EBA/GL/2014/12_Rev1

19. Dezember 2014

Leitlinien

zur Sicherheit von Internetzahlungen

Inhaltsverzeichnis

Leitlinien zur Sicherheit von Internetzahlungen

Status dieser Leitlinien

Das vorliegende Dokument enthält Leitlinien, die gemäß Artikel 16 der 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 („EBA-Verordnung“) erlassen werden. Gemäß Artikel 16 Absatz 3 der EBA-Verordnung müssen die zuständigen Behörden und die Finanzinstitute alle erforderlichen Anstrengungen unternehmen, um den Leitlinien nachzukommen.

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. Die EBA erwartet folglich von allen zuständigen Behörden und Finanzinstituten, an die diese Leitlinien gerichtet sind, dass sie diesen nachkommen. Dazu sollten die zuständigen Behörden 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

Nach Artikel 16 Absatz 3 der EBA-Verordnung müssen die zuständigen Behörden der EBA bis zum 5. Mai 2015 mitteilen, ob sie diesen Leitlinien nachkommen oder nachzukommen beabsichtigen, oder die Gründe nennen, warum sie dies nicht tun. Geht innerhalb der genannten Frist keine Meldung ein, geht die EBA davon aus, dass die zuständige Behörde den Anforderungen nicht nachkommt. Die Meldungen sind unter Verwendung des in Abschnitt 5 enthaltenen Formulars mit dem Betreff „EBA/REC/2014/12” an compliance@eba.europa.eu zu senden. Die Meldungen sollten durch Personen erfolgen, die befugt sind, entsprechende Meldungen im Auftrag ihrer Behörde zu übermitteln.

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

Titel I – Anwendungsbereich und Begriffsbestimmungen

Anwendungsbereich

1. Diese Leitlinien legen eine Reihe von Mindestanforderungen im Bereich der Sicherheit von Internetzahlungen fest. Die Leitlinien basieren auf den Vorschriften der Richtlinie 2007/64/EG[1] („Zahlungsdiensterichtlinie“, „PSD“) über die Informationspflichten für Zahlungsdienste sowie die Pflichten von Zahlungsdienstleistern bei der Erbringung von Zahlungsdiensten. Überdies schreibt Artikel 10 Absatz 4 der PSD vor, dass Zahlungsinstitute über eine solide Unternehmenssteuerung sowie angemessene interne Kontrollmechanismen verfügen müssen.

2. Die Leitlinien gelten für die Erbringung von über das Internet angebotenen Zahlungsdiensten durch Zahlungsdienstleister, die in Artikel 1 der PSD definiert sind.

3. Die Leitlinien richten sich an Finanzinstitute im Sinne des Artikels 4 Absatz 1 der Verordnung (EU) Nr. 1093/2010 sowie an die zuständigen Behörden im Sinne des Artikels 4 Absatz 2 der Verordnung (EU) Nr. 1093/2010. Die zuständigen Behörden in den 28 Mitgliedstaaten der Europäischen Union sollten sicherstellen, dass die in Artikel 1 der PSD definierten Zahlungsdienstleister unter ihrer Aufsicht diese Leitlinien anwenden.

4. Außerdem können die zuständigen Behörden beschließen, Zahlungsdienstleister aufzufordern, ihre Einhaltung der Leitlinien gegenüber der zuständigen Behörde anzuzeigen.

5. Die Gültigkeit der „Recommendations for the security of itnernet payments““ der Europäischen Zentralbank (nachfolgend „der Bericht“[2]) bleibt von diesen Leitlinien unberührt. Insbesondere stellt der Bericht weiterhin das Dokument dar, gegen welches Zentralbanken in ihrer Aufsichtsfunktion für Zahlungssysteme und -instrumente die Einhaltung der Vorschriften bezüglich der Sicherheit von Internetzahlungen prüfen sollten.

6. Die Leitlinien stellen Mindesterwartungen dar. Sie lassen die Verantwortung der Zahlungsdienstleister unberührt, die mit ihren Zahlungsvorgängen verbundenen Risiken zu überwachen und einzuschätzen, ihre eigenen ausführlichen Sicherheitsrichtlinien zu erarbeiten und angemessene Sicherheits-, Notfall- und Vorfallmanagementmaßnahmen sowie Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs umzusetzen, welche für die den erbrachten Zahlungsdiensten innewohnenden Risiken angemessen sind.

7. Zweck dieser Leitlinien ist die Definition von gemeinsamen Mindestanforderungen für die unten aufgeführten Internetzahlungsdienste, unabhängig vom verwendeten Zugangsgerät:

[1] 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.

[2] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html.

- [Karten] die Ausführung von Kartenzahlungen im Internet einschließlich virtueller Kartenzahlungen, sowie die Registrierung von Kartenzahlungsdaten zur Nutzung in „elektronischen Geldbörsen“,

- [Überweisungen] die Durchführung von Überweisungen im Internet,

- [elektronische Einzugsermächtigung] die Erteilung und Änderung elektronischer Einzugsermächtigungen,

- [E-Geld] die Übertragung von elektronischem Geld zwischen zwei E-Geld-Konten über das Internet.

8. Geben die Leitlinien ein Ergebnis vor, kann dieses durch verschiedene Mittel erreicht werden. Neben den im Folgenden angeführten Anforderungen geben diese Leitlinien auch Beispiele für bewährte Vorgehensweisen (im Anhang 1), zu deren Befolgung Zahlungsdienstleister angehalten, jedoch nicht verpflichtet werden.

9. Wird die Bereitstellung von Zahlungsdiensten und -instrumenten über ein Zahlungssystem (z. B. Kartenzahlungssysteme, Überweisungsverfahren, Lastschriftverfahren usw.) angeboten, sollten die zuständigen Behörden und die betreffende Zentralbank mit Aufsichtsfunktion über Zahlungsinstrumente in Zusammenarbeit sicherstellen, dass die Leitlinien von den Akteuren, die für das Funktionieren des Systems bzw. Verfahrens zuständig sind, einheitlich angewandt werden.

10. Anbieter von Integrationslösungen für Bezahlseiten[3], die Zahlungsauslösedienste anbieten, gelten entweder als Internetzahlungsdienste abrechnende Stellen (und somit als Zahlungsdienstleister) oder als externe technische Dienstleister der betreffenden Systeme bzw. Verfahren oder Zahlungsdienstleister. Im letzteren Fall sollten die Anbieter der Integrationslösungen vertraglich zur Einhaltung der Leitlinien verpflichtet werden.

11. Vom Anwendungsbereich der Leitlinien ausgeschlossen sind:

- sonstige durch einen Zahlungsdienstleister über seine Zahlungsseite erbrachten Internetdienste (z. B. Online-Brokerage, Online-Verträge),

- Zahlungen, die per Post, über telefonische Bestellung, Voicemail oder mittels SMS-basierter Technologie angewiesen werden,

- mobile Zahlungen mit Ausnahme von browserbasierten Zahlungen,

- Überweisungen, bei denen ein Dritter auf das Zahlungskonto des Kunden zugreift,

[3] Anbieter von Integrationslösungen für Bezahlseiten stellen dem Zahlungsempfänger (d. h. dem E-Händler) eine standardisierte Schnittstelle zu den durch den Zahlungsdienstleister erbrachten Zahlungsauslösediensten zur Verfügung.

