von **Sarah Thomamüller**

Neue Mindestanforderungen zur Sicherheit von Internetzahlungen

Seit Mai 2015 existiert ein neues Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) mit Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI). Nach einer sechsmonatigen Umsetzungsfrist traten die neuen Regelungen am 5. November 2015 in Kraft.

Was ist der wesentliche Inhalt?

Die MaSI führen für alle Online-Zahlungen verpflichtend eine weitere Methode zur Kundenauthentifizierung ein, sog. "starke Kundenauthentifizierung". Das bedeutet, dass es nicht mehr ausreicht, wenn sich der Kunde zum Beispiel über PIN oder Passwörter identifiziert. Nach den MaSI muss er sich nunmehr über zwei der drei folgenden Möglichkeiten authentifizieren:

- Wissen des Kunden (z.B. Passwort, PIN)
- Gegenstand im Besitz des Kunden (z.B. Smartcard, Mobiltelefon)
- biometrisches Merkmal des Kunden (z.B. Fingerabdruck).

Neben der starken Kundenauthentifizierung sollen sensible Zahlungsdaten (Daten, die für Betrugszwecke missbraucht werden können) durch Zugriffsschutz und Verschlüsselung besonders geschützt werden und schwerwiegende Zahlungssicherheitsvorfälle an die BaFin gemeldet werden. Ein solcher Vorfall liegt vor, wenn ein Angriff wesentliche Auswirkungen auf die Sicherheit, Integrität oder Kontinuität der Zahlungssysteme und/oder die Sicherheit sensibler Zahlungsdaten oder -mittel hat oder haben könnte.

An wen richten sich die Mindestanforderungen?

Die MaSI richten sich an Bankinstitute, die öffentliche Verwaltung und Zahlungsdienstleister gem. § 1 Abs. 1 ZAG, also solche Einrichtungen, die direkt der Bankenaufsicht unterliegen.

Welche Vorgänge werden von den Anforderungen erfasst?

Betroffen sind nur Zahlungsvorgänge mit Beträgen über 30 ?.

Der Kauf auf Rechnung, sowie das Lastschriftverfahren bleiben weiter ohne Einschränkungen möglich. PayPal ist als Zahlungsdienstleister ebenfalls nicht betroffen, da er nicht der deutschen Bankenaufsicht unterliegt.

Möglich ist theoretisch -in der Praxis aber noch kaum wahrgenommen-, dass Kunden vertrauenswürdige Shops auf eine "Whitelist" bei ihren Banken setzen können, sodass die erweiterte Kundenauthentifizierung entfällt und weiterhin die einfache Identifizierung ausreicht.

Was müssen Online Händler nun tun?

Grundsätzlich müssen Händler in ihren Online Shops nun garantieren, dass eine zweite Art der Kundenauthentifizierung zur Verfügung steht. Ob eine Erweiterung der Authentifizierung überhaupt erforderlich ist und wie diese im konkreten Fall aussehen soll, sollte direkt mit den jeweiligen Zahlungsdienstleistern abgesprochen werden.

Bei Transaktionen mit geringem Risiko oder bei Kleinbetragszahlungen kann gegebenenfalls auch auf andere Authentifizierungsmethoden zurückgegriffen werden.

Weiter müssen sensible Zahlungsdaten, die gespeichert, verarbeitet oder übermittelt werden, besonders geschützt werden. Nur dann haben Online Händler auch Zugriff auf diese Daten bei ihrem Zahlungsdienstleister. Näheres regeln hier die jeweiligen Verträge zwischen Zahlungsdienstleistern und Händlern.

Schwere Sicherheitsvorfälle und Angriffe auf ihr System sind von den Händlern zu melden; sie haben im Ernstfall mit Zahlungsdienstleistern und Strafverfolgungsbehörden zu kooperieren.

Mit welchen Konsequenzen müssen Online Händler bei Nichtbeachtung rechnen?

Online-Händler können bei Nichteinhalten der Verträge mit den Zahlungsdienstleistern von diesen abgemahnt werden. Zahlungsdienstleister können darüber hinaus Sanktionen verhängen oder eine Kündigung des Vertrags vornehmen.

Die BaFin selbst wird Strafen nicht verhängen, jedoch handelt es sich bei allen Vorschriften um "Soll"-Vorgaben, die prinzipiell auch als verpflichtend zu verstehen sind.

Zukunftsaussichten

Im Oktober hat das Europäische Parlament den Vorschlag der Kommission über Vorschriften für mehr Sicherheit und Innovation bei europäischen Zahlungen angenommen, eine überarbeitete Zahlungsdiensterichtlinie, sog. PSD2. Auch sie sollen den Verbraucherschutz stärken. Die Mitgliedsstaaten haben zwei Jahre Zeit um die Richtlinien umzusetzen.

Autor:
Sarah Thomamüller
(freie jur. Mitarbeiterin der IT-Recht Kanzlei)