EBA/GL/2017/17

12/01/2018

Leitlinien

zu Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten gemäß der Richtlinie (EU) 2015/2366 (PSD2)

1. Einhaltung der Vorschriften und Meldepflichten

Status dieser Leitlinien

1. Das vorliegende Dokument enthält Leitlinien, die gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010 herausgegeben wurden. [1] Gemäß Artikel 16 Artikel 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden und Finanzinstitute alle erforderlichen Anstrengungen unternehmen, um diesen Leitlinien nachzukommen.

2. Die Leitlinien legen fest, was nach Ansicht der EBA angemessene Aufsichtspraktiken innerhalb des Europäischen Finanzaufsichtssystems sind oder wie das Unionsrecht in einem bestimmten Bereich anzuwenden ist. Dazu sollten die zuständigen Behörden gemäß Artikel 2 Absatz 4 der Verordnung (EU) Nr. 1093/2010 die an sie gerichteten Leitlinien in geeigneter Weise in ihre Aufsichtspraktiken (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren) integrieren, einschließlich der Leitlinien in diesem Dokument, die in erster Linie an Institute gerichtet sind.

Meldepflichten

3. Nach Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden der EBA bis zum 12.03.2018 mitteilen, ob sie diesen Leitlinien nachkommen oder nachzukommen beabsichtigen, oder die Gründe nennen, warum sie dies nicht tun. Geht innerhalb der genannten Frist keine Mitteilung ein, geht die EBA davon aus, dass die zuständige Behörde den Anforderungen nicht nachkommt. Die Mitteilungen sind unter Verwendung des auf der Website der EBA abrufbaren Formulars mit dem Betreff „EBA/GL/2015/XX“ an compliance@eba.europa.eu zu senden. Die Mitteilungen sollten durch Personen erfolgen, die befugt sind, entsprechende Meldungen im Auftrag ihrer Behörde zu übermitteln. Jegliche Änderungen des Status der Einhaltung müssen der EBA ebenfalls gemeldet werden.

4. Die Meldungen werden gemäß Artikel 16 Absatz 3 der EBA-Verordnung auf der Website der EBA veröffentlicht.

[1] Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12).

2. Gegenstand, Anwendungsbereich und Begriffsbestimmungen

Gegenstand und Anwendungsbereich

5. Diese Leitlinien dienen der Erfüllung des Auftrags, der der EBA gemäß Artikel 95 Absatz 3 der Richtlinie (EU) Nr. 2015/2366[2] (PSD2) erteilt wurde.

6. Diese Leitlinien enthalten Anforderungen für die Festlegung, Anwendung und Überwachung der Sicherheitsmaßnahmen, die die Zahlungsdienstleister gemäß Artikel 95 Absatz 1 der Richtlinie (EU) 2015/2366 zur Beherrschung der operationellen und sicherheitsrelevanten Risiken im Zusammenhang mit den von ihnen erbrachten Zahlungsdiensten ergreifen müssen.

Adressaten

7. Diese Leitlinien richten sich an Zahlungsdienstleister gemäß der Definition in Artikel 4 Absatz 11 der Richtlinie (EU) 2015/2366 und gemäß der Definition von „Finanzinstituten“ in Artikel 4 Absatz 1 der Verordnung (EU) 1093/2010 sowie gemäß der Definition von „zuständigen Behörden“ in Artikel 4 Absatz 2 Nummer (i) dieser Verordnung unter Bezugnahme auf die Richtlinie 2007/64/EG [3] (gegenwärtig Richtlinie (EU) 2015/2366[4]).

Begriffsbestimmungen

8. Sofern nicht anders angegeben, haben die in der Richtlinie (EU) 2015/2366 verwendeten und definierten Begriffe in den vorliegenden Leitlinien dieselbe Bedeutung. Für die Zwecke dieser Leitlinien gelten darüber hinaus die folgenden Begriffsbestimmungen:

[2] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35).

[3] Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG (ABl. L 319 vom 5.12.2007, S. 1).

[4] Gemäß dem zweiten Unterabsatz von Artikel 114 der Richtlinie (EU) 2015/2366 gelten Bezugnahmen auf die aufgehobene Richtlinie 2007/64/EG als Bezugnahme auf die Richtlinie (EU) 2015/2366 und sind nach Maßgabe der Entsprechungstabelle in Anhang II der Richtlinie (EU) 2015/2366 zu lesen.

