Entwurf Mindestanforderungen an die Sicherheit von Internetzahlungen, Konsultation 02/2015

Anmerkungen des Bundesverbandes Öffentlicher Banken, VÖB

- Erläuterungen der BaFin zum Text des Rundschreibens sind kursiv gedruckt.
- Änderungen im Vergleich zum Rundschreibenentwurf vom 20.06.2014 sind als Überarbeitung markiert.
- Bereits integrierte Änderungsvorschläge sind gekennzeichnet

Tz	Anforderung	Anmerkung
2	Das Rundschreiben ist auf alle Zahlungsdienstleister im Sinne des § 1 Abs. 1 Zahlungsdiensteaufsichtsgesetz (ZAG) anwendbar, die Zahlungsgeschäfte i. S. d. § 1 Abs. 2 Nr. 2 ZAG im Massenzahlungsverkehr über das öffentliche Internet via Webbrowser anbieten (Internet-Zahlungsdienste). *Werden von Zahlungsdienstleistern Internet-Zahlungsdienste angeboten, so geht das Rundschreiben davon aus, dass die Zahlungen kundenseitig von Menschen über Webbrowser ausgelöst werden.* *Bei der Bereitstellung von Verfahren zur Nutzung von endkundenorientierten Online-Banking-Clients (z.B. FinTS) sind angemessene Sicherheitsvorkehrungen zu treffen, die ein vergleichbares Schutzniveau gewährleisten. Es sind die hier festgelegten Anforderungen entsprechend einzuhalten. Bietet ein Zahlungsdienstleister Zahlungen per Telefonbanking an, so sind die hier festgelegten Anforderungen entsprechend einzuhalten.*	Hier sollte entsprechend Ziffer 7 der EBA-Guidelines eine Auflistung der betroffenen Geschäftsvorfälle erfolgen. Dazu sollten die Ausnahmen aus Ziffer 11 hier gespiegelt werden. Unabhängig davon sind jedenfalls die nachstehenden Klarstellungen zu treffen: Die Ergänzung stellt klar, dass nur Zahlungen erfasst sind, die via Webbrowser vom Kunden initiiert werden. Dies ist ausweislich des Kursivtexts auch so gemeint. Der nicht kursive Text würde aber bei weiterer Auslegung auch international standardisierte Fernkommunikationsverfahren von Firmenkunden einbeziehen, die nicht browserbasiert sind, aber Internettechnologien nutzen (EBICS / DFÜ). Es besteht ein Widerspruch bei der Nutzung von Internet-Zahlungsdiensten per Webbrowser und per Online-Banking-Clients. Apps und Produktsoftware waren weder Bestandteil der SecuRePay-Mindestanforderungen noch der EBA-Richtlinien. Hier wurden mobile und nicht browserbasierte Anwendungen ausgenommen. Änderungen im Feld sind zudem nicht binnen 6 Monaten (inklusive Spezifizierung und Implementierung der starken Authentifizierung für den Kontozugang). FinTS-Clients gibt es beispielsweise bereits seit Jahren für Mobiltelefone und Tablets – auch von nicht-kreditwirtschaftlichen Drittanbietern (analog

Tz	Anforderung	Anmerkung
		für Produkten für PC und MAC). Auch aufgrund des Gleichbehandlungsgrundsatzes im Vergleich zu anderen europäischen Ländern sollten mobile und nicht browserbasierte Anwendungen ausgenommen bleiben! Die Ausdehnung auf das Telefonbanking sollte im Sinne einer einheitlichen Umsetzung wieder herausgenommen werden. Empfehlung: Orientierung am Originaltext der EBA, Seite 10, Punkt 11: „Excluded from the scope of the guidelines are:-…-payments where the instruction is given by post, telephone order, voice mail or using SMS-based technology-…" Bei einer Telefonbanking-Transaktion handelt es sich um gänzlich andere Abläufe. Zudem ist dieser Kanal deutlich weniger geeignet, eine Zwei-Faktor-Authentifizierung durchzuführen. Darüber hinaus sollte das Telefonbanking, wie im Originaltext, nicht als Internetzahlung eingeordnet werden.
	2. Allgemeine Anforderungen an das Sicherheitsmanagement	

Tz	Anforderung	Anmerkung
	2.1 Regelungen und Verantwortlichkeiten	
3	Zahlungsdienstleister haben angemessene Regelungen zur Sicherheit für ihre Internet-Zahlungsdienste aufzustellen, umzusetzen und regelmäßig zu überprüfen. Die Regelungen haben insbesondere die nachfolgenden Anforderungen zu berücksichtigen.	
4	Die Regelungen zur Sicherheit der Internet-Zahlungsdienste sind für sachkundige Dritte nachvollziehbar zu dokumentieren, regelmäßig zu überprüfen und von den verantwortlichen Führungskräften abzunehmen. *Die Regelungen zur Sicherheit der Internet-Zahlungsdienste sind anlassbezogen sowie regelmäßig - mindestens jährlich - zu überprüfen.*	
5	Darin sind Sicherheitsziele zu definieren und die Risikobereitschaft festzulegen.	
6	Die Regelungen zur Sicherheit der Internet-Zahlungsdienste haben Rollen und Verantwortlichkeiten festzulegen, einschließlich der zuständigen Risikomanagement-Funktion, welche direkt an die Geschäftsleitung berichtet. Ebenso sind die Berichtswege für die angebotenen Internet-Zahlungsdienste festzulegen. Dabei ist das Management sensibler Zahlungsdaten unter Berücksichtigung der Risikoanalyse, -kontrolle und -begrenzung festzulegen. *Sensible Zahlungsdaten sind Daten, die genutzt werden bzw. genutzt werden können, um einen Kunden ~~zu identifizieren und~~beim Login und bei der Auftragserteilung im Rahmen von Zahlungsdiensten zu authentisieren ~~(z.B. beim Login, bei der Ausführung von Internet-Zahlungen oder bei der Änderung oder Löschung von E-Mandaten)~~.*	Der Begriff der „sensiblen Zahlungsdaten“ sollte nicht das Ergebnis der Beratungen zur PSD II vorwegnehmen. Hier ist auf kohärente Belegung der Begriffe zu achten. Der Formulierungsvorschlag würde eine schärfere Trennung zwischen allgemeinem Datenschutzrecht und dem speziellen Recht bei Onlinezahlungen sicherstellen. Die Definition wird im Vergleich zum Original stark abgeändert. Im Sinne einer einheitlichen Auslegung sollte dies geändert werden.Empfehlung: Grundsätzlich sollte der Fokus nur auf den Daten liegen, die für einen Missbrauch im Bereich Internetzahlun-

Tz	Anforderung	Anmerkung
		gen geeignet sind, d.h. mit denen betrügerische Transaktionen durchgeführt werden können. An mehreren Stellen (Ziff. 10, 24, 75) ist von sensiblen Daten bzw. sensiblen Zahlungsdaten die Rede. Hier sollte unbedingt eine Definition erfolgen. Die Definition gem. § 3 Abs. 9 BDSG passt ersichtlich nicht. Der Ansatz sollte so sein, dass nicht jedes Datum im Zusammenhang mit Zahlungsverkehrsdiensten, hier Internetzahlungen, als sensibel gilt. Daten, die häufig und an vielen Stellen durch den Betroffenen selbst offengelegt werden (Name, Vorname, Kontonummer, BLZ) sollten nicht als sensibel eingestuft werden. Ansonsten droht die Gefahr, dass der Begriff der "sensiblen Daten" zu sehr ausgeweitet und damit verwaschen wird.
	2.2 Risikoanalyse	
7	Zahlungsdienstleister haben durch ihre zuständige Risikomanagement-Funktion für Zahlungen im Internet und die zugehörigen Dienste eine detaillierte Risikoidentifikation und Schwachstellenanalyse (Risikoanalyse) durchzuführen und zu dokumentieren. In die Risikoanalyse sind insbesondere einzubeziehen a) die Technologie des Zahlungsdienstleisters, b) die Dienste, die bezogen werden, c) die technische Umgebung der Kunden, d) die Risiken im Zusammenhang mit den gewählten Technologie-Plattformen, Anwendungsarchitekturen, Programmiertechniken und Routinen sowohl auf der Seite der Zahlungsdienstleister als auch auf Seiten der Kunden und e) die Ergebnisse der laufenden Überwachung der IT-Sicher-	