- Zahlungsvorgänge, die durch ein Unternehmen über dedizierte Netzwerke vorgenommen werden,

- Kartenzahlungen mittels anonymer und nicht aufladbarer physischer oder virtueller Karten auf Guthabenbasis, bei denen keine dauerhafte Beziehung zwischen dem Aussteller und dem Karteninhaber besteht,

- Clearing und Verrechnung von Zahlungsvorgängen.

Begriffsbestimmungen

12. Im Sinne dieser Leitlinien und zusätzlich zu den in der PSD dargelegten Definitionen gelten die folgenden Begriffsbestimmungen:

- *Authentifizierung* bezeichnet ein Verfahren, das dem Zahlungsdienstleister die Überprüfung der Identität eines Kunden ermöglicht.

- *Starke Kundenauthentifizierung* ist im Sinne dieser Leitlinien ein Verfahren, das auf der Verwendung zweier oder mehrerer der folgenden Elemente basiert, die als Wissen, Besitz und Inhärenz kategorisiert werden: i) etwas, das nur der Nutzer weiß, z. B. ein statisches Passwort, ein Code, eine persönliche Identifikationsnummer, ii) etwas, das nur der Nutzer besitzt, z. B. ein Token, eine Smartcard, ein Mobiltelefon, iii) eine Eigenschaft des Nutzers, z. B. ein biometrisches Merkmal, etwa ein Fingerabdruck. Außerdem müssen die gewählten Elemente unabhängig voneinander sein, d. h. die Verletzung eines Elements darf keinen Einfluss auf das andere bzw. die anderen haben. Mindestens eines der Elemente sollte nicht wiederverwendbar und nicht reproduzierbar (die Inhärenz ausgenommen) sein und nicht heimlich über das Internet entwendet werden können. Das starke Authentifizierungsverfahren sollte so gestaltet sein, dass die Vertraulichkeit der Authentifizierungsdaten gewahrt bleibt.

- *Autorisierung* bezeichnet ein Verfahren, das prüft, ob ein Kunde oder Zahlungsdienstleister zur Durchführung einer bestimmten Handlung berechtigt ist, z. B. zum Transfer von Geldbeträgen oder für den Zugriff auf sensible Daten.

- *Berechtigungsnachweis* bezeichnet die Informationen – im Allgemeinen vertraulicher Natur – die zu Authentifzierungszwecken von einem Kunden oder einem Zahlungsdienstleister bereitgestellt werden. Ein Berechtigungsnachweis kann auch den Besitz eines physischen Hilfsmittels bedeuten, welches diese Informationen enthält (z. B. Einmalpasswort-Generatoren, Smartcards), oder etwas, das der Nutzer sich merkt oder das eine Eigenschaft des Nutzers darstellt (z. B. biometrische Merkmale).

- *Schwerwiegender Zahlungssicherheitsvorfall* bezeichnet einen Vorfall, der wesentliche Auswirkungen auf die Sicherheit, Integrität oder Kontinuität der Zahlungssysteme des Zahlungsdienstleisters und/oder die Sicherheit sensibler Zahlungsdaten oder -mittel hat oder haben könnte. Bei der Beurteilung der Wesentlichkeit sollte die Anzahl der

potenziell betroffenen Kunden, der Risikobetrag und die Folgen für andere Zahlungsdienstleister oder sonstige Zahlungsinfrastrukturen berücksichtigt werden.

- *Transaktionsrisikoanalyse* bezeichnet die Bewertung des mit einer bestimmten Transaktion verbundenen Risikos unter Berücksichtigung von Kriterien wie zum Beispiel Zahlungsmuster (Verhalten) des Kunden, den Wert der betreffenden Transaktion, die Art des Produkts und das Profil des Zahlungsempfängers.

- *Virtuelle Karten* bezeichnet ein kartenbasiertes Zahlungsverfahren, bei dem eine alternative vorübergehende Kartennummer mit reduzierter Geltungsdauer, begrenzter Nutzung und einer vorab festgelegten Ausgabenobergrenze generiert wird, die für Internetkäufe eingesetzt werden kann.

- *Elektronische Geldbörsen* bezeichnet Verfahren, die es einem Kunden ermöglichen, Daten in Verbindung zu einem oder mehreren Zahlungsinstrumenten zu registrieren, um Zahlungen an verschiedene E-Händler auszuführen.

Titel II – Leitlinien zur Sicherheit von Internetzahlungen

Allgemeines Kontroll- und Sicherheitsumfeld

Governance

1. Zahlungsdienstleister sollten formelle Sicherheitsrichtlinien für Internetzahlungsdienste umsetzen und diese regelmäßig überprüfen.

   1.1 Die Sicherheitsrichtlinien sollten ordnungsgemäß dokumentiert und (im Einklang mit Leitlinie 2.4) regelmäßig überprüft und von der Geschäftsleitung genehmigt werden. Sie sollten Sicherheitsziele und die Risikobereitschaft festlegen.

   1.2 Die Sicherheitsrichtlinien sollten Rollen und Zuständigkeiten, einschließlich der Risikomanagement-Funktion mit einer direkten Berichtspflicht gegenüber der Vorstandsebene, und die Berichtspflichten für die erbrachten Internetzahlungsdienste festlegen, einschließlich der Verwaltung sensibler Zahlungsdaten in Bezug auf Risikobewertung, -kontrolle und -minderung.

Risikobewertung

2. Zahlungsdienstleister sollten gründliche Risikobewertungen in Bezug auf die Sicherheit von Internetzahlungen und damit verbundene Dienste durchführen und dokumentieren, sowohl vor Einrichtung dieses Dienstes bzw. dieser Dienste als auch in regelmäßigen Abständen danach.

   2.1 Über ihre Risikomanagement-Funktion sollten Zahlungsdienstleister ausführliche Risikobewertungen für Internetzahlungen und damit verbundene Dienste ausführen und dokumentieren. Zahlungsdienstleister sollten die Ergebnisse der laufenden Überwachung von Sicherheitsbedrohungen für die Internetzahlungsdienste, die sie anbieten oder anzubieten planen, berücksichtigen und dabei i) die von ihnen eingesetzten technologischen Lösungen, ii) die an externe Anbieter ausgelagerten Dienste sowie iii) die technische Umgebung der Kunden beachten. Zahlungsdienstleister sollten die Risiken, die sowohl auf ihrer Seite[4] als auch auf der Seite ihrer Kunden mit den gewählten Technologieplattformen, Anwendungsarchitekturen, Programmiertechniken und Prozeduren verbunden sind,[5] sowie die Ergebnisse des Überwachungsprozesses für Sicherheitsvorfälle (siehe Leitlinie 3) berücksichtigen.

[4] Zum Beispiel die Anfälligkeit des Systems gegenüber Session-Hijacking beim Bezahlvorgang, SQL-Injection, Cross-Site-Scripting, Pufferüberläufen usw.

[5] Zum Beispiel Risiken, die mit der Nutzung von Multimedia-Anwendungen, Browser-Plug-ins, Frames, externen Links usw. verbunden sind.