Leitungsorgan	– Für Zahlungsdienstleister, bei denen es sich um Kreditinstitute handelt, hat dieser Begriff die gleiche Bedeutung wie in der Definition gemäß Artikel 3 Absatz 1 Nummer 7 der Richtlinie 2013/36/EU[5]. – Für Zahlungsdienstleister, bei denen es sich um Zahlungsinstitute oder E-Geld-Institute handelt, umfasst dieser Begriff Geschäftsleiter oder Personen, die für die Geschäftsleitung des Zahlungsdienstleisters verantwortlich sind, sowie gegebenenfalls Personen, die für die Führung der Zahlungsdienstgeschäfte des Zahlungsdienstleisters verantwortlich sind. – Für Zahlungsdienstleister gemäß den Buchstaben c, e und f von Artikel 1 Absatz 1 der Richtlinie (EU) 2015/2366 hat dieser Begriff die ihm gemäß den geltenden EU- oder nationalen Rechtsvorschriften zugewiesene Bedeutung.
Betriebs- oder Sicherheitsvorfall	Ein einzelnes Ereignis, oder eine Reihe zusammenhängender Ereignisse, das/die vom Zahlungsdienstleister nicht geplant wurde/n und das/die sich negativ auf die Integrität, die Verfügbarkeit, die Vertraulichkeit, die Authentizität und/oder die Kontinuität von zahlungsbezogenen Diensten auswirkt/en oder aller Wahrscheinlichkeit nach eine solche negative Auswirkung haben wird/werden.
Geschäftsleitung	(a) Für Zahlungsdienstleister, bei denen es sich um Kreditinstitute handelt, hat dieser Begriff die gleiche Bedeutung wie in der Definition gemäß Artikel 3 Absatz 1 Nummer 9 der Richtlinie 2013/36/EU. (b) Für Zahlungsdienstleister, bei denen es sich um Zahlungsinstitute oder E-Geld-Institute handelt, umfasst dieser Begriff natürliche Personen, die Führungsaufgaben in einem Institut übernehmen und die für die Leitung des Tagesgeschäfts des Zahlungsdienstleisters verantwortlich und gegenüber dem Leitungsorgan rechenschaftspflichtig sind. (c) Für Zahlungsdienstleister gemäß den Buchstaben c, e und f von Artikel 1 Absatz 1 der Richtlinie (EU) 2015/2366 hat dieser Begriff die ihm gemäß den geltenden EU- oder nationalen Rechtsvorschriften zugewiesene Bedeutung.
Sicherheitsrelevantes Risiko	Das Risiko, das aufgrund der Unangemessenheit oder des Versagens von internen Prozessen oder aufgrund von externen Ereignissen entsteht, die negative Auswirkungen auf die Verfügbarkeit, Integrität und Vertraulichkeit der Informations- und Kommunikationstechnologie- (IKT-) Systeme und/oder der für die Erbringung von Zahlungsdiensten verwendeten Informationen haben oder haben können. Dazu gehören auch

[5] Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

	Risiken aufgrund von Cyberattacken oder unzureichender physischer Sicherheit.
Risikobereitschaft	Das Gesamtniveau und die Arten von Risiken, die ein Institut bereit ist, innerhalb seiner Risikokapazität und im Einklang mit seinem Geschäftsmodell zum Erreichen seiner strategischen Ziele einzugehen.

3. Umsetzung

Umsetzungsfrist

9. Diese Leitlinien gelten ab dem 13. Januar 2018.

4. Leitlinien

Leitlinie 1: Allgemeiner Grundsatz

1.1 Alle Zahlungsdienstleister sollten die Bestimmungen dieser Leitlinien einhalten. Die Detailgenauigkeit sollte in einem angemessenen Verhältnis zur Größe des Zahlungsdienstleisters sowie zu Art, Umfang, Komplexität und Risikobehaftung des Dienstes stehen, den der Zahlungsdienstleister erbringt oder zu erbringen beabsichtigt.

Leitlinie 2: Governance

Rahmenwerk für das Management von operationellen und sicherheitsrelevanten Risiken

2.1 Die Zahlungsdienstleister sollten ein wirksames Rahmenwerk für das Management von operationellen und sicherheitsrelevanten Risiken definieren (im Folgenden „Risikomanagementrahmenwerk“ genannt), das vom Leitungsorgan und gegebenenfalls von der Geschäftsleitung genehmigt und mindestens einmal jährlich überprüft wird. Der Schwerpunkt dieses Rahmenwerks sollte auf Sicherheitsmaßnahmen zur Minderung der operationellen und sicherheitsrelevanten Risiken liegen, und dieser sollte vollständig in die gesamten Risikomanagementprozesse des Zahlungsdienstleisters eingebunden werden.

2.2 Das Risikomanagementrahmenwerk sollte:

a) ein umfassendes Dokument zur Sicherheitsstrategie gemäß Artikel 5 Absatz 1 Buchstabe j der Richtlinie (EU) 2015/2366 enthalten;

b) mit der Risikobereitschaft des Zahlungsdienstleisters im Einklang stehen;

c) eine Definition und die Zuweisung der wesentlichen Aufgaben und Zuständigkeiten sowie die relevanten Berichtslinien enthalten, die für die Umsetzung der Sicherheitsmaßnahmen und die Steuerung der sicherheitsrelevanten und operationellen Risiken erforderlich sind;

d) die erforderlichen Verfahren und Systeme für die Identifizierung, Messung, Überwachung und Steuerung der unterschiedlichen Risiken einführen, die sich aus den zahlungsbezogenen Tätigkeiten des Zahlungsdienstleisters ergeben und denen der Zahlungsdienstleister ausgesetzt ist, einschließlich Regelungen zur Aufrechterhaltung des Geschäftsbetriebs (Business Continuity).

2.3 Die Zahlungsdienstleister sollten sicherstellen, dass das Risikomanagementrahmenwerk ordnungsgemäß dokumentiert und während seiner Umsetzung und Überwachung auf der Grundlage dokumentierter gewonnener Erkenntnisse („Lessons learned“) überarbeitet wird.

