikation des Vorfalls. Zudem muss im Zuge der Neuorganisation der drei Meldearten bei Erst- und Zwischenmeldung ein geringerer Informationsstand gemeldet werden. Dies ergibt sich aus der neu eigeführten „Komplettierung“ der Meldeformulare, sodass erst die Abschlussmeldung sämtliche Informationen zum Vorfall enthalten muss. Die bisher als „Level 1“ und „Level 2“ bezeichneten Kriterienarten erwiesen sich als nicht ausreichend selbsterklärend und wurden durch die Begriffe „Lower Impact level“ und „Higher Impact level“ ersetzt. Beim Kriterium Higher Impact Level wurde die Anzahl betroffener Transaktionen von 1 Mio. auf 5 Mio. Euro erhöht.

Ebenfalls beachtenswert ist der Entscheid der EBA, die Delegation der Meldepflichten an einen technischen Dienstleister nicht mehr geographisch auf die Europäische Union zu beschränken. Gleichzeitig stellt die EBA klar, dass der Zahlungsdienstleister verantwortlich für das Meldewesen gegenüber der Aufsicht bleibt und dass die Aufsicht im Vorfeld durch diesen informiert werden sollte, wer in seinem Namen die Meldungen abgibt.

Klarstellungen und Präzisierungen mit größeren Einfluss auf den Meldeaufwand befassen sich mit dem Kreis der zu meldenden Vorfälle. So müssen Vorfälle, die sich zu einem schwerwiegenden Vorfall hätten auswachsen können, jedoch zuvor gelöst werden konnten, nicht mehr gemeldet werden. Hingegen stellt die EBA klar, dass ein bereits als „schwerwiegend“ klassifizierter Vorfall auch dann gemeldet werden müsse, wenn er ebenfalls innerhalb der ersten 4 Stunden gelöst wurde. In diesem Fall könnte die Erstmeldung zugleich auch die Zwischen- und Abschlussmeldung beinhalten.

Angesichts der Änderungen stellt sich das finale Melderegime der EBA wie folgt dar.

2. Klassifizierung eines Vorfalls

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 der internen Eskalation
- Sind Auswirkungen auf andere PSPs / Infrastrukturen gegeben?
- Gibt es Auswirkungen auf Reputation?

Für die ersten 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 Kriterienart „Higher Impact level“ oder mindestens drei Schwellwerte der Kritereienart „Lower Impact level“ erreicht.

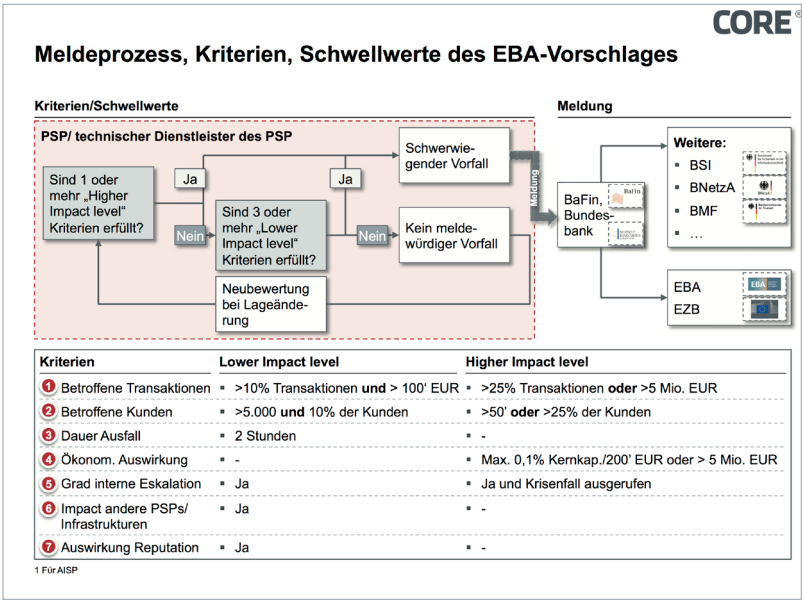

Abbildung 1: Mechanik der Klassifizierung von Betriebs- und Sicherheitsvorfällen in Bezug auf die Schwere der Auswirkungen