2.2 Auf dieser Grundlage sollten Zahlungsdienstleister festlegen, ob und in welchem Umfang Änderungen an bestehenden Sicherheitsmaßnahmen, eingesetzten Technologien und angebotenen Verfahren oder Diensten erforderlich sein könnten. Zahlungsdienstleister sollten die zur Umsetzung der Änderungen (einschließlich der Einführung beim Kunden) erforderliche Zeit berücksichtigen und angemessene einstweilige Maßnahmen zur Minimierung von Sicherheitsvorfällen, Betrug und potenziellen Störungen ergreifen.

2.3 Die Bewertung der Risiken sollte der Notwendigkeit des Schutzes und der Sicherung sensibler Zahlungsdaten Rechnung tragen.

2.4 Zahlungsdienstleister sollten nach schwerwiegenden Vorfällen mit Auswirkungen auf ihre Dienste, vor einer wesentlichen Änderung an Infrastruktur oder Verfahren und bei Erkennung neuer Bedrohungen durch die Risikoüberwachung eine Überprüfung der Risikoszenarien und der bestehenden Sicherheitsmaßnahmen vornehmen. Zusätzlich sollte mindestens einmal jährlich eine allgemeine Überprüfung der Risikobewertung erfolgen. Die Ergebnisse der Risikobewertungen und Überprüfungen sollten der Geschäftsleitung zur Genehmigung vorgelegt werden.

Vorfallüberwachung und Berichterstattung

3. Zahlungsdienstleister sollten eine einheitliche und integrierte Überwachung, Bearbeitung und Nachbereitung von Sicherheitsvorfällen, einschließlich sicherheitsbezogener Kundenbeschwerden, sicherstellen. Zahlungsdienstleister sollten ein Verfahren zur Meldung solcher Vorfälle an die Geschäftsleistung und – bei schwerwiegenden Zahlungssicherheitsvorfällen – an die zuständigen Behörden einrichten.

3.1 Zahlungsdienstleister sollten über ein Verfahren zur Überwachung, Bearbeitung und Nachbereitung von Sicherheitsvorfällen und sicherheitsbezogenen Kundenbeschwerden sowie zur Meldung solcher Vorfälle an die Geschäftsleistung verfügen.

3.2 Zahlungsdienstleister sollten über ein Verfahren verfügen, um bei schwerwiegenden Zahlungssicherheitsvorfällen in Bezug auf die erbrachten Zahlungsdienste gegebenenfalls sofort die zuständigen Behörden (d. h. Aufsichts- und Datenschutzbehörden) zu informieren.

3.3 Zahlungsdienstleister sollten über ein Verfahren verfügen, das ihnen die Zusammenarbeit bei schwerwiegenden Zahlungssicherheitsvorfällen, einschließlich Datenschutzverletzungen, mit den zuständigen Strafverfolgungsbehörden ermöglicht.

3.4 Abrechnende Zahlungsdienstleister sollten E-Händler, die sensible Zahlungsdaten speichern, verarbeiten oder übermitteln, vertraglich zur Zusammenarbeit bei schwerwiegenden Zahlungssicherheitsvorfällen, einschließlich Datenschutzverletzungen, mit den abrechnenden Zahlungsdienstleistern selbst und

den zuständigen Strafverfolgungsbehörden verpflichten. Erhält ein Zahlungsdienstleister Kenntnis davon, dass ein E-Händler nicht vertragsgemäß kooperiert, sollte er Maßnahmen ergreifen, um diese vertragliche Verpflichtung durchzusetzen, oder den Vertrag kündigen.

Risikokontrolle und -minderung

4. Im Einklang mit ihren jeweiligen Sicherheitsrichtlinien sollten Zahlungsdienstleister Sicherheitsmaßnahmen zur Minderung festgestellter Risiken ergreifen. Diese Maßnahmen sollten mehrere Sicherheitsebenen umfassen, so dass das Versagen einer Sicherheitsebene durch die nächste Sicherheitsebene aufgefangen wird („gestaffeltes Sicherheitskonzept“).

4.1 Bei der Gestaltung, Entwicklung und Bereitstellung von Internetzahlungsdiensten sollten Zahlungsdienstleister der angemessenen Trennung von Aufgaben in den Informationstechnologieumgebungen (IT-Umgebungen) (z. B. der Entwicklungs-, Test- und Produktionsumgebung) und der ordnungsgemäßen Umsetzung des Prinzips des geringsten Zugriffsrechts besondere Aufmerksamkeit widmen, die als Grundlage eines soliden Identitäts- und Zugriffsmanagements dienen.[6]

4.2 Zahlungsdienstleister sollten über geeignete Sicherheitslösungen verfügen, um Netzwerke, Websites, Server und Kommunikationsverbindungen gegen Missbrauch oder Angriffe zu schützen. Zahlungsdienstleister sollten ihre Server von allen überflüssigen Funktionen befreien, um sie zu schützen (zu härten) und die Schwachstellen von gefährdeten Anwendungen zu beseitigen oder zu reduzieren. Der Zugriff auf benötigte Daten und Ressourcen durch verschiedene Anwendungen sollte gemäß dem Prinzip des geringsten Zugriffsrechts auf ein Mindestmaß beschränkt werden. Um die Verwendung „gefälschter“ Websites (die rechtmäßige Websites von Zahlungsdienstleistern nachahmen) einzuschränken, sollten Transaktions-Websites, die Internetzahlungsdienste anbieten, durch auf den Namen des Zahlungsdienstleisters ausgestellte Extended-Validation-Zertifikate oder sonstige Authentifizierungsmethoden ähnlicher Art identifiziert werden.

4.3 Zahlungsdienstleister sollten über geeignete Verfahren zur Überwachung, Verfolgung und Zugangsbeschränkung von i) sensiblen Zahlungsdaten und ii) kritischen logischen und physischen Ressourcen wie Netzwerken, Systemen, Datenbanken, Sicherheitsmodulen usw. verfügen. Zahlungsdienstleister sollten zweckdienliche Protokolle und Überwachungsinformationen erzeugen, speichern und auswerten.

[6] „Jedes Programm und jeder berechtigte Nutzer des Systems sollte mit dem geringsten Maß an Zugriffsrechten arbeiten, das zur Erfüllung der Aufgabe erforderlich ist.“ Siehe Saltzer, J. H. (1974), „Schutz und Kontrolle des Informationsaustauschs in Multics (Protection and the Control of Information Sharing in Multics)“, Communications of the ACM, Bd. 17, Nr. 7, S. 388.

4.4 Bei der Gestaltung,[7] Entwicklung und Bereitstellung von Internetzahlungsdiensten sollten Zahlungsdienstleister sicherstellen, dass die Datenminimierung [8] einen wesentlichen Bestandteil der Kernfunktionalität bildet: Die Erfassung, Weiterleitung, Verarbeitung, Speicherung und/oder Archivierung sowie die Visualisierung sensibler Zahlungsdaten sollte auf ein absolutes Mindestmaß beschränkt werden.