2.4 Die Zahlungsdienstleister sollten sicherstellen, dass vor jeder wesentlichen Änderung der Infrastruktur, der Prozesse oder Verfahren und nach jedem schwerwiegenden Betriebs- oder Sicherheitsvorfall, der die Sicherheit der von ihnen erbrachten Zahlungsdienste beeinträchtigt, überprüft wird, ob Änderungen oder Verbesserungen des Risikomanagementrahmenwerks unverzüglich notwendig sind oder nicht.

Risikomanagement- und Kontrollmodelle

2.5 Die Zahlungsdienstleister sollten drei wirksame Verteidigungslinien oder ein vergleichbares internes Risikomanagement- und Kontrollmodell einrichten, um die operationellen und sicherheitsrelevanten Risiken zu ermitteln und zu beherrschen. Die Zahlungsdienstleister sollten sicherstellen, dass das oben genannte interne Kontrollmodell ausreichende Befugnisse, Unabhängigkeit, Ressourcen und direkte Berichtslinien zum Leitungsorgan und gegebenenfalls zur Geschäftsleitung für die jeweiligen Verantwortlichen vorsieht.

2.6 Die Sicherheitsmaßnahmen gemäß diesen Leitlinien sollten von Prüfern, die über Fachkenntnisse in den Bereichen IT-Sicherheit und Zahlungsverkehr verfügen, geprüft werden. Die Prüfer sollten operational unabhängig sein, sowohl innerhalb der Organisation des Zahlungsdienstleisters als auch unabhängig von diesem selber. In Bezug auf die Häufigkeit und den Schwerpunkt solcher Prüfungen sollten die entsprechenden sicherheitsrelevanten Risiken berücksichtigt werden.

Auslagerung

2.7 Wenn betriebliche Aufgaben von Zahlungsdiensten, einschließlich IT-Systeme, ausgelagert werden, sollten die Zahlungsdienstleister sicherstellen, dass die Sicherheitsmaßnahmen gemäß diesen Leitlinien wirksam sind.

2.8 Die Zahlungsdienstleister sollten sicherstellen, dass angemessene und verhältnismäßige Sicherheitsziele, -maßnahmen und Leistungsziele in die mit den Dienstleistern abgeschlossenen Verträge und Dienstleistungsvereinbarungen einbezogen werden, an die die Aufgaben ausgelagert werden. Die Zahlungsdienstleister sollten überwachen und sich vergewissern, inwieweit diese Dienstleister die Sicherheitsziele, -maßnahmen und Leistungsziele erfüllen.

Leitlinie 3: Risikobewertung

Identifizierung von Aufgaben, Prozessen und IT-Betriebsmittel (Assets)

3.1 Die Zahlungsdienstleister sollten ein Verzeichnis ihrer betrieblichen Aufgaben erstellen, Schlüsselpositionen und Unterstützungsprozesse ermitteln und regelmäßig aktualisieren, um die Bedeutung jeder Aufgabe, Position und jedes Unterstützungsprozesses sowie ihre jeweiligen Abhängigkeiten in Bezug auf die operationellen und sicherheitsrelevanten Risiken darzustellen.

3.2 Die Zahlungsdienstleister sollten ein Verzeichnis ihrer IT-Betriebsmittel (Assets) ermitteln, erstellen und regelmäßig aktualisieren, das beispielsweise die IKT-Systeme, ihre Konfigurationen, die sonstigen Infrastrukturen und die Verbindungen mit anderen internen oder externen

Systemen umfasst, um die Bestände verwalten zu können, die ihre kritischen betrieblichen Aufgaben und Prozesse unterstützen.

Klassifizierung von Aufgaben, Prozessen und Datenbeständen

3.3 Die Zahlungsdienstleister sollten die ermittelten betrieblichen Aufgaben, Unterstützungsprozesse und Datenbestände im Hinblick auf ihre Kritikalität klassifizieren.

Risikobewertung in Bezug auf Aufgaben, Prozessen und IT-Betriebsmittel (Assets)

3.4 Die Zahlungsdienstleister sollten sicherstellen, dass sie Bedrohungen und Schwachstellen ständig überwachen und die Risikoszenarien, die Auswirkungen auf ihre betrieblichen Aufgaben, kritischen Prozesse und IT-Betriebsmittel haben, regelmäßig überprüfen. Im Rahmen der Verpflichtung gemäß Artikel 95 Absatz 2 der Richtlinie (EU) 2015/2366, eine aktualisierte und umfassende Risikobewertung bezüglich der operationellen und sicherheitsrelevanten Risiken im Zusammenhang mit den von den Zahlungsdienstleistern erbrachten Zahlungsdiensten sowie der Angemessenheit der zur Beherrschung dieser Risiken ergriffenen Risikominderungsmaßnahmen und Kontrollmechanismen durchzuführen und den zuständigen Behörden zur Verfügung zu stellen, sollten die Zahlungsdienstleister die Risikobewertung in Bezug auf die Aufgaben, Prozesse und IT-Betriebsmittel, die sie für die Identifizierung und Bewertung der wesentlichen operationellen und sicherheitsrelevanten Risiken ermittelt und klassifiziert haben, mindestens jährlich oder in den von der zuständigen Behörde festgelegten kürzeren Abständen durchführen und dokumentieren. Zudem sollten diese Risikobewertungen durchgeführt werden, bevor eine wesentliche Änderung der Infrastruktur, der Prozesse oder Verfahren vorgenommen wird, die die Sicherheit der Zahlungsdienste beeinträchtigt.

