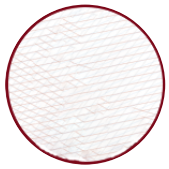
bankenverband

Blog

Cybersicherheit ist Daueraufgabe – nicht nur für Banken

30.09.2019

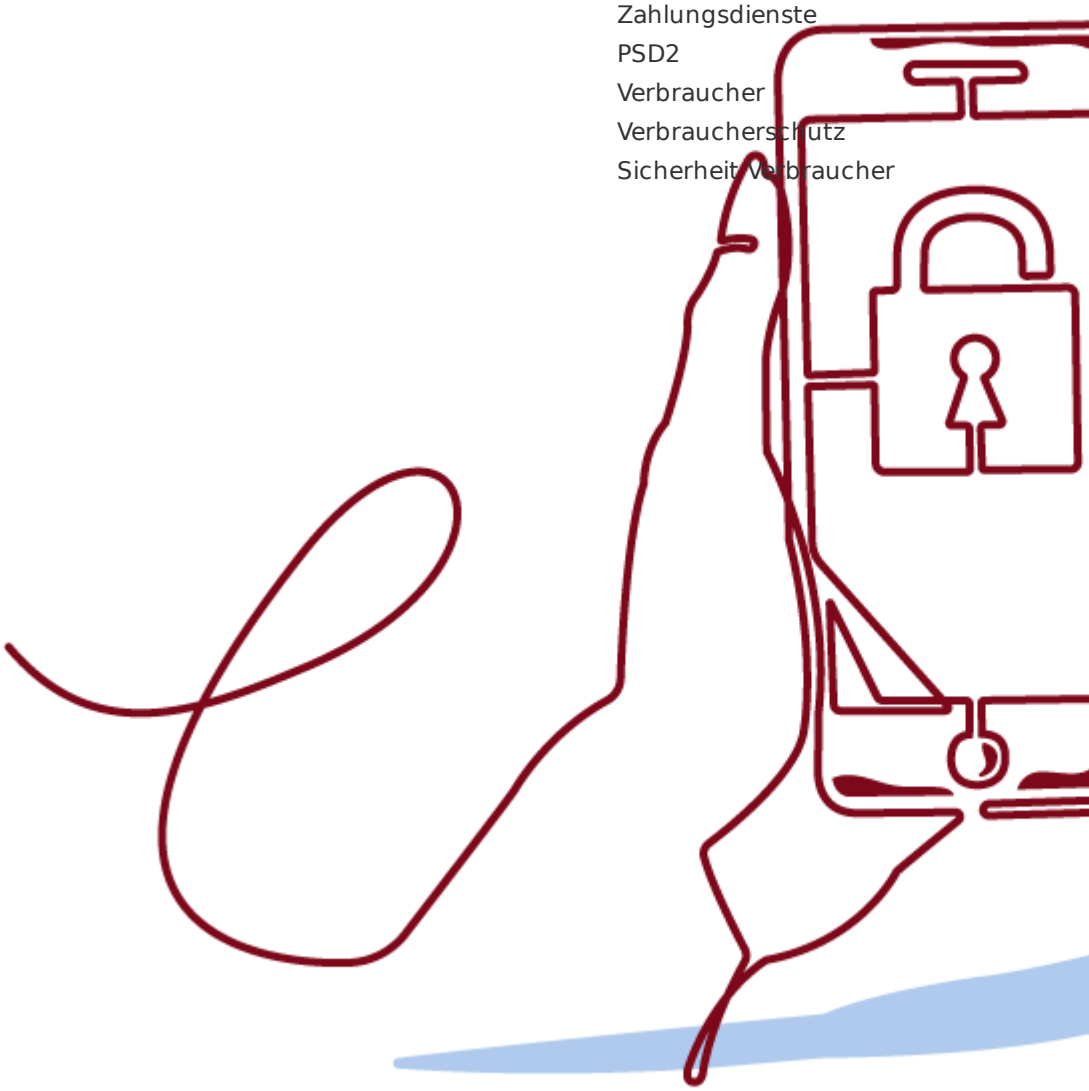
von



Schuster, Fabian

Schlagworte

Cyberattacken
Cybersicherheit
Cyberkriminalität
ECSM
Zahlungsdienste
PSD2
Verbraucher
Verbraucherschutz
Sicherheit Verbraucher



Blog

Mit dem 14. September dieses Jahres hat sich für Bankkunden einiges geändert: Neue gesetzliche Anforderungen für das Onlinebanking und Kartenzahlungen, kurz PSD2, sind in Kraft getreten. Diese dienen einem großen Ziel: Dem Schutz des Kunden vor Cyberbetrug. Und dies europaweit nach gleichen Regeln.