4.5 Die Sicherheitsmaßnahmen für Internetzahlungsdienste sollten unter der Aufsicht der Risikomanagementfunktion getestet werden, um ihre Robustheit und Wirksamkeit sicherzustellen. Sämtliche Änderungen sollten einen formalen Änderungsmanagementprozess durchlaufen, um sicherzustellen, dass alle Änderungen ordnungsgemäß geplant, getestet, dokumentiert und genehmigt werden. Auf Basis der vorgenommenen Änderungen und der beobachteten Sicherheitsbedrohungen sollten die Tests regelmäßig wiederholt werden und Szenarien für relevante und bekannte potenzielle Angriffe beinhalten.

4.6 Die Sicherheitsmaßnahmen des Zahlungsdienstleisters für Internetzahlungsdienste sollten in regelmäßigen Abständen überprüft werden, um ihre Robustheit und Wirksamkeit sicherzustellen. Die Umsetzung und Funktionsweise der Internetzahlungsdienste sollten ebenfalls überprüft werden. Die Häufigkeit und die Schwerpunkte dieser Überprüfungen sollten den jeweiligen Sicherheitsrisiken Rechnung tragen und in einem angemessenen Verhältnis zu ihnen stehen. Die Überprüfungen sollten von zuverlässigen und unabhängigen (internen oder externen) Sachverständigen durchgeführt werden. Diese sollten in keiner Weise an der Entwicklung, Umsetzung oder dem operativen Management der erbrachten Internetzahlungsdienste beteiligt sein.

4.7 Wenn Zahlungsdienstleister Funktionen auslagern, die die Sicherheit der Internetzahlungsdienste betreffen, sollte der entsprechende Vertrag Bestimmungen enthalten, die die Einhaltung der in diesen Leitlinien dargelegten Grundsätze und Leitlinien fordern.

4.8 Zahlungsdienstleister, die Abrechnungsdienste anbieten, sollten E-Händler, die mit sensiblen Zahlungsdaten umgehen (d. h. diese speichern, verarbeiten oder übermitteln), vertraglich dazu verpflichten, im Einklang mit den Leitlinien 4.1 bis 4.7 Sicherheitsmaßnahmen in ihrer IT-Infrastruktur umzusetzen, um einen Diebstahl dieser sensiblen Zahlungsdaten über ihre Systeme zu verhindern. Erlangt ein Zahlungsdienstleister Kenntnis davon, dass ein E-Händler die erforderlichen Sicherheitsmaßnahmen nicht eingerichtet hat, sollte er Maßnahmen ergreifen, um diese vertragliche Verpflichtung durchzusetzen, oder den Vertrag kündigen.

[7] Eingebauter Datenschutz.

[8] Datenminimierung bezeichnet den Grundsatz, die Erhebung personenbezogener Daten auf das für die Erfüllung einer bestimmten Funktion erforderliche Mindestmaß zu beschränken.

Rückverfolgbarkeit

5. Zahlungsdienstleister sollten über Verfahren verfügen, die sicherstellen, dass sämtliche Transaktionen sowie der Prozessablauf elektronischer Einzugsermächtigungen angemessen zurückverfolgt werden.

5.1 Zahlungsdienstleister sollten sicherstellen, dass ihr Dienst Sicherheitsmechanismen zur ausführlichen Protokollierung der Daten zu Transaktionen und elektronischen Einzugsermächtigungen umfasst, einschließlich fortlaufender Transaktionsnummern, Zeitstempel für Transaktionsdaten, Parametrisierungsänderungen und Zugriffe auf Daten zu Transaktionen und elektronischen Einzugsermächtigungen.

5.2 Zahlungsdienstleister sollten Protokolldateien verwenden, um die Rückverfolgung jeglicher Ergänzung, Änderung oder Löschung von Daten zu Transaktionen und elektronischen Einzugsermächtigungen zu ermöglichen.

5.3 Zahlungsdienstleister sollten die Daten zu Transaktionen und elektronischen Einzugsermächtigungen abfragen und analysieren und sicherstellen, dass sie über Tools zur Auswertung der Protokolldateien verfügen. Die entsprechenden Anwendungen sollten nur befugten Mitarbeitern zur Verfügung stehen.

Spezifische Kontroll- und Sicherheitsmaßnahmen für Internetzahlungen

Erstidentifikation des Kunden, Information

6. Kunden sollten im Einklang mit den europäischen Geldwäsche-Gesetzen[9] ordnungsgemäß identifiziert werden und ihre Bereitschaft bestätigen, die Dienste für Internetzahlungen zu verwenden, bevor ihnen Zugang zu diesen Diensten gewährt wird. Zahlungsdienstleister sollten Kunden in angemessener Weise regelmäßig, vorab und gegebenenfalls kurzfristig über die Voraussetzungen (z. B. Geräte, Verfahren) für die Durchführung sicherer Internetzahlungsvorgänge und die damit verbundenen Risiken informieren.

6.1 Zahlungsdienstleister sollten sicherstellen, dass die Identität des Kunden unter Einhaltung der entsprechenden Sorgfaltspflichten festgestellt wurde und dass der Kunde geeignete Ausweisdokumente [10] sowie damit verbundene Informationen vorgelegt hat, bevor ihm Zugang zu den Internetzahlungsdiensten gewährt wird.[11]

[9] Zum Beispiel Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung. ABl. L 309 vom 25.11.2005, S. 15-36. Siehe auch Richtlinie 2006/70/EG der Kommission vom 1. August 2006 mit Durchführungsbestimmungen für die Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates hinsichtlich der Begriffsbestimmung von „politisch exponierten Personen“ und der Festlegung der technischen Kriterien für vereinfachte Sorgfaltspflichten sowie für die Befreiung in Fällen, in denen nur gelegentlich oder in sehr eingeschränktem Umfang Finanzgeschäfte getätigt werden. ABl. L 214 vom 4.8.2006, S. 29-34.

[10] Zum Beispiel den Pass, den nationalen Personalausweis oder die fortgeschrittene elektronische Signatur.

[11] Das Kundenidentifikationsverfahren berührt keine Ausnahmen, die in bestehenden Geldwäsche-Gesetzen festgelegt sind. Unter der Voraussetzung, dass bereits eine Kundenidentifikation erfolgt ist, z. B. für andere bestehende

6.2 Zahlungsdienstleister sollten sicherstellen, dass die dem Kunden bereitgestellten Vorabinformationen [12] bestimmte Einzelheiten zu den Internetzahlungsdiensten beinhalten. Zu diesen Einzelheiten sollten, soweit erforderlich, folgende Angaben gehören:

- klare Informationen zu allen Anforderungen im Sinne kundenseitiger Ausstattung, Software oder sonstiger erforderlicher Tools (z. B. Virenschutzprogramme, Firewalls),
- Leitlinien für die ordnungsgemäße und sichere Nutzung des personalisierten Sicherheits-Berechtigungsnachweises,
- eine Schritt-für-Schritt-Beschreibung des Verfahrens, mit dem der Kunde einen Zahlungsvorgang durchführt und autorisiert und/oder Informationen einholt, einschließlich einer Beschreibung der Folgen jeder Handlung,
- Leitlinien für die ordnungsgemäße und sichere Nutzung der gesamten dem Kunden zur Verfügung gestellten Hardware und Software,
- die Verfahren, die im Fall des Verlusts oder des Diebstahls des personalisierten Sicherheits-Berechtigungsnachweises oder der Kundenhardware oder -software zur Anmeldung oder zur Durchführung von Transaktionen einzuhalten sind,
- die Verfahren, die bei Entdeckung und Verdacht von Missbrauch einzuhalten sind,
- eine Beschreibung der jeweiligen Zuständigkeiten und Haftungen des Zahlungsdienstleisters und des Kunden hinsichtlich der Nutzung des Internetzahlungsdienstes.