3. Meldeprozess

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

Erstmeldung (initial report)
- Was ist passiert?
- Eingetretene/ mögliche Auswirkungen
- Max. 4 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

[1] PSP: Payment Service Provider im Sinne der PSD II

Abschlussmeldung (end report)
- Volle Information über vergangenen Vorfall
- Auswirkungen und Lösung des Vorfalls
- Max. 2 Wochen nach Bewältigung des Vorfalls

Neu ist, dass die drei Meldearten nun komplettiert werden können, d.h. dass erst die Abschlussmeldung alle Informationen zum Vorfall enthalten muss. Zudem sollte im dem Fall, dass ein Vorfall noch innerhalb von 4 Stunden seit seiner Entdeckung behoben werden konnte, eine Abschlussmeldung erfolgen, die auch die Informationen der Erst- und Zwischenmeldung enthalte. Eine Abschlussmeldung hat auch für den Fall zu erfolgen, dass ein initial als schwerwiegend eingestufter Vorfall in der Zwischenzeit als nicht mehr meldewürdig zurückgestuft wurde.

Der Zahlungsdiensteanbiete kann seine Meldepflichten alleine oder im Verbund mit anderen Zahlungsdiensteanbietern an einen technischen Dienstleister auslagern, bleibt jedoch immer verantwortlich für die Meldung schwerwiegender Vorfälle. Ein Dienstleister muss seinen Sitz nun nicht mehr in der Europäischen Union nachweisen. Sind mehrere seiner Kunden durch einen Vorfall betroffen, darf der Dienstleister eine einzige Meldung für diese Zahlungsdiensteanbieter an die Bankenaufsicht übermitteln.

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

Neben den dargestellten detaillierten Vorgaben zum Meldeprozess vom Zahlungsdienstean-

bieter zur Bankenaufsicht skizziert der Entwurf ebenso den Austausch von Informationen zum schwerwiegenden Vorfall zwischen der nationalen Bankenausicht und weiteren kompetenten nationalen Behörden (Section 5) und mit EBA und Europäischer Zentralbank (Section 6).

Im ersten Fall kann die nationale Bankenaufsicht bei drohenden Gefahren für die Finanzmarktstabilität das Finanzministerium einschalten oder weitere Stellen, wenn ein Vorfall bereits große mediale Aufmerksamkeit erfahren hat. In beiden Arten des Informationsaustauschs werden mehr Vorgaben hinsichtlich der Geheimhaltung und Integrität der ausgetauschten Informationen auferlegt.

4. Fazit

Die Anforderungen der EBA an ein Meldewesen im bargeldlosen Zahlungsverkehr werden die Zahlungsdiensteanbieter zwingen, ihre IT- und Datenbanken-Infrastruktur weiter anzupassen. Wie in Abbildung 2 dargestellt, gibt es derzeit mehrere nationale und europäische Initiativen zu Meldepflichten. Die Herausforderung besteht darin, 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.

Die Erhöhung der Schadenshöhe der Kriterienart „Higher Impact level“ von 1 Mio. auf 5 Mio. Euro dürfte mit Hilfe guter Fraud Management-Systeme die Anzahl schwerwiegender Meldungen senken.

Banken sowie Zahlungsdienstabwickler werden nunmehr stärker

sensibilisert sein, einen Vorfall als schwerwiegend einzustufen und zu melden, da nun für jeden diesbezüglichen Vorfall, auch bei der Rückstufung des Vorfalls als nicht meldewürdig, alle Meldearten abzusetzen sind.

Die fehlende Harmonisierung der verschiednen Melderegime ist weiterhin als nachteilig für die europäische Bankenindustrie anzusehen.