Tz	Anforderung	Anmerkung
	heitsvorfälle. Die Risikoanalyse ist vor der Einführung der Dienste durchzuführen und anschließend regelmäßig zu wiederholen.	
	Im Rahmen der Risikoidentifikation und -analyse wird eine Schutzbedarfsanalyse nach Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) erwartet, welche eine Schutzbedarfsfeststellung umfasst. *Bei der Schutzbedarfsfeststellung wird der Schutzbedarf der Geschäftsprozesse, der verarbeiteten Informationen und der IT-Komponenten bestimmt. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung der Grundwerte der Informationssicherheit – Verfügbarkeit, Integrität, Vertraulichkeit oder Authentizität - entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“.*	An dieser Stelle sollte die Anforderung im Rundschreiben neutral formuliert werden und nicht auf spezifische Standards zur IT-Sicherheit Bezug nehmen. Empfehlung, die ISO 27001 zu referenzieren um in Europa gleiche Wettbewerbsbedingungen für alle Marktteilnehmer zu erreichen.
8	Basierend auf den Ergebnissen der Risikoanalyse ist zu bestimmen, inwieweit Änderungen an den existierenden Sicherheitsverfahren, den genutzten Technologien, den Prozessen oder angebotenen Zahlungsdiensten erforderlich sind.	
9	Der Zahlungsdienstleister hat erforderlichenfalls bis zur Umsetzung der Änderungen angemessene Maßnahmen zur Minimierung von IT-Sicherheitsvorfällen und Unterbrechungen zu ergreifen. Dabei ist die Zeit zu berücksichtigen, die erforderlich ist, um die Änderungen umzusetzen (einschließlich der Auslieferung an die Kunden).	

Tz	Anforderung	Anmerkung
10	Die Risikoanalyse hat die Zielsetzung zu verfolgen, sensible Zahlungsdaten zu schützen und zu sichern.	
11	Sowohl nach sicherheitsrelevanten Zwischenfällen als auch vor sicherheitsrelevanten Änderungen der Infrastruktur oder bei neuen Erkenntnissen der Überwachung der Gefährdungen ist eine Überprüfung der Risikoszenarien und der Sicherheitsmaßnahmen durchzuführen.	
12	Darüber hinaus ist eine allgemeine Überprüfung der Risikobewertung mindestens einmal im Jahr durchzuführen.	
13	Die Ergebnisse der Risikoanalysen und ihrer Überprüfung ist den zuständigen Führungskräften zur Genehmigung vorzulegen.	
	2.3 Überwachung und Berichtswesen zu IT-Sicherheitsvorfällen	
14	Zahlungsdienstleister sollten Prozesse zur zentralen Registrierung, Beobachtung und Weiterverfolgung von IT-Sicherheitsvorfällen und sicherheitsbezogenen Kundenbeschwerden etablieren. Die IT-Sicherheitsvorfälle und sicherheitsbezogene Kundenbeschwerden sind an das Management zu berichten.	
15	Kritische IT-Sicherheitsvorfälle sind an die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)~~zuständigen Aufsichtsbehörden~~ ~~sowie gegebenenfalls an die Strafverfolgungsbehörden und die zuständigen Datenschutzbeauftragten zu melden.~~ Als kritisch ist ein IT-Sicherheitsvorfall dann zu betrachten, wenn die Verfügbarkeit, Integrität, Vertraulichkeit oder Authentizität von IT-Systemen, Anwendungen oder Daten mit einem hohen oder sehr hohen Schutzbedarf verletzt oder beeinträchtigt wird. Meldungen an die BaFin sind nach den Formularen ge-	Bargeldversorgung und klassischer Kartenzahlungsverkehr sind keine Onlinebezahlmethoden und deswegen nicht in dem anfangs definierten Anwendungsbereich (Internetzahlungen). Derzeit liegt der Regierungsentwurf eines IT-SiG vor, der diese Bereiche regelt. Hier muss eine zeitlich versetzte Doppelregulierung verhindert werden!

Tz	Anforderung	Anmerkung
	mäß Anlage I und II zu erstatten. ~~Zuständige Behörden können z.B. die Europäische Zentralbank, die BaFin, die Deutsche Bundesbank oder die zuständigen Landesdatenschutzbeauftragten sein. Die Meldewege an die BaFin und an die Deutsche Bundesbank werden separat veröffentlicht.~~ *Als Beispiel für kritische IT-Sicherheitsvorfälle sind insbesondere zu nennen:* • *Ausfälle oder Teilausfälle der nachgenannten bankfachlichen Prozesse über einen Zeitraum von mehr als 1 Stunde:* ~~*Bargeldversorgung*~~ ~~*Jeglicher Zahlungsverkehr einschließlich Kartenzahlung*~~ ○ *Online-Banking einschließlich Mobile-Banking;* • *Vorfälle, die zu einer Verletzung der Vertraulichkeit analog § 42a BDSG geführt haben;* • *Vorfälle, die zu signifikanten Reputationsschäden führen können und* • *Vorfälle, die vom Institut als Notfall gewertet werden und bei denen definierte Notfallmaßnahmen zum Einsatz kommen.*	Deswegen sollte der ganze Abschnitt nach Verabschiedung des IT-SiG Gegenstand eines separaten Rundschreibens werden. In jedem Fall sollten bereits bestehende Meldepflichten aus anderen Rechtsbereichen nicht noch einmal über Verweistechniken in das Aufsichtsrecht hinein gezogen werden. Insbesondere werden hier auch schon bestehende Meldepflichten gemäß § 42a BDSG, Verletzung der Vertraulichkeit, referenziert. Insgesamt werden hier verschiedene Aspekte außerhalb der Regelung von Sicherheitsanforderungen für Internetzahlungen gefordert. Es ist nicht nachvollziehbar, warum ergänzende Meldepflichten im Zusammenhang mit der „Bargeldversorgung“ und „jeglicher Zahlungsverkehr einschließlich Kartenzahlung“ aufgenommen wurden. Dies geht sehr deutlich über SecuRePay und EBA hinaus! Die Meldung dieser Prozesse sollte entfernt werden. Parallel sollen im Rahmen des IT-Sicherheitsgesetzes umfassende Meldepflichten aufgesetzt werden. Vor dem Hintergrund der bereits bestehenden umfangreichen Meldepflichten sollten hier nicht regelungsnotwendige Aspekte ausgeklammert werden – insbesondere wenn es sich zusätzlich um Mehrfachmeldungen handeln wird. Meldepflichten und -wege sollten mit den Anforderungen aus dem IT-Sicherheitsgesetz abgestimmt werden, um Mehrfachaufwand zu vermeiden. Die Meldepflichten gegenüber anderen Behörden sind durch einschlägige Vorschriften geregelt.

