Bundesanstalt für
Finanzdienstleistungsaufsicht

BaFin

Konsultation 02/2015

Entwurf Mindestanforderungen an die Sicherheit von Internetzahlungen

Anmerkung: Erläuterungen zum Text des Rundschreibens sind kursiv gedruckt

Inhaltsübersicht

1. Anwendungsbereich

Tz 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 Internet 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.

2. Allgemeine Anforderungen an das Sicherheitsmanagement

2.1 Regelungen und Verantwortlichkeiten

Tz 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.

Tz 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.

Tz 5

Darin sind Sicherheitsziele zu definieren und die Risikobereitschaft festzulegen.

Tz 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 zu authentisieren (z.B. beim Login, bei der Ausführung von Internet-Zahlungen oder bei der Änderung oder Löschung von E-Mandaten).

2.2 Risikoanalyse

Tz 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-Sicherheitsvorfälle.

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".

Tz 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.

Tz 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 10

Die Risikoanalyse hat die Zielsetzung zu verfolgen, sensible Zahlungsdaten zu schützen und zu sichern.

Tz 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.

Tz 12

Darüber hinaus ist eine allgemeine Überprüfung der Risikobewertung mindestens einmal im Jahr durchzuführen.

Tz 13

Die Ergebnisse der Risikoanalysen und ihrer Überprüfung ist den zuständigen Führungskräften zur Genehmigung vorzulegen.

2.3 Überwachung und Berichtswesen zu IT-Sicherheitsvorfällen

Tz 14

Zahlungsdienstleister sollten Prozesse zur zentralen Registrierung, Beobachtung und Weiterverfolgung von IT-Sicherheitsvorfällen und sicherheitsbezogenen Kundenbe-

schwerden etablieren. Die IT-Sicherheitsvorfälle und sicherheitsbezogene Kundenbeschwerden sind an das Management zu berichten.

Tz 15

Kritische IT-Sicherheitsvorfälle sind an die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) 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 gemäß Anlage I und II zu erstatten.

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.*

Tz 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.

Tz 17

Acquirer haben vertraglich von den Online-Händlern, die sensible Zahlungsdaten speichern, verarbeiten oder übertragen, zu fordern, dass diese bei kritischen IT-Sicherheitsvorfällen sowohl mit den Zahlungsdienstleistern als auch mit den zuständigen Strafverfolgungsbehörden kooperieren.

Tz 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.

2.4 Risikokontrolle und -vermeidung

Tz 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 Verteidigungslinie kompensiert wird.*

Tz 20

Bei der Konzeption, Entwicklung und Pflege von Internet-Zahlungsdiensten ist auf die ausreichende Trennung von Aufgaben im Bereich der IT-Umgebung zu achten. Es sind angemessene Benutzerberechtigungsverfahren 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.

Tz 21

Netzwerke, Webseiten, Server und Kommunikationsverbindungen sind gegen Missbrauch oder Angriffe zu schützen.

Tz 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 aller überflüssigen Funktionen.

Tz 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.

Tz 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.

Tz 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.

Tz 26

Sicherheitsmaßnahmen für Internet-Zahlungsdienste 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.

Tz 27

Alle Änderungen sind einem angemessenen, formalen Änderungsverwaltungsprozess (Change-Management-Prozess) zu unterziehen.

Es soll sichergestellt werden, dass Änderungen richtig geplant, getestet, dokumentiert und autorisiert werden.

Tz 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.

Tz 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.

Tz 30

Übernehmen Externe Sicherheitsfunktionen für den Zahlungsdienstleister, so hat der Zahlungsdienstleister sicherzustellen, dass der Externe die Anforderungen dieses Rundschreibens einhält.

Tz 31

Acquirer haben von ihren Online-Händlern vertraglich zu verlangen, dass diese Sicherheitsmaßnahmen in ihrer IT-Infrastruktur implementieren, die den vorgenannten Anforderungen (Tzn. 20 bis 30) genügen.

2.5 Nachvollziehbarkeit von Transaktionen und E-Mandaten

Tz 32

Zahlungsdienstleister haben sicherzustellen, dass ihre Dienste Sicherheitsmechanismen für das detaillierte Loggen von Transaktionen und E-Mandaten beinhalten.

Zu den Logdaten gehören Transaktions-ID, Zeitstempel sowie Aufzeichnungen für Änderungen der Parametrisierung und des Zugriffs auf Transaktionsdaten.