Aus Sicht der Autoren sollten Banken zusammen mit ihrer Aufsicht eruieren, ob nicht im Zuge der fortschreitenden Digitalisierung das notwendige Meldewesen auf automatisierte Austauschdatenmodelle für eine kontinuierliche Datenerhebung durch die Aufsicht umgestellt werden könnte. Wie das Kontenabrufverfahren seit mehr als einem Jahrzehnt zeigt, ist dies keine Frage der einzusetzenden Technologien, sondern eine Frage des politischen und administrativen Willens. Den Aufsichtsobjekten würde so der Aufbau eines kostenintensiven Melde- und Prüfungswesen erspart und der Aufsicht die gefühlte Bittstellung. Das erkennbare Nutzenpotential läge in enormen Kostensenkungen sowie in Qualitätsgewinnen entlang der durch die Bankensteuerung quantifizierbaren Risiken.

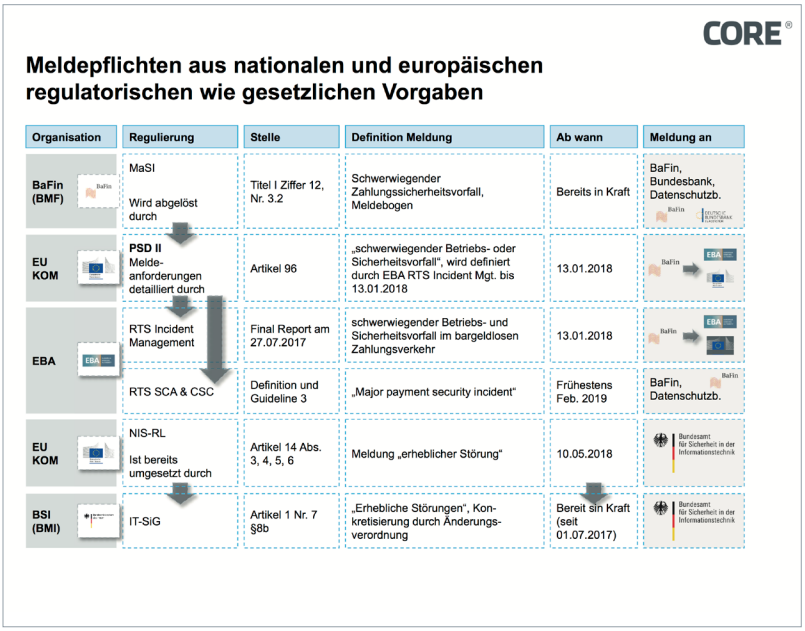

Abbildung 2: Nationale und europäische Meldevorgaben

Quellen

Internet:

https://www.eba.europa.eu/-/eba-publishes-final-guidelines-on-major-incident-reporting-under-psd2

Vorausgehende Posts der Serie:

COREinsitute 2016/2017

https://www.coretechmonitor.com/de/meldepflichten-im-bargeldlosen-zahlungsverkehr-entwurf-neuer-empfehlungen-der-eba-im-kontext-psd-ii/

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-rts-psd-ii/

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

Autoren

Christian Everts

Christian Everts ist Transformation Manager bei CORE und bringt insbesondere seine Erfahrungen im Bereich Regulatorik bei CORE ein. Vor seiner Tätigkeit bei CORE war Christian bei verschiedenen Banken als Compliance Manager tätig, wo er vorrangig regulatorische Anforderungen in deutschen und internationalen Investment- & Universalbanken implementierte.

Mail: christian.everts@core.se

Holger Friedrich

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@core.se

Dr. Waldemar Grudzien

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@core.se

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
https://institute.core.se
Phone: +49 30 26344 020
office@coreinstitute.org

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@core.se

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

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

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

COREtransform MEA LLC
DIFC – 105, Currency House, Tower 1
Dubai P.O. Box 506656 I UAE
https://www.core.se
Phone: +971 4 3230633
office@coretransform.ae