Formatiert: Schriftart: Nicht Kursiv

Tz	Anforderung	Anmerkung
		Wir schlagen vor, die Verweise auf **„**… *sowie gegebenenfalls an die Strafverfolgungsbehörden und die zuständigen Datenschutzbeauftragten*…“ zu streichen. Bitte um Prüfung: Sind im IT-Sicherheitsgesetz bereits Meldepflichten formuliert? (vgl. IT-Sicherheitsgesetz Seite 26, Punkt 7), z.B. werden dadurch identische Vorgänge an BSI und BaFin meldepflichtig. Dieser Aufwand ist für Institute erheblich. Hier sollte nur eine Behörde adressiert werden müssen und die Meldepflichten auf das tatsächlich Notwendigste beschränkt werden.
16	Die Zusammenarbeit mit den zuständigen Strafverfolgungsbehörden im Falle von kritischen IT-Sicherheitsvorfällen ist zu regeln. *Die Zusammenarbeit mit den zuständigen Strafverfolgungsbehörden umfasst auch, betroffene Kunden bei der Stellung eines Strafantrags zu unterstützen.*	Der kursive gedruckte Teil sollte entfallen. Ein Einzelbetrugsfall bei einem Endkunden ist kein kritischer Payment Security Incident und geht auch über Definition 3.3 des EBA-Papiers hinaus.
17	Zahlungsdienstleister, die Zahlungsdienste im Sinne von § 1 Abs. 2 Nr. 4 Alt. 2 ZAG anbieten (Acquirer), ~~Acquirer~~ haben vertraglich von den Online-Händlern, die sensible Zahlungsdaten speichern, verarbeiten oder übertragen, zu fordern, dass diese bei kritischen IT-Sicherheitsvorfällen im Zusammenhang mit Internetzahlungen sowohl mit den Zahlungsdienstleistern als auch mit den zuständigen Strafverfolgungsbehörden kooperieren.	Acquirer sollte definiert werden als ZDL, der Dienst nach § 1 Abs. 2 Nr. 4 Alt. 2 ZAG anbietet Darüber hinaus sollte „Online-Händler“ definiert werden. Fokus Kartenzahlungen: In der Praxis sind nicht alle Zahlungsdienstleister Acquirer, sondern oftmals nur Issuer (z. B. von Kreditkarten internationaler Gesellschaften) und haben somit keinen Einfluss auf die Händlerverträge. Dies sollte im Anwendungsbe-

Tz	Anforderung	Anmerkung
		reich der Regel zum Ausdruck kommen. Pflichten des Acquirers bzgl. Verträgen mit Online-Händlern: Hier müssen ggf. Verträge angepasst werden. Für die Anpassung von Verträgen sind Übergangsfristen notwendig. Als Vorschlag wäre eine zeitliche Abstufung nach Neu- und Bestandsverträgen. Neuverträge können bereits nach 6 Monaten entsprechende Anpassungen enthalten, Bestandsverträge beispielsweise 12 Monate nach Versand des Rundschreibens.
18	Wird bekannt, dass ein Online-Händler nicht wie vertraglich vereinbart kooperiert, sind angemessene Schritte einzuleiten, um die vertraglichen Verpflichtungen durchzusetzen oder den Vertrag zu beenden.	Vertragsanpassungen sind notwendig. Abstufungsvorschlag siehe Tz 17.
	2.4 Risikokontrolle und -vermeidung	
19	In Übereinstimmung mit den Regelungen zur Sicherheit sind Sicherheitsmaßnahmen umzusetzen, um identifizierte Risiken zu verringern. Diese Maßnahmen haben dem Prinzip der Verteidigung in der Tiefe zu genügen. *Das Prinzip der Verteidigung in der Tiefe bedeutet, dass das Versagen ~~von Maßnahmen auf~~ einer Verteidigungslinie durch ~~Maßnahmen auf einer~~ anderen~~n~~ Verteidigungslinie*n *kompensiert wird.*	Hier sollte sich an dem EBA-Text orientiert werden, der eine größere Flexibilität bei den Verteidigungslinien erlaubt. Hier wurden die Verteidigungslinien separat betrachtet, nicht aber eine Kompensation der einen Linie durch eine andere notwendig.
20	Bei der Konzeption, Entwicklung und Pflege von Internet-Zahlungsdiensten ist auf die ausreichende Trennung von Aufgaben im Bereich der IT-Umgebung~~en~~ zu achten. Es sind angemessene Benutzerberech-	

Formatiert: Schriftartfarbe: Automatisch

Formatiert: Schriftartfarbe: Automatisch

Tz	Anforderung	Anmerkung
	tigungsverfahren einzuführen, welche die sichere Verwaltung von Benutzeridentitäten und den wirksamen Schutz des Zugriffs auf Daten und IT-Systeme sicherstellen (Identity and Access Management). *Zur IT-Umgebung gehört beispielsweise die Entwicklungs-, Test- und Produktionsumgebung. Als eine Grundlage wirksamer Benutzerberechtigungsverfahren ist dem Prinzip der minimalen Vergabe von Berechtigungen (Least-Privileged-Prinzip) Rechnung zu tragen. Deshalb ist der Zugang durch die verschiedenen Anwendungen auf die Daten und Ressourcen auf ein absolutes Minimum zu beschränken.*	
21	Netzwerke, Webseiten, Server und Kommunikationsverbindungen sind gegen Missbrauch oder Angriffe zu schützen.	
22	Die Server sind zu härten. *Die Härtung der Server dient der Reduzierung der Verwundbarkeit von Anwendungen. Zur Härtung der Server gehört beispielsweise die Entfernung von allen ~~Beschneidung der Server aller~~ überflüssigen Funktionen.*	
23	Die Websicherheit ist zu gewährleisten. *Es soll insbesondere verhindert werden, dass manipulierte Webseiten verwendet werden. Dazu gehört beispielsweise die Imitierung der legitimen Website des Zahlungsdienstleisters. Insbesondere sind solche Webseiten, über die Transaktionen ausgelöst werden können bzw. die Internet-Zahlungsdienstleistungen anbieten, durch Extended Validation-Zertifikate, die auf den Namen des Zahlungsdienstes lauten, oder durch andere mindestens gleichwertige Authentifizierungsmethoden zu schützen.*	Hier empfehlen wir die konkretere Beschreibung aus der EBA-Richtlinie unter 4.2 zu verwenden. Die Websicherheit ist durch EV-Zertifikate oder durch andere *mindestens gleichwertige Authentifizierungsmethoden zu schützen.* Die Überschrift “Die Websicherheit ist zu gewährleisten“, sollte entfallen.

Tz	Anforderung	Anmerkung
24	Der Zugang zu a) sensiblen Daten b) logischen und physisch kritischen Ressourcen ist zu überwachen, nachzuverfolgen und zu beschränken. Es sind geeignete Logdaten und Prüfprotokolle zu erstellen, zu speichern und zu analysieren.	
25	Bei der Konzeption, der Entwicklung und dem Betrieb von Internet-Zahlungsdiensten ist das Prinzip der Datenminimierung zu beachten. *Das Sammeln, Weiterleiten, Verarbeiten, Speichern und/oder Archivieren sowie die Visualisierung sensibler Zahlungsdaten ist auf ein Minimum zu begrenzen.*	Es sollte klargestellt werden, dass mit „Minimierung“ eine Umsetzung des Prinzips der Datenvermeidung und Datensparsamkeit gem. § 3 a BDSG gemeint ist. Soweit erforderlich sollte auch definiert werden, welche Daten wann erforderlich sind.
26	Sicherheitsmaßnahmen für Internet-~~Payment~~dienste sind unter Aufsicht der Risikomanagement-Funktion zur Sicherstellung ihrer Robustheit und Effektivität regelmäßig zu testen. *Die Tests dienen insbesondere dazu, die Robustheit und Effektivität der Sicherheitsmaßnahmen zu gewährleisten. Dabei sind vorgenommene Änderungen, beobachtete Sicherheitsbedrohungen sowie Szenarien der einschlägig bekannten potentiellen Angriffe zu berücksichtigen.*	Im Sinne der einheitlichen Begriffsverwendung schlagen wir vor, statt „Internet-Dienste“ identisch zu TZ 28/29 etc. den Begriff „Internet-Zahlungsdienste“ zu verwendet.
27	Alle Änderungen sind einem angemessenen, formalen Änderungsverwaltungsprozess (Change-Management-Prozess) zu unterziehen. *Es soll sichergestellt werden, dass Änderungen richtig geplant, getestet,*	