Tz 33

Zur Nachvollziehbarkeit von Ergänzungen, Änderungen oder Löschungen von Transaktionen und E-Mandaten sind Logdateien zu erstellen.

Tz 34

Die Transaktions- und E-Mandat-Daten sind zu analysieren und es ist sicherzustellen, dass die Logdateien jederzeit mit angemessenen Werkzeugen ausgewertet werden können.

Tz 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

Tz 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-Geldwäsche-vorschriften und sonstigen relevanten Vorschriften korrekt zu identifizieren.

Tz 37

Es ist sicherzustellen, dass die erforderlichen vorvertraglichen Informationen, die dem Kunden ausgehändigt werden, Details zum Internet-Zahlungsdienst enthalten.

Welche vorvertraglichen Informationen an den Kunden erforderlich sind, ergibt sich aus der Zahlungsdiensterichtlinie 2007/64/EG in der jeweils geltenden Fassung.

Tz 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;
- 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.

Tz 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.

Tz 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 zu treffen.

Tz 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.

3.2 Starke Kundenauthentisierung

Tz 42

Für die Autorisierung von Internet-Zahlungen durch einen Kunden (inkl. Sammelüberweisungen) und für die Ausgabe oder Änderung von E-Mandaten ist starke Kundenauthentisierung 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 Verfahren 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). Die wesentlichen Transaktionsdaten müssen in die 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.

Tz 43

In folgenden Fällen können auch alternative Authentisierungsverfahren eingesetzt werden:

- ausgehende Zahlungen an vertrauenswürdige Empfänger, die in zuvor angelegten Listen als vertrauenswürdig akzeptierter Zahlungsempfänger (*White Lists*) dieses Kunden enthalten sind,
- Transaktionen zwischen zwei Konten desselben Kunden beim selben Zahlungsdienstleister,
- Transaktionen innerhalb desselben Zahlungsdienstleiters, die durch eine Risikoanalyse gerechtfertigt werden,
- Kleinstbetragszahlungen entsprechend der Zahlungsdiensterichtlinie 2007/64/EG.

Tz 44

Der Zugriff auf sensible Zahlungsdaten und die Änderung dieser Daten (inkl. Erzeugung und Änderung von White Lists) erfordert starke Authentisierung.

Tz 45

Sofern ein Zahlungsdienstleister ausschließlich solche Dienste 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.

Tz 46

Im Falle von Kartentransaktionen ist durch den kartenausgebenden Zahlungsdienstleister die starke Authentisierung des Karteninhabers zu unterstützen.

Tz 47

Alle ausgegebenen Karten müssen technisch dazu in der Lage sein, mit starker Authentisierung genutzt zu werden.

Tz 48

Acquirer haben Technologien zu unterstützen, die es dem Kartenausgeber erlauben, starke Authentisierung des Karteninhabers für Kartenzahlungssysteme durchzuführen, an denen der Acquirer teilnimmt.

Tz 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.

Tz 50

Die Nutzung alternativer Authentisierungsverfahren kann für vordefinierte Kategorien von Transaktionen mit niedrigem Risiko in Betracht gezogen werden.

Die Kategorien der alternativen Authentisierungsverfahren können beispielsweise auf einer transaktionsbezogenen Risikoanalyse basieren oder Kleinstbetragszahlungen gemäß Zahlungsrichtlinie 2007/64/EG berücksichtigen.

Tz 51

Die Regelungen zur Haftung haben starke Authentisierung in angemessener Weise zu berücksichtigen.

Tz 52

Für Kartenzahlungssysteme haben Anbieter von Wallet-Lösungen von den Kartenausgebern starke Authentisierung zu verlangen, wenn der legitimierte Karteninhaber die Kartendaten erstmalig registriert.

Tz 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.

Tz 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 Kleinstbetragszahlungen gemäß Zahlungsdiensterichtlinie 2007/64/EG.

Tz 55

Im Falle virtueller Karten hat die initiale Registrierung in einer sicheren und vertrauenswürdigen Umgebung zu erfolgen.

Tz 56

Bei Ausgabe von virtuellen Karten über das Internet ist für den Generierungsprozess der Daten der virtuellen Karten starke Authentisierung zu nutzen.

Tz 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

Tz 58

Anmeldung und Ausgabe von Authentisierungsmitteln und/oder Software an Kunden haben die folgenden Anforderungen zu erfüllen:

Tz 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 werden müssen.

