Internetzahlungen: Die **MaSI** sind in **Kraft**

Von Andres Prescher und Ulrike Schild

Bis zum 5. November dieses Jahres müssen die von der BaFin am 5. Mai veröffentlichten Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI) umgesetzt werden. Anpassungsbedarf in den IT-Systemen werden nach Einschätzung der Autoren vor allem die erhöhten Anforderungen an Sicherheits- und Risikoprozesse für die Autorisierung von Zahlungsaufträgen sowie die Einhaltung von Kundeninformationspflichten mit sich bringen. Auch Informationsmaterialien und Vertragswerke müssen angepasst werden. Der knappe Umsetzungzeitraum dürfte somit in jedem Fall eine Herausforderung darstellen. Red.

Am 5. Mai 2015 veröffentlichte die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) mit Rundschreiben 4/2015 (BA) die Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI). Diese dienen der Bekämpfung von Cyber-Kriminalität im Zahlungsverkehr und sollen das Vertrauen der Verbraucher in Internet-Zahlungsdienste stärken.

Hierzu decken die MaSI wesentliche Aspekte der Sicherheit im Retail-Zahlungsverkehr ab, welche insbesondere die Governance und das Risikomanagement sowie die Überwachung, Überprüfung und Dokumentation von Internet-Zahlungsvorgängen umfassen. Behandelt werden entsprechende Anforderungen an das Sicherheitsmanagement und die Steuerung (unter anderem Durchführung von Risikobewertungen, Berichtswesen zu IT-Sicherheitsvorfällen), besondere Sicherheitsmaßnahmen für Internet-Zahlungen (unter anderem Einführung einer sogenannten „starken" Kundenauthentifizierung, Schutz sensibler Zahlungsdaten bei Speicherung, Verarbeitung und Übermittlung) sowie weitere Vorgaben zum Kundenschutz (insbesondere Information und Schulung der Kunden zu Sicherheitsfragen). Diese Anforderungen treten als Spezialregelung neben die bekannten Mindestanforderungen an das Risikomanagement von Banken (MaRisk). Es ist deshalb mit einem erheblichen Umsetzungsaufwand bei den Zahlungsdienstleistungsunternehmen zu rechnen.

Regulatorischer Hintergrund

Die MaSI traten unmittelbar mit ihrer Veröffentlichung in Kraft und sind seitdem grundsätzlich einzuhalten. Allerdings hat die BaFin betroffenen Unternehmen eine – ihrerseits als ausreichend befundene – Umsetzungsfrist von sechs Monaten, also bis zum 5. November 2015, eingeräumt. Bis zu diesem Zeitpunkt will die BaFin vorerst von Sanktionen wegen einer Nichtbefolgung der MaSI-Anforderungen inklusive Meldungen absehen. Dennoch ist der Zeitrahmen für die Umsetzung äußerst knapp bemessen, da insbesondere eine Anpassung der IT-Systeme sehr zeitaufwendig ist.

Die MaSI basieren auf den am 19. Dezember 2014 veröffentlichten „Leitlinien zur Sicherheit von Internetzahlungen" der Europäischen Bankenaufsichtsbehörde (EBA), die bis zum 1. August 2015 von den nationalen Aufsichtsbehörden umzusetzen sind und die ihrerseits auf entsprechende Empfehlungen der SecuRePay Bezug nehmen. Bei der SecuRePay handelt es sich um ein europäisches Forum, welches sich aus verschiedenen Zentralbanken und Aufsichtsbehörden zusammensetzt. Dieses Forum hat keine Befugnisse rechtsverbindliche Regelungen zu erlassen, weshalb seine Empfehlungen auch keine unmittelbare Wirkung für ihre Adressaten entfalten.

Nach der Verordnung (EU) Nr. 1093/2010 darf die EBA Leitlinien und Empfehlungen für nationale Aufsichtsbehörden und Finanzinstitute herausgeben, um eine einheitliche Anwendung des Unionsrechts

Zu den Autoren

Andres Prescher und **Ulrike Schild**, beide Rechtsanwälte bei KPMG Rechtsanwaltsgesellschaft mbH, Frankfurt am Main

sicherzustellen und kohärente wirksame Aufsichtspraktiken sowie Chancengleichheit zu schaffen („Level-Playing-Field"). Aber auch die Leitlinien der EBA sind rechtlich nicht verbindlich.

Rechtsgrundlage für die Umsetzung in deutsches Recht ist vielmehr § 7 b Absatz 1 Kreditwesengesetz (KWG), wonach sich die BaFin an den Tätigkeiten der EBA beteiligt. Hierzu bedient sich die BaFin vorliegend eines Rundschreibens, welches die Anforderungen an Zahlungsinstitute hinsichtlich einer soliden Unternehmenssteuerung sowie angemessener interner Kontrollmechanismen konkretisiert.

