Infoblatt zur „Starken Kundenauthentifizierung“

13.09.2019

Um was geht es?

PSD2 = Payment Service Directive / Zahlungsdiensterichtlinie

SKA = Starke Kundenauthentifizierung

Umsetzung der starken Kundenauthentifizierung

Um den EU-Binnenmarkt weiter zu stärken und elektronische Zahlungen sicherer zu machen, wurde 2015 die zweite Zahlungsdiensterichtlinie (Payment Service Directive 2, PSD2) verabschiedet. Eine Regelung der Richtlinie betrifft die sogenannte starke Kundenauthentifizierung (SCA bzw. SKA) bei elektronischen Zahlungen (z. B. Kreditkartenzahlungen im E-Commerce).

Grundbegriffe

Starke Kundenauthentifizierung (SKA): Zwei aus drei Faktoren notwendig

❶ Wissen
❷ Besitz
❸ Inhärenz

Wissen, Besitz, Inhärenz

Starke Kundenauthentifizierung heißt, dass fast alle elektronischen Zahlungen mit zwei der folgenden drei Faktoren bestätigt werden müssen:

(1) Wissen (etwas, was der Nutzer weiß, z. B. Pin/Passwort)
(2) Besitz (etwas, was der Nutzer besitzt, z. B. Smartphone/App oder Karte/Chip)
(3) Inhärenz (etwas, das dem Nutzer inne ist, z. B. Fingerabdruck oder Stimme)

Wer ist betroffen?

Elektronische Zahlung? -> Absicherung durch SKA!

Stichtag für Umsetzung: 14.9.2019

Die neuen Regelungen gelten sowohl für den stationären als auch den Online-Handel

Die neuen Regelungen zur starken Kundenauthentifizierung betreffen elektronische Zahlungsvorgänge innerhalb der EU und wirken sich sowohl auf den stationären als auch auf den Online-Handel aus. Stationär ist die starke Kundenauthentifizierung jedoch nicht neu. Die Bezahlung mit girocard oder Kreditkarte wird grundsätzlich durch zwei Faktoren abgesichert. Hier wird durch die physische Karte bzw. durch den Chip das Merkmal Besitz und durch die Eingabe der PIN das Merkmal Wissen nachgewiesen.

Bezahlt man allerdings mit seiner Kreditkarte in einem Online-Shop, genügt es häufig, nur die Daten der Karte (Kreditkartennummer, Ablaufdatum und Prüfziffer) anzugeben. Betrachtet man z. B. die übliche PayPal-Nutzung, wird hier auch nur das Merkmal Wissen (Benutzername und Passwort) abgefragt, um eine Zahlung erfolgreich abzuschließen. Aufgrund der neuen gesetzlichen Bestimmungen reicht dies ab 14. September 2019 nicht mehr aus.

Wichtig: Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) –

Übergangsfrist verlängert!

die zuständige Aufsichtsbehörde für die Umsetzung der Regelung in Deutschland – hat am 21. August 2019 bekannt gegeben, dass Kreditkartenzahlungen im Internet ab dem 14. September 2019 weiterhin auch ohne starke Kundenauthentifizierung ausgeführt werden dürfen, da sie bei den Zahlungsempfängern noch erheblichen Anpassungsbedarf sieht. Dies ist jedoch zeitlich befristet – einen genauen Zeitrahmen legt die BaFin noch fest.

Ausnahmen

Whitelisting, Kleinbetragszahlungen, wiederkehrende Zahlungen und Transaktionsrisikoanalyse

Keine Regel ohne Ausnahmen

Der Gesetzgeber stellt klar, dass im Grundsatz jeder elektronische Zahlungsvorgang mit einer starken Kundenauthentifizierung durchzuführen ist. Allerdings kann bei Vorliegen bestimmter Voraussetzungen auf die starke Authentifizierung verzichtet werden. Ob eine Ausnahme angewendet oder genutzt werden kann, entscheidet nicht der Händler, sondern der kontoführende Zahlungsdienstleister, also in den meisten Fällen die Bank des Kunden.

Whitelisting

Vertrauenswürdige Empfänger (Whitelisting):
Kunden können u. a. Händler auf eine sogenannte Whitelist, also eine Positivliste von vertrauenswürdigen Zahlungsempfängern setzen, die von ihrem Zahlungsdienstleister geführt wird. Whitelist-Händler sind – in der Regel – von der starken Kundenauthentifizierung ausgenommen.

Kleinbetragszahlungen

Kleinbetragszahlungen:
Auf eine starke Kundenauthentifizierung kann verzichtet werden, wenn der Einzelbetrag der Online-Zahlung nicht größer als 30 € (bei stationären kontaktlosen Kartenzahlungen 50 €) , der Gesamtbetrag der früheren Online-Zahlungen seit der letzten starken Kundenauthentifizierung nicht größer als 100 € (stationär kontaktlos 150 €) oder die Anzahl der aufeinanderfolgenden Online-Zahlungen seit der letzten starken Kundenauthentifizierung nicht größer als fünf ist.