Tz 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.

Tz 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.

Tz 62

Im Falle von Kartentransaktionen ist dem Kunden unabhängig von einem bestimmten Internet-Kaufvorgang die Möglichkeit anzubieten, sich für starke Authentisierung zu registrieren.

Tz 63

Wenn während des Online-Kaufvorgangs eine Aktivierung angeboten wird, hat dies mit Hilfe der Umleitung des Kunden in eine sichere und vertrauenswürdige Umgebung zu erfolgen.

Tz 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

Tz 65

Werden Einmalpasswörter (One-Time-Passwords, z. B. per ChipTan generierte Codes) für die Authentisierung genutzt, so ist deren Gültigkeit auf das notwendige Minimum zu begrenzen.

Tz 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.

Tz 67

Es ist ein sicheres Verfahren einzurichten, das es ermöglicht, gesperrte Internet-Zahlungsdienste zu reaktivieren.

Tz 68

Eine inaktive Session ist nach einer vorgegebenen Zeit automatisch zu beenden.

3.5 Transaktionsüberwachung

Tz 69

Es sind Systeme zur Erkennung und Verhinderung von Manipulationen einzusetzen, die verdächtige Transaktionen identifizieren, bevor die Transaktion bzw. das E-Mandat final autorisiert wird.

Derartige Systeme 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.

Tz 70

Die Systeme müssen auch in der Lage sein, Anzeichen einer Malware-Infektion in einer Session und bekannte Angriffsszenarien zu erkennen.

Tz 71

Umfang, Komplexität und die Anpassungsfähigkeit der Überwachung-Lösungen sind unter Einhaltung der einschlägigen Datenschutzvorschriften in angemessener Weise an den Ergebnissen der Risikobewertung auszurichten.

Tz 72

Acquirer haben Betrugserkennungs- und -verhinderungssysteme zu betreiben, die eine Überwachung der Aktivitäten der Online-Händler ermöglichen.

Tz 73

Transaktions-Screening- und Evaluierungsverfahren sind innerhalb angemessener Frist durchzuführen, so dass die Initiierung und/oder Ausführung des Internet-Zahlungsdienstes nicht unnötig verzögert wird.

Tz 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

Tz 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.

Tz 76

Es ist sicherzustellen, dass bei einem Austausch von sensiblen Zahlungsdaten über das Internet eine sichere Ende-zu-Ende-Verschlüsselung zwischen Bank und Kunde 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.

Tz 77

Acquirer haben ihre Online-Händler aufzufordern, keine sensiblen Zahlungsdaten zu speichern.

Tz 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.

Tz 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.

4. Schutz der Kunden

4.1 Kundenschulung und Kommunikation

Tz 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.

Tz 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 Kanäle, z. B. E-Mail, nicht vertrauenswürdig ist.

Tz 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.

Tz 83

Über diesen gesicherten Kanal sind die Kunden regelmäßig über Änderungen bei den Sicherheitsmaßnahmen in Bezug auf Internet-Zahlungsdienste zu informieren.

Tz 84

Alle Warnungen über bedeutende neue Risiken (z. B. Social-Engineering) sind ebenfalls über diesen Kanal bereitzustellen.

Tz 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.

Tz 86

Die Kunden sind in geeigneter Weise darüber zu informieren, wie diese Kundenbetreuung in Anspruch genommen werden kann.

Tz 87

Es sind angemessene Maßnahmen zur Kundenschulung und Kundensensibilisierung durchzuführen, die sicherstellen, dass Kunden verstehen,

- 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.

Tz 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

Tz 89

Es sind Limite für die Internet-Zahlungsdienste zu setzen und den Kunden Möglichkeiten für eine weitere Risikobegrenzung bereitzustellen.

Tz 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 91

Der Zahlungsdienstleister hat den Kunden zu ermöglichen, die begrenzenden Internet-Zahlungsfunktionen zu deaktivieren.

4.3 Kundenzugang zu Informationen über den Status der Zahlungsvorgänge

Tz 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.

Tz 93

Es ist den Kunden zu ermöglichen, ihre Transaktionen und Kontosalden jederzeit in Echtzeit in einer sicheren und vertrauenswürdigen Umgebung zu überprüfen.

Tz 94

Jeder elektronische Kontoauszug ist in einer sicheren und vertrauenswürdigen Umgebung zur Verfügung zu stellen.

Tz 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.