Tz	Anforderung	Anmerkung
	dokumentiert und autorisiert werden.	
28	Die Sicherheitsmaßnahmen sind in regelmäßigen Abständen zu prüfen. Die Prüfungen sind von vertrauenswürdigen und unabhängigen (internen bzw. externen) Experten durchzuführen. Diese Experten dürfen nicht in irgendeiner Weise in die Entwicklung, Implementierung oder den Betrieb des Internet-Zahlungsdienstes eingebunden sein. Die Prüfung soll bestätigen, ob die Sicherheitsmaßnahmen Robustheit und Effektivität gewährleisten.	
29	Die Umsetzung und das Funktionieren der Internet-Zahlungsdienste sind ebenfalls zu prüfen. Die Häufigkeit und die Schwerpunkte dieser Prüfungen sind abhängig von den Sicherheitsrisiken festzulegen.	
30	Übernehmen Externe Sicherheitsfunktionen für den Zahlungsdienstleister, so hat der Zahlungsdienstleister sicherzustellen, dass der Externe die Anforderungen dieses Rundschreibens einhält.	
31	Acquirer haben von ihren Online ~~E-~~Händlern vertraglich zu verlangen, dass diese Sicherheitsmaßnahmen in ihrer IT-Infrastruktur implementieren, die den vorgenannten Anforderungen (Tzn. ~~..~~ 20 bis ~~..~~30) genügen.	Bei Kreditkartenzahlungen liegt die Erfüllung der Anforderung nicht in der Hoheit des Kartenherausgebers, sondern obliegt den Verfahrensregeln der Kreditkartenorganisation. Siehe Tz 17: Übergangsregelungen für Neu- und Bestandskunden von Acquirern aufgrund von Vertragsänderungen.
	2.5 Nachvollziehbarkeit von Transaktionen und E-Mandaten	
32	Zahlungsdienstleister haben ~~Es ist~~ sicherzustellen, dass ~~die~~ ihre Dienste Sicherheitsmechanismen für das detaillierte Loggen von Transaktionen	

Tz	Anforderung	Anmerkung
	und E-Mandaten beinhalten. *Zu den Logdaten gehören Transaktions-ID, Zeitstempel sowie Aufzeichnungen für Änderungen der Parametrisierung und des Zugriffs auf Transaktionsdaten.*	
33	Zur Nachvollziehbarkeit von Ergänzungen, Änderungen oder Löschungen von Transaktionen und E-Mandaten sind Logdateien zu erstellen.	
34	Die Transaktions- und E-Mandat-Daten sind zu analysieren und es ist sicherzustellen, dass die Logdateien jederzeit mit angemessenen Werkzeugen ausgewertet werden können.	
35	Es ist sicherzustellen, dass entsprechende Anwendungen bzw. Werkzeuge nur autorisiertem Personal zugänglich sind.	
	3. Besondere Anforderungen an die Steuerung und die Sicherheitsmaßnahmen für die Internet-Zahlungen **3.1 Initiale Kundenidentifikation und Information**	
36	Bevor einem Kunden Zugang zu Internet-Zahlungsdiensten gewährt wird, ist nachweisbar eine Willenserklärung einzuholen, dass der betroffene Kunde Internet-Zahlungsdienste in Anspruch nehmen will. Zudem ist vorab sicherzustellen, dass der Kunde die für die Identifizierung erforderlichen Verfahren durchlaufen hat und ausreichende Ausweispapiere und damit zusammenhängende Informationen vorgewiesen hat. *Kunden sind nach den Vorgaben der nationalen und europäischen Anti-Geldwäschevorschriften und sonstigen relevanten Vorschriften korrekt*	Bislang regeln Kreditkartenverträge die unterschiedlichen Nutzungen der Karte nicht explizit. Die Möglichkeit des Karteneinsatzes im Internet ist aber eine allgemein bekannte Standardfunktion der Karte und damit auch ohne wörtliche Erwähnung im Rahmen einer Vertragsauslegung als vereinbarte Funktion zu werten. Sofern eine darüber hinausgehende explizite Darstellung im Vertrag erwartet wird, sollte klargestellt werden, dass dies nur für zukünftige Verträge gilt, damit nicht mit allen Bestandskunden, die heute bereits Kreditkarten im Internet nutzen, neue Verträge

Tz	Anforderung	Anmerkung
	zu identifizieren.	zu vereinbaren sind. Die Einhaltung der geldwäscherechtlichen Vorschriften des GwG ist selbstverständlich und sollte deswegen nicht durch Erwähnung an dieser Stelle einen neuen aufsichtsrechtlichen Charakter erhalten.
37	Es ist sicherzustellen, dass die erforderlichen vorvertraglichen Informationen, die dem Kunden ~~ausgehändigt~~ zur Verfügung gestellt werden, Details zum Internet-Zahlungsdienst enthalten. *Welche vorvertraglichen Informationen an den Kunden erforderlich sind, ergibt sich aus Art. 248 EGBGB~~der EU-Zahlungsdiensterichtlinie 2007/64/EG in der jeweils geltenden Fassung~~.*	Die Terminologie „Aushändigen“ passt bei Online-Zahlungen nicht, da die Informationserteilung regelmäßig auf anderen Kanälen als durch physische Übergabe erfolgt. Dies wird durch den weiteren Wortlaut „zur Verfügung stellen“, der sich an die PSD-Terminologie anlehnt, deutlich. Die ZDRL gilt in Deutschland nicht unmittelbar, sondern ist in Art. 248 EGBGB umgesetzt, weshalb hierauf verwiesen werden sollte.
38	Darin ist, soweit angemessen, Folgendes anzugeben: • eindeutige Angaben über etwaige Anforderungen hinsichtlich der Kunden-Hardware und -Software oder andere notwendige Werkzeuge; • einen Leitfaden für die ordnungsgemäße und sichere Nutzung von personalisierten Sicherheitsinformationen; • eine Beschreibung für die schrittweise Vorgehensweise des Kunden zur Einreichung und Autorisierung einer Zahlung einschließlich der Auswirkungen der einzelnen Schritte;	Hier ist evtl. eine Ergänzung der institutsspezifischen Hinweisblätter zu verfahrenstechnischen Themen erforderlich.

Formatiert: Schriftartfarbe: Automatisch

Tz	Anforderung	Anmerkung
	• einen Leitfaden für die ordnungsgemäße und sichere Verwendung aller an den Kunden ausgegebenen Hard- und Software; • die Verfahren, die im Falle von Verlust oder Diebstahl der persönlichen Sicherheits- und Anmeldungsinformationen oder der Hard- und Software des Kunden für die Anmeldung oder Durchführung von Transaktionen zu befolgen sind; • die Verfahren, die im Falle eines entdeckten oder vermuteten Missbrauchs zu befolgen sind; • eine Beschreibung der Verantwortlichkeiten und der Haftung des Zahlungsdienstleisters sowie des Kunden in Bezug auf die Nutzung des Internet-Zahlungsdienstes. *Zu den notwendigen Werkzeugen gehören beispielsweise Antivirus-Software oder Firewalls.*	
39	Der Rahmenvertrag mit dem Kunden legt im Einzelnen fest, dass der Zahlungsdienstleister eine spezifische Transaktion oder das Zahlungsinstrument auf der Basis von Sicherheitsbedenken sperren darf.	Es wird darauf hingewiesen, dass diese Anforderung mit Anpassungen der aktuell bestehenden AGBs verbunden sein könnte.
40	Der Rahmenvertrag hat das Verfahren und die Bedingungen der Benachrichtigung des Kunden sowie die Art und Weise festzulegen, wie der Kunde den Zahlungsdienstleister kontaktieren kann, um eine Transaktion bzw. den Service wieder zu entsperren. Die Festlegungen sind im Einklang mit der Zahlungsdiensterichtlinie 2007/64/EG in der jeweils geltenden Fassung~~PSD~~ zu treffen.	MERKER: Verweis auf nationales Recht vor die Klammer ziehen. Es wird darauf hingewiesen, dass diese Anforderung in Bezug auf die PSD zu Zielkonflikten führen könnte. Daher wäre es wünschenswert, wenn die rechtlichen Rahmenbedingungen vorab von der Aufsicht geprüft würden.