Wiederkehrende Zahlungen

Wiederkehrende Zahlungsvorgänge (z. B. Dauerauftrag):
Bei Erstellung, Änderung oder Auslösung wiederkehrender Zahlungen (gleicher Betrag, gleicher Zahlungsempfänger) ist eine starke Kundenauthentifizierung erforderlich, bei weiteren Zahlungen innerhalb einer solchen Serie nicht mehr.
Transaktionsrisikoanalyse:

Infoblatt zur „Starken Kundenauthentifizierung“

13.09.2019

Transaktionsrisikoanalyse

Für jede Zahlung (Überweisungen, Kartenzahlungen) wird untersucht, ob ein Betrugsrisiko vorliegt. Ist das Risiko gering und überschreitet der Zahlungsdienstleister eine bestimmte Betrugsrate nicht (abhängig von Betrag und Zahlungsverfahren), kann der Zahlungsdienstleister auf eine SKA bei Zahlungen bis maximal 500 € verzichten.

Was ist zu tun?

Worauf Sie sich als Händler vorbereiten sollten

Information

- Zunächst sollten Sie sich als Händler mit den neuen gesetzlichen Vorgaben vertraut machen. Kontaktieren Sie hierzu auch Ihren Payment Service Provider und/oder die Anbieter Ihrer Zahlungsverfahren. Viele bieten Infomaterial zur Umsetzung an.

Technische Anpassungen nötig?

Lastschrift/Rechnung/Vorkasse/Nachnahme sind nicht betroffen!

- Zudem sollten Sie mit Ihren Zahlungsdienstleistern klären, ob und welche technischen Anpassungen nötig sind. Dies hängt vor allem von den angebotenen Zahlungsverfahren ab. Die Lastschrift ist von den Anforderungen der starken Kundenauthentifizierung ausgenommen. Rechnung/Vorkasse/Nachnahme werden losgelöst von der eigentlichen Bestellung abgewickelt und sind nicht Teil des Bezahlprozesses im Online-Shop. Sollten Sie daher nur diese Zahlverfahren anbieten, müssen Sie keine Anpassungen vornehmen.

3-D Secure schon im Einsatz?

- Wenn Sie als Online-Händler Kreditkartenzahlungen akzeptieren, müssen diese – spätestens bei Einführung der starken Kundenauthentifizierung – mit dem Sicherheitsprotokoll 3-D Secure abgesichert werden. Auch hierzu sollten Sie sich an Ihren Payment Service Provider und/oder Kreditkartenacquirer wenden.

Kundeninformation

- Nach der Umsetzung eventueller Anpassungen testen Sie diese ausführlich und informieren Sie Ihre Kunden bzw. stellen ihnen eine Anleitung für die neuen Bezahlprozesse zur Verfügung.

AGB & Datenschutzerklärung überprüfen

- Überprüfen Sie, inwieweit durch die geänderten Bezahlprozesse Anpassungen in Ihren AGB und Ihrer Datenschutzerklärung notwendig sind.

Schulen Sie Ihre Mitarbeiter!

- Ihr Kundensupport sollte die ggf. neuen Bezahlprozesse kennen und auf Nachfragen der Kunden vorbereitet sein.

Infoblatt zur „Starken Kundenauthentifizierung“

4

13.09.2019

Zusammenfassung

Die starke Kundenauthentifizierung wird den Zahlungsverkehr – besonders im Online-Handel – verändern. Damit es kein böses Erwachen gibt, sollten sich Online-Händler informieren und vorbereiten. Die ggf. nötigen technischen Anpassungen in den Bezahlprozessen sollten ausgiebig getestet und im Nachgang für die Kunden verständlich dargestellt werden.

Rechtliche Grundlagen

Die rechtlichen Grundlagen für die starke Kundenauthentifizierung sind die PSD2 sowie die sie ergänzenden regulatorisch technischen Standards (RTS). Die aufsichtsrechtlichen Bestimmungen finden sich dabei im Zahlungsdiensteaufsichtsgesetz (ZAG) und die zivilrechtlichen Vorgaben im Bürgerlichen Gesetzbuch (BGB) wieder. Die RTS und damit die neuen Regelungen zur starken Kundenauthentifizierung sind grundsätzlich ab bzw. seit dem 14. September 2019 für Zahlungstransaktionen verpflichtend.

- Richtlinie (EU) 2015/2366 über Zahlungsdienste im Binnenmarkt (PSD2): https://bit.ly/2KKlka1
- Delegierte Verordnung (EU) 2018/389 zu technischen Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation (RTS): https://bit.ly/2Z0ncAH
- Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz – ZAG): https://bit.ly/2ORhEZu
- Bürgerliches Gesetzbuch (BGB), § 675c bis § 676c: https://bit.ly/301AuhI

Impressum

Autoren

Nils Deichner | ibi research GmbH | Galgenbergstraße 25 | 93053 Regensburg, Mail: nils.deichner@ibi.de
Dr. Ernst Stahl | ibi research GmbH | Galgenbergstraße 25 | 93053 Regensburg, Mail: ernst.stahl@ibi.de

Redaktion

Dr. Ulrike Regele | DIHK - Deutscher Industrie- und Handelskammertag e. V. | Breite Straße 29 | 10178 Berlin
Mail: regele.ulrike@dihk.de