6.3 Zahlungsdienstleister sollten sicherstellen, dass im Rahmenvertrag mit dem Kunden angegeben ist, dass der Zahlungsdienstleister eine bestimmte Transaktion oder das Zahlungsinstrument [13] aufgrund von Sicherheitsbedenken sperren kann. Der Rahmenvertrag sollte die Methode und die Bedingungen der Benachrichtigung des Kunden sowie Möglichkeiten darlegen, wie der Kunde im Einklang mit der PSD die Aufhebung der Sperre für den Internetzahlungsvorgang bzw. -dienst beim Zahlungsdienstleister beantragen kann.

Zahlungsdienste oder bei der Eröffnung eines Kontos, müssen Zahlungsdienstleister kein gesondertes Kundenidentifikationsverfahren für die Internetzahlungsdienste durchführen.

[12] Diese Information ergänzt Artikel 42 der PSD, der die Informationen anführt, die der Zahlungsdienstleister dem Zahlungsdienstnutzer vor Abschluss eines Vertrags über die Erbringung von Zahlungsdiensten mitteilen muss.

[13] Siehe Artikel 55 der PSD zur Begrenzung der Nutzung des Zahlungsinstruments.

Starke Kundenauthentifizierung

7. Die Auslösung von Internetzahlungen und der Zugang zu sensiblen Zahlungsdaten sollten durch eine starke Kundenauthentifizierung geschützt sein. Zahlungsdienstleister sollten über ein Verfahren für die in den vorliegenden Leitlinien definierte starke Kundenauthentifizierung verfügen.

7.1 [Überweisungen/elektronische Einzugsermächtigung/E-Geld] Zahlungsdienstleister sollten eine starke Kundenauthentifizierung für die Autorisierung von Internetzahlungsvorgängen durch den Kunden (einschließlich Sammelüberweisungen) und die Erteilung und Änderung elektronischer Einzugsermächtigungen durchführen. Jedoch sollten Zahlungsdienstleister in Erwägung ziehen, für folgende Transaktionen alternative Mechanismen zur Kundenauthentifizierung einzurichten:

- Zahlungsausgänge zugunsten vertrauenswürdiger Begünstigter, die auf für diesen Kunden im Voraus erstellten weißen Listen verzeichnet sind,
- Transaktionen zwischen zwei Konten desselben Kunden bei demselben Zahlungsdienstleister,
- Transfers innerhalb desselben Zahlungsdienstleisters, die durch eine Transaktionsrisikoanalyse gerechtfertigt werden,
- die in der PSD erwähnten Kleinbetragszahlungen.[14]

7.2 Für eine Gewährung des Zugangs zu sensiblen Zahlungsdaten und die Änderung dieser Daten (einschließlich der Erstellung und Änderung von weißen Listen) ist eine starke Kundenauthentifizierung erforderlich. Bietet ein Zahlungsdienstleister reine Beratungsdienste an, bei denen keine sensiblen Kunden- oder Zahlungsdaten wie Zahlungskartendaten angezeigt werden, die einfach zu Betrugszwecken missbraucht werden könnten, kann der Zahlungsdienstleister seine Authentifizierungsanforderungen auf der Grundlage seiner Risikobewertung anpassen.

7.3 [Karten] Bei Kartentransaktionen sollten alle Karten ausstellenden Zahlungsdienstleister die starke Authentifizierung des Karteninhabers unterstützen. Alle ausgestellten Karten müssen aus technischer Sicht bereit (registriert) sein, um mit starker Authentifizierung verwendet zu werden.

7.4 [Karten] Zahlungsdienstleister, die Abrechnungsdienste anbieten, sollten Technologien unterstützen, die dem Aussteller die Durchführung einer starken Authentifizierung des Karteninhabers für das Kartenzahlungssystem ermöglichen, an dem der Abrechnungsdienstleister teilnimmt.

[14] Siehe Definition von Kleinbetragszahlungsinstrumenten in Artikel 34 Absatz 1 und Artikel 53 Absatz 1 der PSD.

7.5 [Karten] Zahlungsdienstleister, die Abrechnungsdienste anbieten, sollten von ihrem E-Händler die Unterstützung von Technologien verlangen, die dem Aussteller die Durchführung einer starken Authentifizierung des Karteninhabers für Kartentransaktionen über das Internet ermöglichen. Die Nutzung alternativer Authentifizierungsmaßnahmen könnte für im Vorfeld identifizierte Kategorien von Transaktionen mit niedrigem Risiko, z. B. auf der Grundlage einer Transaktionsrisikoanalyse, oder für die in der PSD erwähnten Kleinbetragszahlungen in Betracht gezogen werden.

7.6 [Karten] Für die durch den Dienst akzeptierten Kartenzahlungssysteme sollten Anbieter von elektronischen Geldbörsen von dem Aussteller eine starke Authentifizierung verlangen, wenn der rechtmäßige Inhaber die Kartendaten erstmals registriert.

7.7 Anbieter von elektronischen Geldbörsen sollten eine starke Kundenauthentifizierung unterstützen, wenn sich Kunden bei den Zahlungsdiensten elektronischer Geldbörsen anmelden oder Kartentransaktionen über das Internet durchführen. Die Nutzung alternativer Authentifizierungsmaßnahmen könnte für im Vorfeld identifizierte Kategorien von Transaktionen mit niedrigem Risiko, z. B. auf der Grundlage einer Transaktionsrisikoanalyse, oder für die in der PSD erwähnten Kleinbetragszahlungen in Betracht gezogen werden.

7.8 [Karten] Bei virtuellen Karten sollte die Erstregistrierung in einer sicheren und vertrauenswürdigen Umgebung stattfinden.[15] Die starke Kundenauthentifizierung sollte für den Prozess der Datengenerierung für die virtuelle Karte verpflichtend sein, falls die Karte in der Internetumgebung ausgestellt wird.

7.9 Zahlungsdienstleister sollten eine ordnungsgemäße wechselseitige Authentifizierung sicherstellen, wenn sie mit E-Händlern zum Zwecke der Auslösung von Internetzahlungen und des Zugangs zu sensiblen Zahlungsdaten kommunizieren.

Anmeldung bei Authentifizierungstools und deren Bereitstellung und/oder an den Kunden gelieferte Software

8. Zahlungsdienstleister sollten sicherstellen, dass die Kundenanmeldung bei Authentifizierungstools, die zur Nutzung der Internetzahlungsdienste erforderlich sind, sowie deren Erstbereitstellung und/oder die Lieferung von Zahlungssoftware an Kunden auf eine sichere Weise durchgeführt wird.