Tz	Anforderung	Anmerkung
41	Die Kunden sind fortlaufend und anlassbezogen über ihre Verantwortung hinsichtlich der sicheren Nutzung des Dienstes zu informieren. Dazu sind geeignete Mittel, wie z.B. Broschüren oder Internetseiten, einzusetzen.	Die Anforderung wurde von der EBA gestrichen: “PSPs should also ensure that customers are provided, on an ongoing or, where applicable, ad hoc basis, and via appropriate means (e.g. leaflets, website pages), with clear and straightforward instructions explaining their responsibilities regarding the secure use of the service.” Deswegen sollte es auch hier gestrichen werden. Die Fortlaufende Unterrichtung des Kunden über Sicherheitsmaßnahmen: Wird i.d.R. bereits erfüllt; insbesondere durch aktuelle Sicherheitshinweise auf der Online-Banking-Seite sowie Informationen über Kreditkartenabrechnungen und ggf. Mobil-Applikationen (obwohl hier nur webbasierte Lösungen umfasst sind).
	3.2 Starke Kundenauthentisierung	
42	Für die Autorisierung von Internet-Zahlungen durch einen Kunden (inkl. Sammelüberweisungen) und für die Ausgabe oder Änderung von E-Mandaten ist starke Kundena~~A~~uthentisierung einzusetzen. *Unter starker Kundenauthentisierung ist ein Verfahren zur Validierung der Identifizierung einer natürlichen oder juristischen Person auf der Grundlage von mindestens zwei Elementen der Kategorien Wissen, Besitz und Inhärenz zu verstehen, die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt und durch die Auslegung des Verfahrens die Vertraulichkeit der Authentifizierungsdaten geschützt ist. Die Kategorie Wissen umfasst Informationen, die ausschließlich der zu identifizierenden Person zur Verfügung stehen (z. B. Passwörter oder PINs) und die durch das Verfahren hinreichend stark gegen Imitation, Kopie bzw. Missbrauch durch Dritte geschützt sind. Die Kategorie Besitz umfasst physische Gegenstände, die durch ihre Ausgestaltung und das Verfah-*	

Tz	Anforderung	Anmerkung
	ren hinreichend stark gegen Imitation, Kopie bzw. Missbrauch durch Dritte geschützt sind. *Die Kategorie Inhärenz umfasst unveränderliche biologische Merkmale natürlicher Personen, die durch das Verfahren hinreichend stark vor Imitation, Kopie bzw. Missbrauch geschützt sind.*	
	Endgeräte (einschließlich Software und Hardware) und Verfahren, über die dem Kunden eine TAN zur Verfügung gestellt wird, sind angemessen zu schützen, siehe z.B. die Technische Richtlinie TR-03107-1 des Bundesamts für Sicherheit in der Informationstechnik (BSI).~~In der Technischen Richtlinie TR-03107-1 des Bundesamts für Sicherheit in der Informationstechnik werden die Anforderungen an ein TANGenerator-basiertes Verfahren konkretisiert, welches die genannten Bedingungen erfüllt. Demnach muss der TAN-Generator selbst individuell und durch eine PIN geschützt sein.~~	Verweis auf DK-Schreiben zum „PIN-Schutz des TAN-Generators“ vom 22.09.2014
	Die wesentlichen Transaktionsdaten müssen in die ~~Generation~~ Generierung der TAN eingehen und dem Nutzer unabhängig von der primären Verbindung zum Zahlungsdienstleister angezeigt werden. Die Zwei-Faktor-Authentisierung ist unabhängig von der primären Verbindung zum Zahlungsdienstleister auszugestalten.	Die Transaktionsbindung wird von EBA/EZB nicht gefordert und gefährdet u.U. TAN-Listen-Verfahren und dynamische Passwörter bei 3D Secure (Vorgriff auf „strong transaction authorisation“ in der PSD II). Der Satz „*Die Zwei-Faktor-Authentisierung ist unabhängig von der primären Verbindung zum Zahlungsdienstleister auszugestalten.“ sollte gestrichen werden, weil er in dem EBA-Dokument unter Kapitel 7 nicht auftaucht.*
43	In folgenden Fällen können auch alternative Authentisierungsverfahren eingesetzt werden: • ausgehende Zahlungen an vertrauenswürdige Empfänger, die in zuvor angelegten Listen als vertrauenswürdig akzeptierter Zah-	Vorschlag: „in folgenden Fällen können auch alternative Kunden-Authentisierungsverfahren eingesetzt werden“ Vorschlag: Beim 1. Punkt sollte der Begriff „dieses Kunden“ ersetzt werden in „für diesen Kunden“ gemäß EBA 7.1 S.18 erster

Tz	Anforderung	Anmerkung
	lungsempfänger (White Lists) ~~dieses~~ für diesen Kunden enthalten sind, • Transaktionen zwischen zwei Konten desselben Kunden beim selben Zahlungsdienstleister, • Transaktionen innerhalb desselben IT-Dienst~~Zahlungsdienst~~leisters, die durch eine Risikoanalyse gerechtfertigt werden, • ~~Niedrig~~Zahlungen, entsprechend den Betragsgrenzen ~~Kleinstbetragszahlungen entsprechend~~des § 675i BGB~~der EU-Zahlungsdiensterichtlinie 2007/64/EG~~.	Spiegelstrich. Aus Sicherheitsaspekten ist es sinnvoll, nicht auf denselben Zahlungsdienstleiser abzustellen, sondern darauf, ob die Zahlung innerhalb eines Systems abgewickelt wird (z. B. innerhalb eines IT-Dienstleisters einer Verbundgruppe oder eines Bankkonzerns). Eine entsprechende Berücksichtigung würde Wettbewerbsnachteile deutscher Anbieter z. B. gegenüber PayPal verringern.
44	Der Zugriff auf sensible Zahlungsdaten und die Änderung dieser Daten (inkl. Erzeugung und Änderung von White Lists) erfordert starke Authentisierung. *Die Regel bezieht sich auf die Verarbeitung der Daten während und infolge der Transaktion. Kontoauszugsinformationen sind hiervon ausgenommen.*	Hier ist klarzustellen, dass dies nicht die Anzeige von Kontoauszugsinformationen betrifft. Es wird an dieser Stelle nochmals darauf hingewiesen, dass sensible Zahlungsdaten analog zum Punkt Tz 6 im Sinne der originalen Definition verstanden werden sollten. Die Erfordernis der 2-Faktor-Authentisierung durch den Kunden richtet sich nach dem Schutzbedarf der jeweiligen sensiblen Zahlungsdaten. Nicht immer sind sensible Zahlungsdaten auch vertraulich. Beispielsweise sollten die Zielkontodaten auf einer White-List nicht vertraulich sein. Fazit: „…erfordert starke Authentisierung entsprechend dem Schutzbedarf der Daten.“
45	~~Sofern~~ Wenn ein Zahlungsdienstleister ~~ausschließlich solche~~ Dienste	Die Formulierung wäre andernfalls dahingehend missverständ-