3.5 Auf der Grundlage der Risikobewertungen sollten die Zahlungsdienstleister feststellen, ob und in welchem Umfang Änderungen der bestehenden Sicherheitsmaßnahmen, der verwendeten Technologien und der Verfahren und angebotenen Zahlungsdienste erforderlich sind. Die Zahlungsdienstleister sollten die für die Umsetzung der Änderungen benötigte Zeit sowie die Zeit, die für die Durchführung angemessener vorläufiger Sicherheitsmaßnahmen zur Minimierung von Betriebs- oder Sicherheitsvorfällen, Betrug und möglichen Störungen bei der Erbringung der Zahlungsdienste erforderlich ist, berücksichtigen.

Leitlinie 4: Schutz

4.1 Die Zahlungsdienstleister sollten vorbeugende Sicherheitsmaßnahmen gegen die ermittelten operationellen und sicherheitsrelevanten Risiken festlegen und umsetzen. Durch diese Maßnahmen sollte ein angemessenes Sicherheitsniveau garantiert werden, das im Einklang mit den ermittelten Risiken steht.

4.2 Die Zahlungsdienstleister sollten ein gestaffeltes Sicherheitskonzept festlegen und umsetzen („Defence-in-depth“), bei dem Sicherheitsmaßnahmen (Controls) über mehrere Ebenen eingeführt werden, die Personen, Prozesse und die Technologie umfassen, wobei jede Ebene als

Sicherheitsnetz für vorhergehenden Ebenen dient. Der gestaffelte Ansatz sollte so verstanden werden, dass mehr als eine Sicherheitsmaßnahme für das gleiche Risiko festgelegt wird, wie beispielsweise das Vier-Augen-Prinzip, die Zwei-Faktor-Authentifizierung, Netzwerksegmentierung und mehrfache Firewalls.

4.3 Die Zahlungsdienstleister sollten die Vertraulichkeit, Integrität und Verfügbarkeit ihrer wesentlichen logischen und physischen Datenbestände, Ressourcen und sensiblen Zahlungsdaten ihrer Zahlungsdienstnutzer sicherstellen, unabhängig davon, ob diese sich im Ruhezustand befinden, übermittelt oder verwendet werden. Wenn die Daten personenbezogene Daten umfassen, sollten Maßnahmen gemäß der Verordnung (EU) 2016/679 [6] oder gegebenenfalls gemäß der Verordnung (EG) 45/2001 [7] umgesetzt werden.

4.4 Die Zahlungsdienstleister sollten fortlaufend feststellen, ob Änderungen des bestehenden operativen Umfelds Auswirkungen auf die bestehenden Sicherheitsmaßnahmen haben oder weitere Maßnahmen zur Minderung des betreffenden Risikos erforderlich machen. Diese Änderungen sollten einen Teil des formalen Änderungsmanagementprozesses des Zahlungsdienstleisters darstellen, durch den sichergestellt werden sollte, dass alle Änderungen ordnungsgemäß geplant, getestet, dokumentiert und zugelassen werden. Auf der Grundlage der festgestellten Sicherheitsrisiken und der vorgenommenen Änderungen sollten Tests durchgeführt werden, um Szenarien bezüglich relevanter und bekannter potenzieller Angriffe einzubeziehen.

4.5 Bei der Planung, Entwicklung und Erbringung von Zahlungsdiensten sollten die Zahlungsdienstleister sicherstellen, dass der Grundsatz der Aufgabentrennung und das Prinzip der geringsten Privilegien („Least Privilege“-Prinzip) angewandt werden. Die Zahlungsdienstleister sollten besonders auf die Trennung von IT-Umgebungen achten, insbesondere in Bezug auf die Entwicklungs-, Test- und Produktionsumgebungen.

Integrität und Vertraulichkeit der Daten und Systeme

4.6 Bei der Planung, Entwicklung und Erbringung von Zahlungsdiensten sollten die Zahlungsdienstleister sicherstellen, dass die Erfassung, das Routing, die Verarbeitung, Speicherung und/oder Archivierung sowie die Darstellung von sensiblen Zahlungsdaten der Zahlungsdienstnutzer angemessen, notwendig und auf das für die Erbringung des Zahlungsdienstes notwendige Maß beschränkt sind.

4.7 Die Zahlungsdienstleister sollten regelmäßig überprüfen, ob die für die Erbringung von Zahlungsdiensten verwendete Software, einschließlich der zahlungsbezogenen Software der Nutzer, auf dem aktuellen Stand ist und ob kritische Sicherheitspatches verwendet werden. Die

[6] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

[7] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

Zahlungsdienstleister sollten sicherstellen, dass Mechanismen zur Überprüfung der Integrität der Software, Firmware und Informationen über ihre Zahlungsdienste vorhanden sind.