[15] Zu den Umgebungen unter der Verantwortung des Zahlungsdienstleisters, in denen eine angemessene Authentifizierung des Kunden und des den Dienst anbietenden Zahlungsdienstleisters sowie der Schutz vertraulicher/sensibler Daten gewährleistet sind, gehören: i) die Geschäftsräume des Zahlungsdienstleisters, ii) Internetbanking- oder sonstige sichere Websites, z. B. wenn der GA vergleichbare Sicherheitsfunktionen wie unter anderem in Leitlinie 4 definiert bietet, oder iii) Dienste von multifunktionalen Bankautomaten. (Im Fall von Bankautomaten ist eine starke Kundenauthentifizierung erforderlich. Diese erfolgt üblicherweise mittels Chip und PIN oder Chip und biometrische Merkmale.)

8.1 Die Anmeldung bei Authentifizierungstools und deren Bereitstellung und/oder an den Kunden gelieferte Zahlungssoftware sollten die folgenden Anforderungen erfüllen:

- Die damit zusammenhängenden Verfahren sollten in einer sicheren und vertrauenswürdigen Umgebung unter Berücksichtigung möglicher Risiken durchgeführt werden, die von Geräten außerhalb der Kontrolle des Zahlungsdienstleisters ausgehen.

- Für die Lieferung des personalisierten Sicherheits-Berechtigungsnachweises, der Zahlungssoftware und aller personalisierten, für Internetzahlungen relevanten Geräte sollten wirksame und sichere Verfahren eingerichtet sein. Über das Internet gelieferte Software sollte außerdem durch den Zahlungsdienstleister digital signiert werden, um den Kunden die Überprüfung ihrer Authentizität und Unversehrtheit zu ermöglichen.

- [Karten] Bei Kartentransaktionen sollte der Kunde die Option haben, sich unabhängig von einem bestimmten Internetkauf für eine starke Authentifizierung zu registrieren. Wird eine Aktivierung während des Online-Einkaufs angeboten, sollte der Kunde hierfür in eine sichere und vertrauenswürdige Umgebung weitergeleitet werden.

8.2 [Karten] Aussteller sollten Karteninhaber aktiv zu einer Anmeldung für die starke Authentifizierung ermutigen und ihren Karteninhabern nur in Ausnahmefällen und bei einer begrenzten Anzahl von Fällen gestatten, die Anmeldung zu umgehen, wenn das mit dieser bestimmten Kartentransaktion verbundene Risiko dies rechtfertigt.

Anmeldeversuche, Sitzungs-Timeout, Gültigkeit von Authentifizierungen

9. Zahlungsdienstleister sollten die Anzahl der Anmelde- oder Authentifizierungsversuche begrenzen, Regeln für das Sitzungs-Timeout bei Internetzahlungsdiensten festlegen und die Gültigkeit von Authentifizierungen zeitlich befristen.

9.1 Wird zum Zwecke der Authentifizierung ein Einmalpasswort verwendet, sollten Zahlungsdienstleister sicherstellen, dass die Gültigkeitsdauer dieser Passwörter sich auf den absolut erforderlichen Mindestzeitraum beschränkt.

9.2 Zahlungsdienstleister sollten die Höchstanzahl fehlgeschlagener Anmelde- oder Authentifizierungsversuche festlegen, nach welcher der Zugang zum Internetzahlungsdienst (vorübergehend oder dauerhaft) gesperrt wird. Sie sollten über ein sicheres Verfahren zur Wiederaktivierung gesperrter Internetzahlungsdienste verfügen.

9.3 Zahlungsdienstleister sollten den Höchstzeitraum festlegen, nach dem inaktive Sitzungen bei Internetzahlungsdiensten automatisch beendet werden.

Transaktionsüberwachung

10. Vor der endgültigen Autorisierung durch den Zahlungsdienstleister sollten Transaktionsüberwachungsmechanismen mit dem Ziel der Verhinderung, Erkennung und Sperrung betrügerischer Zahlungsvorgänge ausgeführt werden. Verdächtige Transaktionen oder solche mit hohem Risiko sollten einem Prüfungs- und Bewertungsprozess unterzogen werden. Entsprechende Mechanismen zur Sicherheitsüberwachung und Autorisierung sollten auch für die Erteilung elektronischer Einzugsermächtigungen eingerichtet sein.

10.1 Zahlungsdienstleister sollten Betrugserkennungs- und -verhütungssysteme verwenden, um verdächtige Transaktionen zu identifizieren, bevor sie die Transaktionen oder elektronischen Einzugsermächtigungen endgültig autorisieren. Solche Systeme sollten zum Beispiel auf parametrisierten Regeln (wie etwa schwarze Listen mit missbräuchlich verwendeten oder gestohlenen Kartendaten) basieren und ungewöhnliche Verhaltensmuster des Kunden oder des Zugangsgerätes des Kunden überwachen (wie zum Beispiel die Änderung einer Internetprotokolladresse (IP-Adresse)[16] oder des IP-Bereichs während der Sitzung bei Internetzahlungsdiensten, die mitunter durch die Überprüfung der Geolokation der IP-Adresse aufgedeckt wird,[17] untypische Kategorien eines E-Händlers für einen bestimmten Kunden oder ungewöhnliche Transaktionsdaten usw.). Solche Systeme sollten Anzeichen für eine Infizierung durch Schadprogramme während einer Sitzung (z. B. durch die Prüfung, ob der Nutzer ein Skript oder ein Mensch ist) und bekannte Betrugsszenarien erkennen können. Unter Einhaltung der maßgeblichen Datenschutzgesetze sollten der Umfang, die Komplexität und die Anpassbarkeit der Überwachungslösungen den Ergebnissen der Risikobewertung entsprechen.

10.2 Abrechnende Zahlungsdienstleister sollten über Betrugsermittlungs- und -verhütungssysteme verfügen, um die Tätigkeiten der E-Händler zu überwachen.

10.3 Zahlungsdienstleister sollten alle Prüfungs- und Bewertungsprozessen bei Transaktionen innerhalb einer angemessenen Frist durchführen, damit die Auslösung und/oder Ausführung des betreffenden Zahlungsdienstes nicht unnötig verzögert werden.

10.4 Entschließt der Zahlungsdienstleister im Einklang mit seinen Risikoleitlinien, einen als potenziell betrügerisch erkannten Zahlungsvorgang zu sperren, sollte er diese Sperre für eine möglichst kurze Zeit aufrechterhalten, bis die Sicherheitsprobleme beseitigt sind.

[16] Eine IP-Adresse ist ein eindeutiger Zahlencode, durch den jeder mit dem Internet verbundene Computer identifiziert wird.

[17] Durch die Ermittlung der „Geo-IP“ kann geprüft werden, ob das erteilende Land mit der IP-Adresse übereinstimmt, von der aus der Nutzer die Transaktion auslöst.