Formatiert: Nicht Durchgestrichen

Formatiert: Einzug: Links: 0,63 cm, Hängend: 0,63 cm

Formatiert: Schriftart: Kursiv

Formatiert: Schriftart: Kursiv

Formatiert: Schriftartfarbe: Automatisch

Tz	Anforderung	Anmerkung
	anbietet, bei denen keine Transaktionen ausgeführt werden und keine sensiblen Kunden- oder Zahlungsdaten angezeigt werden, die leicht für betrügerische Zwecke verwendet werden könnten, kann er seine Authentisierungsanforderungen auf Basis seiner Risikoanalyse entsprechend anpassen.	lich, dass nur Zahlungsdienstleister von der Erleichterung profitierten, die kein weiteres Geschäft betr~~i~~eiben. Dies ist aber offenbar nicht gemeint und wäre auch vor dem Hintergrund gleicher Wettbewerbsbedingungen ~~-~~abzulehnen.
46	Im Falle von Kartentransaktionen, die Internetzahlungsdienste betreffen, ist durch den kartenausgebenden Zahlungsdienstleister die starke Authentisierung des Karteninhabers zu unterstützen.	Um die geschäftspolitische Diversifikation zu erhalten, muss es Zahlungsdienstleistern zukünftig gestattet sein, Zahlungskarten herauszugeben, die nicht für Internetzahlungen zugelassen sind. .
47	Alle neu ausgegebenen Karten, die im Internet eingesetzt werden können, müssen technisch dazu in der Lage sein, mit starker Authentisierung genutzt zu werden.	Die Formulierung könne missverstanden werden. Empfehlung für eine alternative Formulierung: „Für alle ausgegebenen Karten muss technisch sichergestellt werden, dass diese mit starker Authentisierung genutzt werden können.“
48	Acquirer haben Technologien zu unterstützen, die es dem Kartenausgeber erlauben, starke Authentisierung des Karteninhabers für Kartenzahlungssysteme durchzuführen, an denen der Acquirer teilnimmt.	
49	Acquirer haben von ihren Online-Händlern zu fordern, Lösungen zu unterstützen, die es dem Kartenherausgeber erlauben, starke Authentisierung des Karteninhabers für Kartentransaktionen über das Internet durchzuführen.	
50	Die Nutzung alternativer Authentisierungsverfahren kann für vordefinierte Kategorien von Transaktionen mit niedrigem Risiko in Betracht gezogen werden. *Die Kategorien der alternativen Authentisierungsverfahren können bei-*	

Tz	Anforderung	Anmerkung
	spielsweise auf einer transaktionsbezogenen Risikoanalyse basieren oder Kleinst~~Niedrig~~betragszahlungen gemäß § 675i BGB ~~EU-Zahlungsrichtlinie 2007/64/EG~~ berücksichtigen.	
51	Die Regelungen zur Haftung haben starke Authentisierung in angemessener Weise zu berücksichtigen.	Dies stellt einen Vorgriff auf die PSD II dar. Die Differenzierung stünde auch im Widerspruch zur (noch) geltenden zivilrechtlichen Regelung der §§ 675u, v BGB. Abgesehen davon ist sie auch in der EBA-Version vor dem Hintergrund der laufenden Beratung gestrichen worden. Dies sollte hier ebenfalls erfolgen, damit nicht nach Verabschiedung der PSD II eine neuerliche Bedingungsanpassung notwendig wird. Dieser Punkt sollte gestrichen werden, da nicht in EBA-Guidelines enthalten. Unklar, in welcher Weise die Haftung zu berücksichtigen ist ([Recommendations], S. 10: „The liability regime should provide that a PSP must refund other PSPs for any fraud resulting from weak customer authentication").
52	Für Kartenzahlungssysteme haben Anbieter von Wallet-Lösungen von den Kartenausgebern starke Authentisierung zu verlangen, wenn der legitimierte Karteninhaber die Kartendaten erstmalig registriert.	
53	Anbieter von Wallet-Lösungen haben starke Authentisierung für die Fälle zu unterstützen, wenn Kunden sich in den Wallet-Zahlungsdienst einloggen oder Kartentransaktionen über das Internet durchführen.	Eine starke Authentifizierung sollte ausschließlich für die Durchführung von Zahlungen oder die Ergänzung eines Zahlungsdienstes notwendig sein – nicht aber für den Einblick bzw. Login in die Wallet. Der Unterschied zwischen „Wallet-Lösung" und

Tz	Anforderung	Anmerkung
		„Wallet-Zahlungsdienst“ müsste klargestellt werden.
54	Die Nutzung alternativer Authentisierungsverfahren kann für vordefinierte Kategorien von Transkationen mit niedrigem Risiko in Betracht gezogen werden, z. B. basierend auf einer transaktionsbasierten Risikoanalyse, oder bei KleinstNiedrigbetragszahlungen gemäß Zahlungsdiensterichtlinie 2007/64/EG§ 675i BGB.	
55	Im Falle virtueller Karten hat die initiale Registrierung in einer sicheren und vertrauenswürdigen Umgebung zu erfolgen.	
56	Bei Ausgabe von virtuellen Karten über das Internet ist für den Generierungsprozess der Daten der virtuellen Karten starke Authentisierung zu nutzen.	
57	Während der Kommunikation der Zahlungsdienstleister mit Online-Händlern zum Zweck der Initiierung von Internet-Zahlungen und dem Zugriff auf sensible Zahlungsdaten ist ordnungsgemäße bilaterale Authentisierung sicherzustellen.	
	3.3 Registrierung und Ausgabe von Authentisierungswerkzeugen und/oder Software an Kunden	
58	Anmeldung und Ausgabe von Authentisierungsmitteln und/oder Software an Kunden haben die folgenden Anforderungen zu erfüllen:	Dies ist keine Anforderung (sollte mit Tz 59 verknüpft werden)
59	Die Prozesse haben in einer sicheren und vertrauenswürdigen Umgebung zu erfolgen, wobei mögliche Risiken durch Geräte, die sich nicht unter der Kontrolle des Zahlungsdienstleisters befinden, berücksichtigt	

Formatiert: Schriftartfarbe: Text 1

Formatiert: Schriftartfarbe: Text 1

Tz	Anforderung	Anmerkung
	werden müssen.	
60	Für die Ausgabe personalisierter Sicherheits-Anmeldeinformationen, für zahlungsbezogene Software und für alle personalisierten Geräte, die für Internet-Zahlungen genutzt werden, sind effiziente und sichere Prozesse einzusetzen. *Mit zahlungsbezogener Software ist eine Software gemeint, die im Rahmen eines Authentisierungsverfahrens zum Einsatz kommt (z. B. softwarebasierte TAN-Generatoren), nicht aber herkömmliche Finanzverwaltungssoftware ohne Zahlungsfunktion.*	
61	Software, die über das Internet verteilt wird, ist ~~vom Zahlungsdienstleister digital~~ so zu signieren, dass es dem Kunden ermöglicht wird, deren Authentizität und Integrität zu verifizieren.	„ist vom Zahlungsdienstleister digital zu signieren“ sollte ersetzt werden gegen „ist vom Hersteller der Software digital zu signieren“. Hinweis: Banken stellen oftmals SW von Drittherstellern zur Verfügung. Aus diesem Grund ist es nicht immer möglich, dass der Zahlungsdienstleister die SW selbst signiert. Hinweis 2: Auf einigen Kundenumgebungen erfolgt die Verifikation automatisch durch das System ohne Prüfmöglichkeit durch den Endkunden. Auch Drittanbieter, die Personal Finance Management (PFM) anbieten, sollten die Authentizität ihrer SW gewährleisten.
62	Im Falle von Kartentransaktionen ist dem Kunden unabhängig von einem bestimmten Internet-Kaufvorgang die Möglichkeit anzubieten, sich für starke Authentisierung zu registrieren.	Diese Anforderung kann nicht vom Issuer der Karte eingehalten werden, sondern richtet sich an den Online-Händler, der nicht Adressat des Rundschreibens ist. Bestenfalls könnten Acquirer verpflichtet werden, dies mit Händlern vertraglich zu vereinbaren.