Schutz vor Betrug mit Zwei-Faktor-Authentifizierung

Die meisten Bankkunden kommen mit der PSD2 vor allem aus zwei Gründen in Berührung: Erstens, weil mit ihr die noch aus den Anfangszeiten des Onlinebanking stammende iTAN (Liste) weitestgehend Geschichte ist. Zweitens, weil damit neue Anforderungen an den Kontozugriff im Onlinebanking verbunden sind. Durch die sogenannte Starke Kundenauthentifizierung, eine Freigabe mit zwei Faktoren, wird der Prozess beim Log-In besser geschützt.

Natürlich bedeuten die Neuerungen für Bankkunden zunächst einmal eine Umgewöhnung: Zusätzlich zur bisherigen Eingabe beim Log-In muss nun auch eine eigens generierte Transaktionsnummer (TAN) eingegeben oder eine Bestätigung über ein verknüpftes Gerät vorgenommen werden. Ja, das ist erstmal aufwändiger und damit weniger bequem für den Nutzer. Aber sollte man aus Bequemlichkeit auf Sicherheit verzichten? Die Antwort darauf kann nur ein klares Nein sein. Denn die gute Nachricht lautet: das „Phishing“, bei dem Betrüger Zugangsdaten des Kunden abfangen, ist durch den neuen Sicherheitsstandard für Angreifer wirtschaftlich unattraktiv bis unmöglich geworden. Und auch der Kontozugriff ist für Kriminelle durch die Zwei-Faktor-Authentifizierung deutlich erschwert. Selbst wenn der Betrüger durch Phishing in den Besitz von Kontonummer oder Passwort gelangt sein sollte, kann er hiermit keine Zahlung auslösen. Hier schiebt die Zwei-Faktor-Authentifizierung einen Riegel vor.

Zwei-Faktor-Authentifizierung künftig auch für Social-Media-Accounts?

Während die Banken die Umstellung auf das neue Sicherheitsverfahren nun flächendeckend vollzogen haben, wird mit Blick auf weitere digitale Anwendungen andernorts über die Zwei-Faktor-Authentifizierung noch intensiv diskutiert. Insbesondere seitdem mehrere Fälle bekannt wurden, bei denen Kriminelle Social-Media-Accounts Prominenter zeitweise übernommen und missbraucht hatten, unterstützen auch immer mehr Online-Dienste den neuen Sicherheitsstandard; allerdings ist bisher nur von einer optionalen und nicht verbindlichen Einführung die Rede. Von politischer Seite gibt es daher nicht unberechtigte Vorstöße, Internet-Dienste zu einer Umstellung zu verpflichten, um den Nutzern eine größere Sicherheit vor unbefugten Zugriffen zu bieten. Wahrscheinlich ist es also nur eine Frage der Zeit, bis wir in nahezu allen Bereichen der

digitalen Welt solche Sicherheitsmaßnahmen vorfinden werden.

Der Mensch als Einfallstor für Cyber-Angriffe

Dennoch greifen die derzeitigen Diskussionen um technische Sicherheitsvorkehrungen zu kurz. Denn es steht außer Frage, dass auch die jeweils neuesten Verfahren Angriffe von Betrügern nicht gänzlich unterbinden können. Weil Cybersicherheit ein hochkomplexes Aktionsfeld mit vielen Beteiligten ist, wäre es fahrlässig, das Thema nur unter dem Gesichtspunkt der technischen Sicherheit zu betrachten. Erfahrungsgemäß ist der Mensch immer noch das größte Einfallstor für Bedrohungen aus dem digitalen Raum. So zielt ein Großteil der bekannten Angriffsszenarien von Kriminellen darauf ab, menschliches Verhalten zu manipulieren, um technische Sicherheitsmaßnahmen zu überwinden (sog. Social Engineering). Ganz gleich ob durch Phishing, CEO-Fraud oder Technical Support Scam – Online-Betrüger versuchen immer wieder, mit gefälschten Mails, Informationen oder „gefakten“ Websites Kunden dazu zu verleiten, persönliche Daten preiszugeben oder Transaktionen zu veranlassen.

Information, Sensibilisierung, Aufklärung

Um Schaden zu vermeiden, sind alle beteiligten Akteure gefordert: Die Nutzer sollten sich möglicher Konsequenzen ihrer Handlungen im digitalen Raum stets bewusst sein und entsprechend umsichtig agieren. Unternehmen sollten sich selbst in der Verantwortung sehen, ihre Kunden regelmäßig aufzuklären. Und schließlich ist auch der Staat gefordert, möglichst einheitliche Rahmenbedingungen für die Sicherheit von Informationstechnologien und elektronischen Informationen zu schaffen, um eine wirksame „Verteidigungslinie“ gegenüber Cyberangriffen aufzubauen.

Als Bankenverband setzen wir uns seit Jahren für mehr Cybersicherheit ein und leisten unseren Beitrag zur Verbraucheraufklärung und Betrugsprävention im digitalen Raum. Der Schutz persönlicher Daten im Netz, insbesondere beim Banking, ist für uns ein zentrales Thema, über das wir auch im Rahmen des European Cyber Security Month (ECSM) umfassend informieren.

Mehr zum Thema Cybersicherheit können Sie hier nachlesen.