Schutz sensibler Zahlungsdaten

11. Sensible Zahlungsdaten sollten bei ihrer Speicherung, Verarbeitung und Übermittlung geschützt werden.

11.1 Alle zur Identifizierung und Authentifizierung von Kunden verwendeten Daten (z. B. bei der Anmeldung, bei der Auslösung von Internetzahlungen und bei Erteilung, Änderung und Widerruf der elektronischen Einzugsermächtigung), sowie die Kundenschnittstelle (Website des Zahlungsdienstleisters oder des E-Händlers) sollten angemessen gegen Diebstahl und unbefugten Zugriff oder Änderungen gesichert werden.

11.2 Zahlungsdienstleister sollten sicherstellen, dass beim Austausch sensibler Zahlungsdaten über das Internet während der gesamten Kommunikationssitzung eine sichere Ende-zu-Ende-Verschlüsselung[18] zwischen den kommunizierenden Parteien eingesetzt wird, um die Vertraulichkeit und Integrität der Daten zu wahren. Zu diesem Zweck sollten starke und weithin anerkannte Verschlüsselungstechniken verwendet werden.

11.3 Zahlungsdienstleister, die Abrechnungsdienste anbieten, sollten ihre E-Händler ermutigen, keine sensiblen Zahlungsdaten zu speichern. Falls E-Händler mit sensiblen Zahlungsdaten umgehen, d. h. diese speichern, verarbeiten oder übermitteln, sollten die betreffenden Zahlungsdienstleister die E-Händler vertraglich zur Einrichtung der zum Schutz dieser Daten erforderlichen Maßnahmen verpflichten. Zahlungsdienstleister sollten regelmäßige Prüfungen durchführen. Erhält ein Zahlungsdienstleister Kenntnis davon, dass ein mit sensiblen Zahlungsdaten umgehender E-Händler nicht über die erforderlichen Sicherheitsmaßnahmen verfügt, sollte der Zahlungsdienstleister Maßnahmen ergreifen, um diese vertragliche Verpflichtung durchzusetzen, oder den Vertrag kündigen.

[18] Bei Ende-zu-Ende-Verschlüsselung erfolgt die Verschlüsselung innerhalb oder beim Ausgangsendsystem und die entsprechende Entschlüsselung ausschließlich innerhalb oder beim Zielendsystem. ETSI EN 302 109 V1.1.1. (2003-06).

Kundenaufklärung, -information und -kommunikation

Kundeninformation und -kommunikation

12. Zahlungsdienstleister sollten Kunden Unterstützung und Orientierung bei der sicheren Nutzung der Internetzahlungsdienste bieten. Zahlungsdienstleister sollten mit ihren Kunden auf eine Weise kommunizieren, die den Kunden die Authentizität der empfangenen Nachrichten bestätigt.

12.1 Zahlungsdienstleister sollten mindestens einen gesicherten Kanal[19] für die laufende Kommunikation mit Kunden über die korrekte, sichere Nutzung der Internetzahlungsdienste bereitstellen. Zahlungsdienstleister sollten die Kunden über diesen Kanal informieren und erläutern, dass jede Nachricht im Namen des Zahlungsdienstleisters, die in Bezug auf die korrekte, sichere Nutzung der Internetzahlungsdienste über andere Wege versandt wird, nicht zuverlässig ist. Der Zahlungsdienstleister sollte Folgendes erläutern:

- das Verfahren, über das Kunden dem Zahlungsdienstleister (als solche im Verdacht stehende) betrügerische Zahlungen, verdächtige Vorfälle oder Unregelmäßigkeiten während der Sitzung bei Internetzahlungsdiensten und/oder mögliche Versuche von Social Engineering[20] melden können,

- die nächsten Schritte, d. h. wie der Zahlungsdienstleister dem Kunden antworten wird,

- wie der Zahlungsdienstleister den Kunden über (potenziell) betrügerische Transaktionen oder ihre Nichtauslösung in Kenntnis setzen oder ihn vor Angriffen (z. B. Phishing-E-Mails) warnen wird.

12.2 Zahlungsdienstleister sollten ihre Kunden über den sicheren Kanal über Aktualisierungen der Sicherheitsverfahren für Internetzahlungsdienste auf dem Laufenden halten. Alle Warnungen bezüglich erheblicher neu entstehender Risiken (z. B. Warnungen über Social Engineering) sollten ebenfalls über den gesicherten Kanal erfolgen.

12.3 Zahlungsdienstleister sollten für sämtliche Fragen, Beschwerden, Support-Anfragen und Meldungen über Unregelmäßigkeiten oder Vorfälle im Zusammenhang mit Internetzahlungen und damit verbundenen Diensten einen Kundendienst einrichten und Kunden sollten in geeigneter Weise informiert werden, wie sie diesen Kundendienst in Anspruch nehmen können.

[19] Wie zum Beispiel ein spezielles Postfach auf der Website des Zahlungsdienstleisters oder eine gesicherte Website.

[20] In diesem Zusammenhang werden mit Social Engineering Techniken bezeichnet, die zur Manipulation von Menschen eingesetzt werden, um Informationen zu erlangen (z. B. über E-Mail oder Telefon), oder das Abrufen von Informationen in sozialen Netzwerken zu Betrugszwecken oder um sich unbefugt Zugriff zu einem Computer oder Netzwerk zu verschaffen.

12.4 Zahlungsdienstleister sollten Programme zur Kundeninformation und -aufklärung einrichten, die sicherstellen sollen, dass die Kunden als Mindestanforderung die Notwendigkeit folgender Vorkehrungen verstehen:

- den Schutz ihrer Passwörter, Sicherheits-Tokens, persönlicher Angaben und sonstiger vertraulicher Daten,
- die ordnungsgemäße Verwaltung der Sicherheit ihres persönlichen Geräts (z. B. ihres Computers) durch die Installierung und Aktualisierung von Sicherheitskomponenten (Virenschutzprogramme, Firewalls, Sicherheits-Patches),
- die Berücksichtigung der erheblichen Bedrohungen und Risiken, die mit dem Herunterladen von Software über das Internet verbunden sind, wenn der Kunde nicht mit hinreichender Sicherheit feststellen kann, ob die Software echt ist und nicht manipuliert wurde,
- die Nutzung der Original-Website des Zahlungsdienstleisters für Internetzahlungen.

12.5 Abrechnende Zahlungsdienstleister sollten E-Händler verpflichten, dass sie Zahlungsprozesse klar vom Online-Shop trennen, um Kunden die Feststellung zu erleichtern, wann sie mit dem Zahlungsdienstleister und nicht dem Zahlungsempfänger kommunizieren (z. B. durch Weiterleitung des Kunden und Öffnen eines neuen Fensters, so dass der Zahlungsprozess nicht innerhalb eines Frames des E-Händlers angezeigt wird).

Mitteilungen, Festlegung von Grenzwerten

13. Zahlungsdienstleister sollten Grenzwerte für Internetzahlungsdienste festlegen und könnten ihren Kunden innerhalb dieser Grenzen Möglichkeiten zur weitergehenden Risikobegrenzung bieten. Sie können außerdem Warnungs- und Kundenprofilmanagementdienste erbringen.

13.1 Vor der Erbringung von Internetzahlungsdiensten für einen Kunden sollten Zahlungsdienstleister die für diese Dienste geltenden Grenzwerte[21] festlegen (z. B. einen Höchstbetrag für jede Einzelzahlung oder einen kumulativen Betrag für einen bestimmten Zeitraum) und ihre Kunden entsprechend informieren. Zahlungsdienstleister sollten ihren Kunden die Deaktivierung der Internetzahlungsfunktion gestatten.