Formatiert: Schriftartfarbe: Text 1

Formatiert: Schriftartfarbe: Automatisch

Tz	Anforderung	Anmerkung
63	Wenn während des Online-Kaufvorgangs eine Aktivierung angeboten wird, hat dies mit Hilfe ~~des Redirects~~ der Umleitung des Kunden in eine sichere und vertrauenswürdige Umgebung zu erfolgen.	
64	Kartenausgeber haben aktiv die Registrierung der Karteninhaber für eine starke Authentisierung zu fördern und den Karteninhabern nur in begrenzten Ausnahmefällen zu erlauben, die Registrierung zu umgehen. Dies ist durch das Risiko der spezifischen Kartentransaktion zu rechtfertigen.	
	3.4 Login-Versuche, Session-Timeout, Gültigkeit der Authentisierung	
65	Werden Einmalpasswörter (One-Time-Passwords, z. B. per ChipTan generiete Codes) für die Authentisierung genutzt, so ist deren Gültigkeit auf das notwendige Minimum zu begrenzen.	
66	Die maximale Anzahl ungültiger Login- oder Authentisierungsversuche, nach denen der Zugriff auf den Internet-Zahlungsdienst temporär oder permanent gesperrt wird, ist auf ein Minimum zu begrenzen.	
67	Es ist ein sicheres Verfahren einzurichten, das es ermöglicht, gesperrte Internet-Zahlungsdienste zu reaktivieren.	
68	Eine inaktive Session ist nach einer vorgegebenen Zeit automatisch zu beenden.	
	3.5 Transaktionsüberwachung	

Formatiert: Schriftartfarbe: Text 1

Formatiert: Schriftartfarbe: Text 1

Tz	Anforderung	Anmerkung
69	Es sind ~~Systeme~~ Mechanismen zur Erkennung und Verhinderung von Manipulationen einzusetzen, die verdächtige Transaktionen identifizieren, bevor die Transaktion bzw. das E-Mandat final ~~autorisiert~~ ausgeführt wird. *Derartige ~~Systeme~~ Mechanismen sollten z. B. auf parametrisierten Regeln beruhen (z.B. Black Lists kompromittierter oder gestohlener Karten) und ungewöhnliche Verhaltensmuster des Kunden bzw. des Zugangsgerätes des Kunden überwachen, wie z. B. Wechsel der IP-Adresse oder der IP-Range während der Session, ungewöhnliche Online-Händler-Kategorien für spezielle Kunden oder ungewöhnliche Transaktionsdaten etc.*	Es wird empfohlen, das Wort „System“ durch die flexiblere Formulierung „Mechanismen“ zu ersetzen. Kapitel 5 der EZB-Empfehlungen spricht in diesem Zusammenhang treffend von Sicherheits-Mechanismen. Dies sollte auf andere Kapitel übertragen werden. Komplexe Mechanismen und Prozesse sind nicht notwendigerweise in eigenständigen (Hardware-)Systemen abgebildet. Darüber hinaus ist das Wort System oft vielfältig konnotiert z.B. ISMS (Information Security Management System). Der zweite Halbsatz sollte angepasst werden, um die Intention stärker zu betonen und den Abläufen in der deutschen Kreditwirtschaft anzunähern: […] bevor die Transaktion bzw. das E-Mandat final durch den Zahlungsdienstleister ausgeführt wird.
70	Die Systeme müssen auch in der Lage sein, Anzeichen einer Malware-Infektion in einer Session und bekannte Angriffsszenarien zu erkennen.	Nach wie vor ist unklar, was mit „Malware-Infektion gemein ist. In jedem Fall ist zu präzisieren, dass sich die Anforderung nur auf die Teile der IT-Infrastruktur erstreckt, die sich in der Institutssphäre befindet. Ein Scannen des Kunden-PCs ist nicht möglich.
71	Umfang, Komplexität und die Anpassungsfähigkeit der Überwachung-Lösungen sind unter Einhaltung der ~~einschlägigen~~ Datenschutzvorschriften in angemessener Weise an den Ergebnissen der Risikobewertung auszurichten.	Bundesdatenschutzgesetz (BDSG) und Telemediengesetz (TMG) enthalten keine „einschlägigen Vorschriften“ speziell in diesem Bereich.
72	Acquirer haben Betrugserkennungs- und -verhinderungssysteme zu betreiben, die eine Überwachung der Aktivitäten der Online-Händler	

Formatiert: Schriftartfarbe: Automatisch

Tz	Anforderung	Anmerkung
	ermöglichen.	
73	Transaktions-Screening- und Evaluierungsverfahren sind innerhalb angemessener Frist durchzuführen, so dass die Initiierung und/oder Ausführung des Internet-Zahlungsdienstes nicht unnötig verzögert wird.	
74	Wird wegen des Risikos entschieden, eine Zahlung, die als potentiell betrügerisch erkannt wurde, anzuhalten, so darf diese Zahlung nur solange angehalten werden, bis das Sicherheitsproblem gelöst wurde.	
	3.6 Schutz sensibler Zahlungsdaten	
75	Sensible Zahlungsdaten sind bei der Speicherung, Verarbeitung und Übermittlung zu schützen. Sensible Zahlungsdaten und die Kunden-Web-Schnittstelle (Webseite des Zahlungsdienstleisters bzw. des Online-Händlers) sind auf angemessene und wirksame Weise gegen Diebstahl, unerlaubten Zugriff und Modifizierung zu schützen.	Die Definition sensibler Zahlungsdaten ist momentan noch offen. Es wird davon ausgegangen, dass beim Online-Banking die Absicherung der Übertragung sensibler Daten per SSL die Anforderung erfüllt. TANs, die auf Basis von Transaktionsdaten generiert werden, gehören nicht zu den sensiblen Zahlungsdaten, da sie gemäß starker Auth. transaktionsbezogen sind damit direkt kein Betrug erfolgen kann.
76	Es ist sicherzustellen, dass bei einem Austausch von sensiblen Zahlungsdaten über das Internet eine sichere Ende-zu-Ende-Verschlüsselung zwischen ~~Bank und Kunde~~den kommunizierenden Teilnehmern während des gesamten Dialoges erfolgt, welche die Vertraulichkeit und Integrität der Daten sicherstellt. Dazu sind starke und allgemein anerkannte Verschlüsselungsmethoden anzuwenden. *Der zwischen der Bank und Kunde geführte Kaufdialog wird nicht von dieser Anforderung erfasst.*	Der Vorschlag orientiert sich am Originalwortlaut der EBA-Guidelines, welcher berücksichtigt, dass die kommunizierenden Teilnehmer – zB bei mehrstufigen Prozessen im Kartenzahlungsverkehr – nicht zwangsläufig Kunde und Zahlungsdienstleister sein müssen.