Physische Sicherheit

4.8 Die Zahlungsdienstleister sollten angemessene physische Sicherheitsmaßnahmen eingerichtet haben, insbesondere Maßnahmen zum Schutz der sensiblen Zahlungsdaten der Zahlungsdienstnutzer sowie der IKT-Systeme, die für die Erbringung der Zahlungsdienste verwendet werden.

Zugriffskontrolle

4.9 Der physische und logische Zugriff auf IKT-Systeme sollte nur berechtigten Personen gestattet sein. Die Berechtigung sollte in Übereinstimmung mit den Aufgaben und Verantwortlichkeiten der Mitarbeiter erteilt und auf Personen beschränkt werden, die entsprechend geschult wurden und beaufsichtigt werden. Die Zahlungsdienstleister sollten Sicherheitsmaßnahmen und Kontrollen einrichten, die den Zugriff auf die IKT-Systeme zuverlässig auf die Personen beschränken, bei denen dies aufgrund von betrieblichen Anforderungen gerechtfertigt ist. Der elektronische Zugriff auf Daten und Systeme durch Anwendungen sollte auf das für die Erbringung des entsprechenden Dienstes erforderliche Mindestmaß beschränkt werden.

4.10 Die Zahlungsdienstleister sollten strenge Sicherheitsmaßnahmen und Kontrollen über privilegierten Zugriff auf ein System einrichten, indem Mitarbeiter, die weiterreichende Zugriffsrechte auf das System haben, stark beschränkt und genau überwacht werden. Es sollten Sicherheitsmaßnahmen und Kontrollen wie der rollenbasierte Zugang, Protokollierung und Überprüfung der Tätigkeiten von privilegierten Nutzern im System, starke Authentifizierung und Überwachung von Unregelmäßigkeiten eingeführt werden. Die Zahlungsdienstleister sollten die Zugriffsrechte zu Datenbeständen und ihren Unterstützungssystemen so regeln, dass nur Personen, die Kenntnis von den entsprechenden Informationen haben müssen, der Zugriff gestattet wird. Die Zugriffsrechte sollten regelmäßig überprüft werden.

4.11 Gemäß Leitlinie 3.1 und Leitlinie 3.2 sowie unbeschadet der Aufbewahrungspflichten gemäß den EU- und nationalen Rechtsvorschriften sollten die Zugriffsprotokolle für einen Zeitraum aufbewahrt werden, der hinsichtlich der Kritikalität der ermittelten betrieblichen Aufgaben, der Unterstützungsprozesse und Datenbestände angemessen ist. Die Zahlungsdienstleister sollten diese Informationen nutzen, um die Identifizierung und Untersuchung von ungewöhnlichen Aktivitäten, die hinsichtlich der Erbringung von Zahlungsdiensten festgestellt wurden, zu vereinfachen.

4.12 Um eine sichere Kommunikation zu gewährleisten und die Risiken zu reduzieren, sollte ein administrativer Fernzugriff auf kritische IKT-Komponenten nur Personen gestattet werden, die Kenntnis von den entsprechenden Informationen haben müssen; in diesem Fall müssen starke Authentifizierungslösungen verwendet werden.

4.13 Durch den Betrieb von Produkten, Instrumenten und Verfahren im Zusammenhang mit den Verfahren der Zugriffskontrolle sollte verhindert werden, dass die Verfahren der Zugriffskontrolle beeinträchtigt oder umgangen werden. Dies umfasst die Registrierung, die Lieferung, den Widerruf in Bezug auf und die Rücknahme von entsprechenden Produkten, Instrumenten und Verfahren.

Leitlinie 5: Erkennung

Kontinuierliche Überwachung und Erkennung

5.1 Die Zahlungsdienstleister sollten Prozesse und Kapazitäten zur kontinuierlichen Überwachung der betrieblichen Aufgaben, Unterstützungsprozesse und Datenbestände einrichten und implementieren, um ungewöhnliche Aktivitäten bei der Erbringung von Zahlungsdiensten zu erkennen. Im Rahmen dieser kontinuierlichen Überwachung sollten Zahlungsdienstleister über angemessene und effektive Fähigkeiten zur Erkennung physischen oder logischen Eindringens sowie zur Erkennung von Verstößen gegen die Regelungen bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit von Datenbeständen, die bei der Erbringung von Zahlungsdiensten verwendet werden, verfügen.

5.2 Die kontinuierlichen Überwachungs- und Erkennungsprozesse sollten umfassen:

a) relevante interne und externe Faktoren, einschließlich betrieblicher und IKT-Verwaltungsfunktionen;

b) Transaktionen zur Erkennung von missbräuchlichem Zugriff durch Dienstleister oder sonstiger Stellen; und

c) potenzielle interne und externe Gefahren.

5.3 Die Zahlungsdienstleister sollten Erkennungsmaßnahmen zur Feststellung möglicher Datenlecks, schädlichem Code und sonstiger Sicherheitsrisiken sowie von öffentlich bekannten Schwachstellen von Software und Hardware einführen, und sie sollten nach entsprechenden Sicherheits-Updates suchen.