[21] Solche Grenzwerte können entweder global (d. h. für alle Zahlungsinstrumente, die Internetzahlungen ermöglichen) oder individuell gelten.

Zugang des Kunden zu Informationen über den Status der Zahlungsauslösung und -ausführung

14. Zahlungsdienstleister sollten die Zahlungsauslösung ihren Kunden gegenüber bestätigen und den Kunden rechtzeitig die Informationen zur Verfügung stellen, die zur Überprüfung erforderlich sind, ob ein Zahlungsvorgang korrekt ausgelöst und/oder ausgeführt wurde.

14.1 [Überweisungen/elektronische Einzugsermächtigung] Zahlungsdienstleister sollten Kunden eine Vorrichtung bieten, durch die sie jederzeit[22] und beinahe in Echtzeit den Status der Ausführung von Transaktionen sowie Kontostände in einer sicheren und vertrauenswürdigen Umgebung prüfen können.

14.2 Alle ausführlichen elektronischen Kontoauszüge sollten in einer sicheren und vertrauenswürdigen Umgebung bereitgestellt werden. Wenn Zahlungsdienstleister Kunden über einen alternativen Kanal, zum Beispiel über SMS, E-Mail oder per Anschreiben darüber informieren, dass elektronische Kontoauszüge bereitstehen (z. B. regelmäßig, wenn ein periodischer Kontoauszug ausgestellt wurde, oder ad hoc nach der Ausführung einer Transaktion), sollten diese Mitteilungen keine sensiblen Zahlungsdaten enthalten bzw. falls solche Daten enthalten sind, sollten diese maskiert und wirksam geschützt sein.

Titel III – Schlussbestimmungen und Umsetzung

15. Die vorliegenden Leitlinien gelten ab dem 01.08.2015.

[22] Ausgenommen ist die Nichtverfügbarkeit der Einrichtung in Ausnahmefällen aus Gründen der technischen Wartung oder infolge schwerwiegender Vorfälle.

Anhang 1: Beispiele für bewährte Vorgehensweisen

Zusätzlich zu den oben dargelegten Anforderungen beschreiben diese Leitlinien einige bewährte Vorgehensweisen, zu deren Übernahme Zahlungsdienstleister und die relevanten Marktteilnehmer angehalten, jedoch nicht verpflichtet sind. Zur besseren Übersicht erfolgt eine ausdrückliche Nennung der Kapitel, für die diese bewährten Vorgehensweisen gelten.

Allgemeines Kontroll- und Sicherheitsumfeld

Governance

BV 1: Die Sicherheitsrichtlinien könnten in einem eigens dafür bestimmten Dokument festgelegt werden.

Risikokontrolle und -minderung

BV 2: Zahlungsdienstleister könnten Sicherheits-Tools (z. B. ordnungsgemäß gesicherte Geräte und/oder kundenspezifisch angepasste Browser) zur Verfügung stellen, um die Kundenschnittstelle gegen rechtswidrige Nutzung oder Angriffe (z. B. „Man-in-the-Browser"-Angriffe) zu schützen.

Rückverfolgbarkeit

BV 3: Zahlungsdienstleister, die Abrechnungsdienste anbieten, könnten E-Händler, die Zahlungsinformationen speichern, vertraglich zur Einrichtung angemessener Prozesse zur Unterstützung der Rückverfolgbarkeit verpflichten.

Spezifische Kontroll- und Sicherheitsmaßnahmen für Internetzahlungen

Erstidentifikation des Kunden, Information

BV 4: Der Kunde könnte einen gesonderten Dienstleistungsvertrag über die Durchführung von Internetzahlungsvorgängen unterzeichnen, anstatt dass die Bedingungen in einen allgemeineren Dienstleistungsvertrag mit dem Zahlungsdienstleister aufgenommen werden.

BV 5: Zahlungsdienstleister könnten auch sicherstellen, dass die Kunden laufend oder gegebenenfalls ad hoc und über angemessene Wege (z. B. Faltblätter, Webseiten) klare und direkten Anweisungen erhalten, die ihre Verantwortung in Bezug auf die sichere Nutzung des Dienstes erläutern.

Starke Kundenauthentifizierung

BV 6: [Karten] E-Händler könnten die starke Authentifizierung des Karteninhabers durch den Aussteller in Kartentransaktionen über das Internet unterstützen.

BV 7: Zum Zwecke der einfacheren Handhabung für den Kunden könnten Zahlungsdienstleister in Erwägung ziehen, für die starke Kundenauthentifizierung ein einziges Tool für alle

Internetzahlungsdienste zu verwenden. Dies könnte die Akzeptanz der Lösung bei den Kunden verbessern und die ordnungsgemäße Nutzung erleichtern.

BV 8: Die starke Kundenauthentifizierung könnte Elemente beinhalten, die die Authentifizierung an einen bestimmten Betrag und Zahlungsempfänger knüpfen. Dies könnte Kunden mehr Sicherheit bei der Autorisierung von Zahlungen gewähren. Die Technologie, die die Verknüpfung der starken Authentifizierungsdaten mit den Transaktionsdaten ermöglicht, sollte manipulationssicher sein.

Schutz sensibler Zahlungsdaten

BV 9: Es ist wünschenswert, dass E-Händler, die mit sensiblen Zahlungsdaten umgehen, ihre mit Betrugsbekämpfung befassten Mitarbeiter angemessen schulen und diese Schulungen regelmäßig aktualisieren, um sicherzustellen, dass die Inhalte für eine dynamische Sicherheitsumgebung relevant bleiben.

Kundeninformation und -kommunikation

BV 10: Es ist wünschenswert, dass Zahlungsdienstleister, die Abrechnungsdienste anbieten, für ihre E-Händler Fortbildungsprogramme zum Thema Betrugsbekämpfung organisieren.

Mitteilungen, Festlegung von Grenzwerten

BV 11: Innerhalb dieser festgelegten Grenzwerte könnten Zahlungsdienstleister ihren Kunden eine Vorrichtung zur Verfügung stellen, in der sie die Grenzwerte für Internetzahlungsdienste in einer sicheren und vertrauenswürdigen Umgebung verwalten können.

BV 12: Auf der Grundlage ihrer Risikomanagementrichtlinien könnten Zahlungsdienstleister im Falle von verdächtigen Zahlungsvorgängen oder Zahlungsvorgängen mit hohem Risiko Warnungen für Kunden einrichten, zum Beispiel über Telefonanrufe oder SMS.

BV 13: Zahlungsdienstleister könnten Kunden ermöglichen, allgemeine, personalisierte Regeln als Parameter für ihr Verhalten bei Internetzahlungen und damit verbundenen Diensten festzulegen, z. B. dass sie Zahlungen nur aus bestimmten Ländern auslösen und dass von anderen Standorten aus ausgelöste Zahlungen gesperrt werden sollten, oder dass sie bestimmte Zahlungsempfänger auf weiße oder schwarze Listen aufnehmen können.