Ein weiterer in diesem Zusammenhang relevanter regulatorischer Hintergrund ist die Überarbeitung der EU-Zahlungsdiensterichtlinie (Payment Services Directive, PSD 2). Die Arbeiten an der PSD 2 sind zwar noch nicht abgeschlossen, die MaSI sollen jedoch die Zeit bis zu deren Inkrafttreten überbrücken. Deshalb finden einige in der PSD 2 angedachte Regelungen (insbesondere bestimmte Sicherheitsanforderungen, zum Beispiel die mehrstufige Authentifizierung) bereits Niederschlag in den MaSI. Insoweit ist allerdings nicht auszuschließen, dass einzelne Regelungsinhalte der MaSI nach Veröffentlichung der PSD 2 noch einmal überarbeitet werden.

Von allen Zahlungsdienstleistern gemäß ZAG einzuhalten

Die MaSI müssen von allen Zahlungsdienstleistern im Sinne des Zahlungsdiensteaufsichtsgesetzes (ZAG) beachtet und eingehalten werden, die Zahlungsdienste über das Internet anbieten. Betroffen sind somit sämtliche Kreditinstitute, E-Geldinstitute und Unternehmen, die als Zahlungsinstitute gewerbsmäßig Zahlungsdienste erbringen.

Gegenstand der MaSI sind angemessene Regelungen zur Sicherheit für Internet-Zahlungsdienste, die von den Instituten aufzustellen, umzusetzen und regelmäßig zu überprüfen sind. Im Kern geht es um Risikobewertung, -kontrolle und -minderung. Betroffen davon sind alle Internetzahlungen und zugehörige Dienste, also konkret Überweisungen, Erteilung und Änderung elektronischer Lastschriftmandate, Kartenzahlungen (ohne Kreditgewährung) oder der Transfer von E-Geld zwischen zwei E-Geld-Konten. In diesem Bereich soll sich jeder Zahlungsdienstleister über alle von ihm eingegangenen beziehungsweise ihn möglicherweise betreffenden Risiken in vollem Umfang bewusst sein. Dabei geben die MaSI lediglich die zu erreichenden Ziele vor, überlassen die Mittel jedoch dem jeweiligen Institut.

Ging der ursprüngliche Entwurf der MaSI vom 4. Februar 2015 noch weit über die Vorschläge der EBA und der SecuRePay hinaus (zum Beispiel auch Erfassung des Telefonbankings), hat die BaFin hiervon – insbesondere aufgrund der scharfen Kritik der deutschen Banken, Zahlungsdienstleister und Handelsunternehmen – Abstand genommen. Nunmehr werden die Leitlinien der EBA fast wortgleich übernommen.

Allgemeines Kontroll- und Sicherheitsumfeld

Die MaSI verlangen, dass betroffene Institute Sicherheitsrichtlinien für Internetzahlungsdienste umsetzen, welche Sicherheitsziele und Risikobereitschaft, Rollen und Zuständigkeiten sowie Berichtswege festlegen. Unter anderem ist eine zuständige Risikomanagementfunktion zu benennen, welche direkt an die Geschäftsleitung berichtet. Die getroffenen Regelungen sind von der Geschäftsleitung zu genehmigen, ordnungsgemäß zu dokumentieren und regelmäßig – mindestens jährlich – sowie anlassbezogen zu überprüfen.

Die Risikomanagementfunktion hat eine – ebenfalls zu dokumentierende – Risikobewertung durchzuführen. Hierin sind unter anderem die vom Zahlungsdienstleister eingesetzten technischen Lösungen, die an externe Anbieter ausgelagerten Dienste und die technische Umgebung der Kunden einzubeziehen sowie die Risiken im Zusammenhang mit Technologieplattformen, Anwendungsarchitekturen, Programmiertechniken und Prozeduren zu berücksichtigen. Anhand der Ergebnisse der Risikobewertung sind erforderliche Änderungen an Sicherheitsverfahren, Technologien, Verfahren oder Zahlungsdiensten vorzunehmen.

Ein wichtiger Punkt der MaSI ist das Berichtswesen zu Sicherheitsvorfällen. Dabei sind Prozesse einzuführen, die eine Überwachung, Bearbeitung und Nachbereitung von Sicherheitsvorfällen sowie die Aufnahme sicherheitsbezogener Kundenbeschwerden und deren Meldung an die Geschäftsleitung beinhalten.