Überwachung und Meldung von Betriebs- oder Sicherheitsvorfällen

5.4 Die Zahlungsdienstleister sollten geeignete Kriterien und Grenzwerte für die Klassifizierung eines Vorfalls als Betriebs- oder Sicherheitsvorfall gemäß der Definition im Abschnitt „Begriffsbestimmungen“ sowie Frühwarnindikatoren festlegen, durch die die Zahlungsdienstleister gewarnt werden, so dass ihnen die frühzeitige Erkennung von Betriebs- oder Sicherheitsvorfällen ermöglicht wird.

5.5 Die Zahlungsdienstleister sollten geeignete Prozesse und Organisationsstrukturen einrichten, um die einheitliche und integrierte Überwachung, Behandlung und Nachverfolgung von Betriebs- und Sicherheitsvorfällen zu gewährleisten.

5.6 Die Zahlungsdienstleister sollten ein Verfahren für die Meldung solcher Betriebs- oder Sicherheitsvorfälle sowie von sicherheitsbezogenen Kundenbeschwerden an die Geschäftsleitung einführen.

Leitlinie 6: Geschäftsfortführung

6.1 Die Zahlungsdienstleister sollten zuverlässige Maßnahmen zur Geschäftsfortführung einführen, um ihre Fähigkeit zu verbessern, Zahlungsdienste kontinuierlich zu erbringen und Verluste im Fall von schwerwiegenden Betriebsstörungen zu begrenzen.

6.2 Bei der Einführung der Maßnahmen zur Geschäftsfortführung sollten die Zahlungsdienstleister sorgfältig analysieren, inwieweit sie durch schwerwiegende Betriebsstörungen gefährdet sind, und sie sollten deren potenzielle Auswirkungen anhand von internen und/oder externen Daten und einer Szenario-Analyse quantitativ und qualitativ bewerten. Auf der Grundlage der ermittelten und klassifizierten kritischen Aufgaben, Prozesse, Systeme, Transaktionen und Abhängigkeiten gemäß Leitlinie 3.1 bis Leitlinie 3.3 sollten die Zahlungsdienstleister die Maßnahmen zur Geschäftsfortführung priorisieren, wobei sie einen risikobasierten Ansatz anwenden sollten, der sich auf die gemäß Leitlinie 3 durchgeführte Risikobewertung stützen kann. Abhängig von dem Geschäftsmodell des Zahlungsdienstleisters kann dies beispielsweise die weitere Verarbeitung von kritischen Transaktionen vereinfachen, während die Arbeiten zur Behebung des Vorfalls fortgeführt werden.

6.3 Auf der Grundlage der gemäß der Leitlinie 6.2 durchgeführten Analyse sollten die Zahlungsdienstleister:

a) Pläne zur Geschäftsfortführung einführen, durch die angemessen auf Notfälle reagiert werden kann und durch die die wesentlichen Geschäftstätigkeiten aufrecht erhalten werden können; und

b) Risikominderungsmaßnahmen einführen, die für den Fall der Beendigung der eigenen Zahlungsdienste und der Beendigung von bestehenden Verträgen ergriffen werden, um negative Auswirkungen auf Zahlungssysteme und auf die Zahlungsdienstnutzer zu vermeiden und um die Durchführung von noch nicht ausgeführten Zahlungsvorgängen sicherzustellen.

Szenariobasierte Planung der Geschäftsfortführung

6.4 Die Zahlungsdienstleister sollten eine Reihe verschiedener Szenarien berücksichtigen, einschließlich extremer, jedoch denkbarer Szenarien, denen sie ausgesetzt sein können, und sie sollten die möglichen Auswirkungen dieser Szenarien bewerten.

6.5 Auf der Grundlage der gemäß der Leitlinie 6.2 durchgeführten Analyse und denkbarer Szenarien gemäß der Leitlinie 6.4 sollten die Zahlungsdienstleister Notfall- und Wiederherstellungspläne ausarbeiten, die:

a) sich auf die Auswirkungen auf die Ausführung der kritischen Aufgaben, Prozesse, Systeme, Transaktionen und Abhängigkeiten konzentrieren;

b) dokumentiert werden und den Geschäfts- und Unterstützungseinheiten zur Verfügung gestellt werden und im Notfall leicht zugänglich sind; und

c) in Übereinstimmung mit den bei Tests gewonnenen Erkenntnissen, mit festgestellten neuen Risiken und Bedrohungen sowie mit geänderten Wiederherstellungszielen und -prioritäten aktualisiert werden.

Testen von Plänen zur Geschäftsfortführung

6.6 Die Zahlungsdienstleister sollten ihre Pläne zur Geschäftsfortführung testen und sicherstellen, dass der Betrieb ihrer kritischen Aufgaben, Prozesse, Systeme, Transaktionen und Abhängigkeiten mindestens jährlich getestet wird. Die Pläne sollten den Schutz und gegebenenfalls die Wiederherstellung der Integrität und Verfügbarkeit ihrer Geschäftsvorgänge sowie die Wahrung der Vertraulichkeit ihrer Datenbestände unterstützen.