Tz	Anforderung	Anmerkung
77	Acquirer haben ihre Online-Händler aufzufordern, keine sensiblen Zahlungsdaten zu speichern.	Wir weisen zudem darauf hin, dass der Händler nach HGB, TMG u.a. Archivierungspflichten von Abrechnungsunterlagen und technischen Protokollen haben kann.
78	Im Falle, dass Online-Händler sensible Zahlungsdaten speichern, verarbeiten oder übertragen, haben die Acquirer die Online-Händler vertraglich zu verpflichten, die notwendigen Maßnahmen zu ergreifen, um diese Daten zu schützen.	Ggf. Widerspruch zu Tz 77?
79	Dazu sind regelmäßige Kontrollen durchzuführen. Wenn ein Zahlungsdienstleister erkennt, dass ein Online-Händler die erforderlichen Maßnahmen zur Gefahrenabwehr nicht umgesetzt hat, so hat er angemessene Schritte zu unternehmen, um diese vertragliche Verpflichtung durchzusetzen, oder er hat den Vertrag zu kündigen.	Siehe Anmerkung Tz 78
	4. Schutz der Kunden **4.1 Kundenschulung und Kommunikation**	
80	Es ist den Kunden zumindest ein sicherer Kanal für die laufende Kommunikation in Bezug auf die korrekte und sichere Benutzung des Zahlungsdienstes mit anzubieten. *Zum sicheren Kanal gehört beispielsweise ein vereinbartes, angemessen gesichertes elektronisches Postfach auf der Internetseite des Zahlungsdienstleisters oder eine sichere Webseite.*	
81	Die Kunden sind über diesen Kanal zu informieren. Ihnen ist zu erklären, dass jede Nachricht des Zahlungsdienstleisters in Bezug auf die korrekte und sichere Nutzung des Internet-Zahlungsdienstes über andere Ka-	

Tz	Anforderung	Anmerkung
	näle, z. B. E-Mail, nicht vertrauenswürdig ist.	
82	Der Zahlungsdienstleister hat über diesen Kanal Folgendes zu erläutern: • den Prozess für Kunden, um (möglicherweise) manipulierte Zahlungen, verdächtige Vorfälle oder Anomalien während eines Internet-Bezahlungsvorganges oder mögliche Social-Engineering-Angriffe zu melden; • die nächsten Schritte, z. B. wie der Zahlungsdienstleister dem Kunden antworten wird; • die Art und Weise, wie der Zahlungsdienstleister den Kunden über (möglicherweise) manipulierte Transaktionen bzw. deren Nichtausführung informieren wird, oder wie er den Kunden über das Auftreten von Angriffen (z. B. Phishing-E-Mails) warnen wird.	
83	Über ~~diesen~~ einen gesicherten Kanal sind die Kunden regelmäßig über Änderungen bei den Sicherheitsmaßnahmen in Bezug auf Internet-Zahlungsdienste zu informieren.	Es sollte eine Auswahl bzw. eine Kombination von mehreren Kanälen möglich sein.
84	Alle Warnungen über bedeutende neue Risiken (z. B. Social-Engineering) sind ebenfalls über diesen Kanal bereitzustellen.	
85	Es ist eine Kundenbetreuung für alle Fragen, Beschwerden, Bitten um Unterstützung und Meldungen von Anomalien und Vorfällen in Bezug auf Internet-Zahlungsdienste und zugehörigen Dienste zur Verfügung zu stellen.	
86	Die Kunden sind in geeigneter Weise darüber zu informieren, wie diese	

Tz	Anforderung	Anmerkung
	Kundenbetreuung in Anspruch genommen werden kann.	
87	Es sind angemessene Maßnahmen zur Kundenschulung und Kundensensibilisierung durchzuführen, ~~die sicherstellen, dass Kunden verstehen~~um Kunden zu erklären, • wie sie ihre Passwörter, Sicherheitstoken oder andere vertrauliche Daten schützen können, • wie sie die Sicherheit ihrer Geräte (z. B. PC) durch Installation und Update von Sicherheitskomponenten (z. B. Antivirus, Firewall, Sicherheitspatches) gewährleisten können, • wie sie die Gefahren und Risiken durch heruntergeladene Software einschätzen können, wenn der Kunde nicht sicher sein kann, dass die Software authentisch ist, • wie die korrekte Internetseite des Zahlungsdienstleisters sicher erkannt und benutzt wird.	Eine Sicherung von Verständnis ist bei Zahlungsdienstenutzern nicht möglich. Ein Hinwirken auf ein Verständnis ist praxisnäher.
88	Acquirer haben Online-Händler dazu aufzufordern, zahlungsrelevante Prozesse klar vom Online-Shop zu trennen, um es für Kunden einfacher zu machen, zu erkennen, wann sie mit dem Zahlungsdienstleister und nicht mit dem Zahlungsempfänger kommunizieren (z. B. im Falle einer Umleitung eines Kunden durch Öffnen eines neuen Fensters, so dass der Bezahlvorgang nicht im Rahmen des Online-Händlers gezeigt wird).	
	4.2 Benachrichtigungen und Festlegung von Limiten	
89	Es sind Limite für die Internet-Zahlungsdienste zu ~~setzen~~ ermöglichen und den Kunden Möglichkeiten für eine weitere Risikobegrenzung be-	Die Verpflichtung sollte sich nur auf die Ermöglichung beschränken, da es Kunden gibt (z. B. im gewerblichen Bereich), die heute

Tz	Anforderung	Anmerkung
	reitzustellen.	ohne Limit verfügen können.
90	Vor der Zulassung zur Nutzung des Zahlungsdienstes hat der Zahlungsdienstleister Limite zu setzen (z. B. maximaler Betrag pro Einzelzahlung oder kumulativer Betrag für einen bestimmten Zeitraum) und den Kunden darüber zu informieren.	Tz 89 und 90 sollten zusammengefasst werden.
91	Der Zahlungsdienstleister hat den Kunden zu ermöglichen, die ~~begrenzenden~~ Internet-Zahlungsfunktionen zu deaktivieren.	Empfehlung: Das Wort „begrenzenden“ sollte im Sinne des Originaltextes gestrichen werden, denn dort ist die Deaktivierung der Zahlungsfunktion und nicht die des Limits gemeint. (EBA/EZB: „PSPs should allow customers to disable the internet payment functionality.”).
	4.3 Kundenzugang zu Informationen über den Status der Zahlungsvorgänge	
92	Die erfolgreiche Ausführung der Zahlungsinitiierung ist den Kunden zeitnah zu bestätigen und dabei die notwendigen Informationen bereitzustellen, welche die Prüfung der korrekten Initiierung und Ausführung der Zahlung ermöglicht.	Hier sollte klargestellt werden, dass die Anforderungen nicht strenger sind als zivilrechtlich in Art. 248 §§ 7 ff. EGBGB gefordert.
93	Es ist den Kunden zu ermöglichen, jederzeit ihre Transaktionen und Kontosalden unverzüglich ~~jederzeit in Echtzeit~~ in einer sicheren und vertrauenswürdigen Umgebung zu überprüfen.	Es sollte berücksichtigt werden, dass teilweise nur ein oder zweimal am Tag Buchungsschnitte erfolgen. Diesem technischen Determinismus trägt die Originalformulierung „near real time“ besser Rechnung. Hinweis: Die Zahlungsverkehrs- und Banksysteme stellen Transaktionsdaten und Kontosalden zeitnah bereit, jedoch nicht in Echtzeit. Im Text der EZB wird auf „near real time“ verwiesen. Empfehlung: Anpassung der Formulierung: „Es ist den Kunden

Formatiert: Schriftartfarbe: Automatisch

Tz	Anforderung	Anmerkung
		zu ermöglichen, ihre Transaktionen und Kontosalden ohne Verzug / unverzüglich in einer sicheren und vertrauenswürdigen Umgebung zu überprüfen.“
94	Jeder elektronische Kontoauszug ist in einer sicheren und vertrauenswürdigen Umgebung zur Verfügung zu stellen.	
95	Informieren Zahlungsdienstleister Kunden über die Verfügbarkeit elektronischer Auszüge (z. B. immer wenn ein periodischer elektronischer Auszug übermittelt wurde oder ad-hoc nach Zahlungsinitiierung) über alternative Kanäle, wie SMS, E-Mail oder Brief, dürfen keine sensiblen Zahlungsdaten enthalten sein bzw. falls solche Daten enthalten sind, sind diese zu maskieren und wirksam zu schützen.	

Formatiert: Schriftartfarbe: Text 1