Neu ist, dass schwerwiegende Zahlungssicherheitsvorfälle an die Aufsicht (BaFin, Bundesbank) sowie die Datenschutzbehörden zu melden sind. Zudem ist ein Verfahren für die Zusammenarbeit mit den Strafverfolgungsbehörden vorzusehen. Für die Meldung an die BaFin sind den MaSI Meldebögen beigefügt.

Im Abschnitt „Risikokontrolle und -minderung" gehen die MaSI detailliert auf verschiedene technische Sicherheitsmaßnahmen ein. Neu ist hierbei insbesondere die Forderung eines „gestaffelten Sicherheitskonzepts", wobei nach dem Prinzip der Verteidigung in der Tiefe mehrere Verteidigungslinien eingezogen werden sollen (beispielsweise Identity & Access Management, Serverhärtung oder Datenminimierung). Die Sicherheitsmaßnahmen sollen in regelmäßigen Abständen überprüft werden.

„Starke Kundenauthentifizierung"

Kunden müssen vor Erteilung des Zugangs zu Zahlungsdiensten ordnungsge-

mäß identifiziert und über die Zahlungsdienste informiert werden sowie ihre Bereitschaft bestätigen, die Dienste für Internetzahlungen zu verwenden. Zur „starken Kundenauthentifizierung" wird dabei die Verwendung von mindestens zwei Elementen der drei Kategorien Wissen (zum Beispiel Passwörter oder PINs), Besitz (physische Gegenstände, zum Beispiel Smartphones) und Inhärenz (unveränderliche biologische Merkmale, zum Beispiel Fingerabdruck) vorgeschrieben.

Die verwendeten Elemente müssen voneinander unabhängig sein. Mindestens eines der Elemente darf nicht wiederverwendbar und nicht reproduzierbar sein und nicht heimlich über das Internet entwendet werden können. Zusätzlich soll die Gültigkeitsdauer von Einmalpasswörtern und die Anzahl von erlaubten ungültigen Anmeldeversuchen auf ein Minimum reduziert werden.

Ausnahmen für Kleinstbeträge oder Whitelists

Auch Karten müssen mit der starken Kundenauthentifizierung genutzt werden können. Bei der Verwendung von Karten sei insbesondere auf die Verpflichtung zum Aufbau sicherer und vertrauenswürdiger Umgebungen für die Registrierung und Aktivierung virtueller Karten sowie für die wechselseitige Authentifizierung in der Kommunikation zwischen Zahlungsdienstleister und Online-Händler hingewiesen.

Ein eingeräumter Spielraum für alternative Authentifizierungsformen greift nur in Ausnahmefällen, beispielsweise bei der Staffelung von Beträgen (Kleinstbeträge), bei Anwendung von „Whitelists" für vertrauenswürdige Empfänger oder auch bei Transaktionen zwischen zwei Konten derselben Person.

Als weiteres Sicherheitsmerkmal wird das Setzen von Limits für Transaktionen vorgeschrieben, innerhalb derer den Kunden zudem Möglichkeiten für eine weitere Risikobegrenzung bereitgestellt werden können (zum Beispiel kundenseitig einstellbare Limits).

Die Beantragung und Auslieferung von Authentifizierungs-Tools sowie die Bereitstellung von personalisierten Anmeldeinformationen, zahlungsbezogener Software und personalisierter Hardware muss in einer sicheren und vertrauensvollen Umgebung stattfinden. Dabei müssen mögliche Risiken berücksichtigt werden, die von Geräten ausgehen, die sich nicht unter der Kontrolle der Zahlungsdienstleister befinden. Auch elektronische Auszüge müssen innerhalb einer gesicherten Umgebung bereitgestellt werden.

Letztlich muss der Kunde auch die Authentizität und Integrität von Software, die über das Internet verteilt wird, prüfen und zur Überwachung und Nachvollziehbarkeit von Transaktionen „beinahe in Echtzeit" alle Informationen über den Status und Statusänderungen der von ihm initiierten Transaktionen einsehen können. Vor der endgültigen Autorisierung einer Transaktion ist zu prüfen, ob es Anzeichen für Betrug gibt (Transaktionsüberwachung). Hierzu sollen verdächtige oder risikobehaftete Transaktionen mittels EDV-gestützter Monitoring-Systeme identifiziert und einem Prüfungs- und Bewertungsprozess unterzogen werden.

Die MaSI stellen klare Anforderungen an den Umgang, die Übermittlung, das Speichern und die Verarbeitung von Daten. Im Detail zu definieren ist das Risikomanagement sensibler Zahlungsdaten, die genutzt werden können, um einen Kunden zu identifizieren und zu authentifizieren (zum Beispiel beim Log-in oder der Ausführung von Internetzahlungen).