6.7 Die Pläne sollten mindestens jährlich und gegebenenfalls nach Änderungen der Systeme und Prozesse aktualisiert werden; diese Aktualisierung sollte sich auf Testergebnisse, aktuelle Informationen über Gefahren, Informationsaustausch und aus früheren Vorfällen gewonnene Erkenntnisse sowie auf sich ändernde Wiederherstellungsziele und eine Analyse von noch nicht eingetretenen betrieblich und technisch denkbaren Szenarien stützen. Bei der Einführung ihrer Pläne zur Geschäftsfortführung sollten die Zahlungsdienstleister sich mit den relevanten internen und externen Stakeholdern beraten und abstimmen.

6.8 Beim Testihrer Pläne zur Geschäftsfortführung sollten die Zahlungsdienstleister:

a) einen angemessenen Satz von Szenarien einbeziehen, wie in der Leitlinie 6.4 angegeben;

b) die Tests so gestalten, dass die Annahmen, auf die sich die Pläne zur Geschäftsfortführung stützen, einschließlich der Unternehmenssteuerungsregelungen (Governance) und der Krisenkommunikationspläne, hinterfragt werden; und

c) Verfahren zur Überprüfung der Fähigkeit ihrer Mitarbeiter und Prozesse, angemessen auf die oben genannten Szenarien zu reagieren, in die Prüfung einbeziehen.

6.9 Die Zahlungsdienstleister sollten die Wirksamkeit ihrer Pläne zur Geschäftsfortführung im Krisenfall regelmäßig überprüfen und alle Probleme oder Fehler, die sich aus diesen Tests ergeben, dokumentieren und analysieren.

Krisenkommunikation

6.10 Bei einer Störung oder einem Notfall und während der Umsetzung der Pläne zur Geschäftsfortführung sollten die Zahlungsdienstleister sicherstellen, dass sie wirksame Maßnahmen zur Krisenkommunikation eingeführt haben, so dass alle relevanten internen und

externen Stakeholder, einschließlich externer Dienstleister, rechtzeitig und angemessen informiert werden.

Leitlinie 7: Testen von Sicherheitsmaßnahmen

7.1 Die Zahlungsdienstleister sollten eine Testumgebung einrichten und implementieren, in der die Robustheit und die Wirksamkeit der Sicherheitsmaßnahmen überprüft wird, und sie sollten sicherstellen, dass die Testumgebung neue Bedrohungen und Schwachstellen berücksichtigen kann, die im Rahmen von Tätigkeiten zur Risikoüberwachung ermittelt wurden.

7.2 Die Zahlungsdienstleister sollten sicherstellen, dass Tests bei Änderungen an der Infrastruktur, der Prozesse oder Verfahren sowie bei Änderungen, die infolge von schwerwiegenden Betriebs- oder Sicherheitsvorfällen vorgenommen wurden, durchgeführt werden.

7.3 Die Testumgebung sollte zudem die Sicherheitsmaßnahmen umfassen, die für (i) Zahlungsterminals und -Geräte, die für die Erbringung von Zahlungsdiensten verwendet werden, (ii) Zahlungsterminals und -geräte, die für die Authentifizierung der Zahlungsdienstnutzer verwendet werden, und (iii) Geräte und Software, die ein Zahlungsdienstleister dem Zahlungsdienstnutzer zur Verfügung stellt, um einen Authentifizierungscode zu generieren/erhalten, relevant sind.

7.4 Die Testumgebung sollte sicherstellen, dass Tests:

a) im Rahmen eines formalen Änderungsmanagementprozesses des Zahlungsdienstleisters durchgeführt werden, um ihre Robustheit und Wirksamkeit sicherzustellen;

b) von unabhängigen Testern durchgeführt werden, die über ausreichende Kenntnisse, Kompetenzen und Fachkenntnisse bezüglich Tests von Sicherheitsmaßnahmen für Zahlungsdienste verfügen und die nicht an der Entwicklung der Sicherheitsmaßnahmen für die entsprechenden Zahlungsdienste oder -systeme, die geprüft werden sollen, beteiligt sind; dies gilt zumindest für abschließende Tests, bevor die Sicherheitsmaßnahmen eingeführt werden; und

c) Anfälligkeitsprüfungen und Penetrationstests umfassen, die dem Risikograd entsprechen, der für Zahlungsdienste ermittelt wurde.

7.5 Die Zahlungsdienstleister sollten fortlaufende und wiederholte Tests bezüglich der Sicherheitsmaßnahmen für ihre Zahlungsdienste durchführen. Für Systeme, die für die Erbringung ihrer Zahlungsdienste von wesentlicher Bedeutung sind (wie in der Leitlinie 3.2 beschrieben), sollten diese Prüfungen mindestens einmal jährlich durchgeführt werden. Tests von Systemen, die nicht von wesentlicher Bedeutung sind, sollten regelmäßig im Rahmen eines risikobasierten Ansatzes, jedoch mindestens alle drei Jahre durchgeführt werden.

7.6 Die Zahlungsdienstleister sollten die Ergebnisse der durchgeführten Tests prüfen und bewerten und für den Fall von kritischen System ihre Sicherheitsmaßnahmen unverzüglich entsprechend aktualisieren.

Leitlinie 8: Situationsbewusstsein und kontinuierliches Lernen

Gefahrenlage und Situationsbewusstsein

8.1 Die Zahlungsdienstleister sollten Prozesse und Organisationsstrukturen einrichten und implementieren, um sicherheitsrelevante und operationelle Gefahren, die ihre Fähigkeit zur Erbringung der Zahlungsdienste beeinträchtigen könnten, zu ermitteln und ständig zu überwachen.

8.2 Die Zahlungsdienstleister sollten Betriebs- oder Sicherheitsvorfälle, die innerhalb und/oder außerhalb der Organisation ermittelt wurden oder eingetreten sind, analysieren. Die Zahlungsdienstleister sollten die aus diesen Analysen gewonnenen wesentlichen Erkenntnisse berücksichtigen und die Sicherheitsmaßnahmen entsprechend aktualisieren.

8.3 Die Zahlungsdienstleister sollten technologische Entwicklungen aktiv überwachen, um sicherzustellen, dass sie Kenntnis von sicherheitsrelevanten Risiken haben.

Schulungsprogramme und Programme zur Förderung des Sicherheitsbewusstseins

8.4 Die Zahlungsdienstleister sollten ein Schulungsprogramm für alle Mitarbeiter einrichten, um sicherzustellen, dass sie für die Durchführung ihrer Aufgaben und Verantwortlichkeiten in Übereinstimmung mit den einschlägigen Sicherheitsrichtlinien und -verfahren geschult sind, so dass menschliches Versagen, Diebstahl, Betrug, Missbrauch oder Verlust reduziert werden. Die Zahlungsdienstleister sollten sicherstellen, dass die Mitarbeiter gemäß dem Schulungsprogramm mindestens jährlich, und wenn nötig häufiger, Schulungen erhalten.

8.5 Die Zahlungsdienstleister sollten sicherstellen, dass die Mitarbeiter, die Schlüsselpositionen gemäß der Leitlinie 3.1 einnehmen, jährlich, oder wenn nötig häufiger, eine gezielte Schulung zur Informationssicherheit erhalten.

8.6 Die Zahlungsdienstleister sollten regelmäßige Programme zur Förderung des Sicherheitsbewusstseins einrichten und durchführen, um ihre Mitarbeiter zu schulen und auf Risiken im Zusammenhang mit der Informationssicherheit hinzuweisen. Im Rahmen dieser Programme sollten die Mitarbeiter des Zahlungsdienstleisters verpflichtet sein, alle ungewöhnlichen Aktivitäten und Vorfälle zu melden.

Leitlinie 9: Pflege der Kundenbeziehungen mit Zahlungsdienstnutzern

Bewusstsein der Zahlungsdienstnutzer bezüglich sicherheitsrelevanter Risiken und Maßnahmen zur Risikominderung

9.1 Die Zahlungsdienstleister sollten Prozesse einrichten und implementieren, durch die das Bewusstsein der Zahlungsdienstnutzer in Bezug auf sicherheitsrelevante Risiken in Verbindung mit den Zahlungsdiensten verbessert wird, indem die Zahlungsdienstnutzer unterstützt und beraten werden.

9.2 Die den Zahlungsdienstnutzern angebotene Unterstützung und Beratung sollten im Hinblick auf neue Gefahren und Schwachstellen aktualisiert werden, und Änderungen sollten den Zahlungsdienstnutzern mitgeteilt werden.

9.3 Wenn die Produktfunktionalität dies zulässt, sollten die Zahlungsdienstleister den Zahlungsdienstnutzern gestatten, bestimmte Zahlungsfunktionen in Verbindung mit den Zahlungsdiensten, die die Zahlungsdienstleister den Zahlungsdienstnutzern anbieten, zu deaktivieren.

9.4 Wenn der Zahlungsdienstleister gemäß Artikel 68 Absatz 1 der Richtlinie (EU) 2015/2366 Ausgabenobergrenzen für Zahlungsvorgänge, die durch dieses Zahlungsinstrument durchgeführt werden, mit dem Zahler vereinbart, sollte der Zahlungsdienstleister dem Zahler die Möglichkeit gewähren, diese Obergrenzen bis zum vereinbarten Höchstbetrag der Obergrenzen anzupassen.

9.5 Die Zahlungsdienstleister sollten den Zahlungsdienstnutzern die Möglichkeit anbieten, Warnungen bezüglich veranlasster oder fehlgeschlagener Versuche zur Auslösung von Zahlungsvorgängen zu erhalten, so dass sie eine betrügerische oder missbräuchliche Nutzung ihres Kontos erkennen können.

9.6 Die Zahlungsdienstleister sollten die Zahlungsdienstnutzer über Aktualisierungen der Sicherheitsverfahren informieren, die in Bezug auf die Erbringung von Zahlungsdiensten Auswirkungen auf die Zahlungsdienstnutzer haben.

9.7 Die Zahlungsdienstleister sollten die Zahlungsdienstnutzer in Bezug auf alle Fragen, Unterstützungsanfragen, Benachrichtigungen über Unregelmäßigkeiten oder alle sicherheitsrelevanten Fragen hinsichtlich der Zahlungsdienste unterstützen. Die Zahlungsdienstnutzer sollten angemessen darüber informiert werden, wie sie diese Unterstützung erhalten können.