Falls ein Online-Händler oder ein externer Dienstleister hier nicht wie vertraglich vereinbart kooperiert oder erforderliche Maßnahmen zur Gefahrenabwehr nicht umsetzt, hat der Zahlungsdienstleister entsprechende Schritte einzuleiten, um die vertraglichen Verpflichtungen durchzusetzen oder den Vertrag zu beenden. Ferner muss während des gesamten Zahlungsvorgangs eine sichere „End-to-End"-Verschlüsselung bestehen.

Kundenaufklärung, -information und -kommunikation

Die Kunden sollen in der sicheren Nutzung der Internetzahlungsdienste sowie im Umgang mit möglichen Sicherheitsvorfällen unterwiesen werden. Sie sollen verstehen, wie sie ihre Sicherheitsmerkmale und vertrauliche Daten schützen und die Sicherheit der von ihnen verwendeten Geräte wie PCs und Tablets herstellen und erhalten können.

Außerdem soll ein sicherer Kanal für die Kommunikation mit Kunden zur Benut-

zung des Zahlungsdienstes angeboten werden, über den regelmäßig und anlassbezogen über aktuelle Sicherheitsrisiken informiert wird. Zusätzlich soll ein Kundendienst bei Fragen, Beschwerden und Meldung von Unregelmäßigkeiten und Vorfällen unterstützen.

Implikationen und möglicher Handlungsbedarf für die Institute

Für das einzelne Institut richtet sich der konkrete Handlungsbedarf danach, ob und inwieweit die Anforderungen der MaSI bereits durch vorhandene Anwendungen, Prozesse und Regelungen abgedeckt sind. Insoweit umfassen zum einen die MaRisk bereits wesentliche Anforderungen auch des Risikomanagements von Internetzahlungen, welche durch die MaSI lediglich weiter spezifiziert werden. Zum anderen sind einige der in den MaSI kodifizierten technischen Anforderungen, zum Beispiel an Log-in-Daten, Einmalpasswörter, Limits oder Session-Timeouts, bereits weitgehend Standard im Online-Banking.

In einem ersten Schritt sind daher die IT-Systeme auf Relevanz und Einhaltung der in den MaSI zusammengefassten Sicherheitsfunktionalitäten zu überprüfen. Die notwendige Klarheit über den individuellen Umsetzungsaufwand kann nur eine detaillierte Analyse des Status quo und der Anforderungen der MaSI schaffen. Da Bereiche von der Strategie über die IT bis zum Kunden betroffen sind, ist ein ganzheitlicher Projektansatz empfehlenswert.

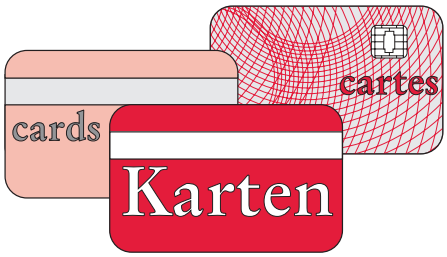
Für viele betroffene Institute dürften die erhöhten Anforderungen an Sicherheits- und Risikoprozesse für die Autorisierung von Zahlungsaufträgen sowie die Einhaltung von Kundeninformationspflichten eine Anpassung des Sicherheitskonzepts sowie gegebenenfalls die Implementierung geeigneter Methoden, Tools, Software oder anderer IT-Lösungen mit sich bringen.

Darüber hinaus sollte die durch die neuen Vorschriften veranlasste Überprüfung der Risikobewertungsprozesse auch zur Definition und Umsetzung einer umfassenden Sicherheitsstrategie genutzt werden, inklusive der Analyse der Auswirkungen auf das bestehende Risk Operating Model inklusive Richtlinien, Organisation und Prozessen.

Alle Institute müssen eine laufende Risikobewertung und -evaluierung der eingesetzten Technologien und Dienste etablieren sowie Prozesse für die frühzeitige Erkennung und Bewertung von Risiken und Sicherheitsvorfällen implementieren. Hierfür empfiehlt sich unter anderem die Definition von geeigneten quantitativen und qualitativen Indikatoren, die Konkretisierung von Berichtslinien oder die Einführung spezieller Intrusion-Detection- und Reporting-Systeme.

Knapper Umsetzungszeitraum als Herausforderung

Die Einführung kundenseitig bedienbarer Limitsysteme bedingt Anpassungen von Funktionalitäten in Online-Banking-Portalen und Kontrollen in Abwicklungssystemen. Die Erfüllung der Sicherheitsstandards in eingesetzter Hard- und Software berührt auch Produkte und Anwendungen, die dem Kunden für Internetzahlungen bereitgestellt wurden. Nicht zuletzt betrifft die Herstellung von Transparenz über eingesetzte Zahlungsmechanismen und die umfassende vorvertragliche Information der Kunden die Bereiche von Marketing, Kundenbetreuung und Recht, welche ihre Informationsmaterialien oder Vertragswerke anzupassen haben. Insbesondere stellt der sehr kurze Zeitraum bis zur verpflichtenden Umsetzung zum 5. November 2015 eine Herausforderung dar, müssen doch zahlreiche Prozesse umgesetzt und IT angepasst werden. Der damit einhergehende Aufwand und die damit verbundenen Herausforderungen sind nicht zu unterschätzen. Die Zeit drängt. ■



Verlag und Redaktion:
Verlag Fritz Knapp GmbH
Postfach 111151, 60046 Frankfurt am Main,
Aschaffenburger Straße 19, 60599 Frankfurt am Main,
Telefon 0 69/97 08 33-0,
Telefax 0 69/7 07 84 00,
E-Mail: red.karten@kreditwesen.de
www.kreditwesen.de

Herausgeber: Klaus-Friedrich Otto

Chefredaktion: Dr. Berthold Morschhäuser, Swantje Benkelberg, Philipp Otto.

Redaktion: Horst Bertram (CvD), Maite Beisser, Barbara Hummel, Frankfurt/M.

Die mit Namen versehenen Beiträge geben nicht immer die Meinung der Redaktion wieder. Bei unverlangt eingesandten Manuskripten ist anzugeben, ob dieser oder ein ähnlicher Beitrag bereits einer anderen Zeitschrift angeboten worden ist. Beiträge werden nur zur Alleinveröffentlichung angenommen.

Die Zeitschrift und alle in ihr enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig.

Manuskripte: Mit der Annahme eines Manuskripts zur Veröffentlichung erwirbt der Verlag vom Autor das ausschließliche Verlagsrecht sowie das Recht zur Einspeicherung in eine Datenbank und zur weiteren Vervielfältigung zu gewerblichen Zwecken in jedem technisch möglichen Verfahren. Die vollständige Fassung der Redaktionsrichtlinien finden Sie unter www.kreditwesen.de.

Verlags- und Anzeigenleitung: Uwe Cappel

Anzeigenverkauf:
Hans-Peter Schmitt, Tel. 0 69/97 08 33-43.

Anzeigendisposition:
Alexander Schumacher, Tel. 0 69/97 08 33-26,
sämtl. Frankfurt am Main, Aschaffenburger Straße 19.

Zurzeit gilt Anzeigenpreisliste Nr. 26 vom 1.1.2015.

Erscheinungsweise: Jeweils am 1. Februar, 1. Mai, 1. August und 1. November 2015.

Diese Ausgabe liegt der Zeitschrift „bank und markt – Zeitschrift für Retailbanking", Heft 8/2015, als Supplement bei.

Bezugsbedingungen: Abonnementspreise incl. MwSt. und Versandkosten: jährlich € 138,17. Ausland: jährlich € 139,37. Preis des Einzelheftes € 27,50 (zuzügl. Versandkosten).

Studentenabonnement: 50% Ermäßigung (auf Grundpreis).

Zusätzliche, kostenlose Serviceleistung für alle „Karten"-Abonnenten: 8xjährlich der „Karten"-Infobrief aus „bank und markt – Zeitschrift für Retailbanking".

Probeheftanforderungen bitte unter 0 69/97 08 33-25.

Der Bezugszeitraum gilt jeweils für ein Jahr. Er verlängert sich automatisch um ein weiteres Jahr, wenn nicht einen Monat vor Ablauf dieses Zeitraumes eine schriftliche Abbestellung vorliegt.

Bestellungen direkt an den Verlag oder an den Buchhandel.

Bei Nichterscheinen ohne Verschulden des Verlages oder infolge höherer Gewalt entfallen alle Ansprüche.

Bankverbindungen:
Landesbank Hessen-Thüringen – Girozentrale,
Frankfurt am Main IBAN: DE73 5005 0000 0010 5550 01
BIC: HELADEFF
Postbank Frankfurt IBAN: DE96 5001 0060 0060 4826 09
BIC: PBNKDEFF

Druck: Druck- und Verlagshaus Zarbock GmbH & Co. KG, Sontraer Straße 6, 60386 Frankfurt am Main.

ISSN 0937-597X