PSD2: Open Banking braucht Sicherheit

Interview mit Daniel Heck

Durch Umsetzung der EU-Richtlinie Payment Services Directive 2 (PSD2) müssen Banken auf Wunsch des Kunden externen Finanzdienstleistern Zugriff auf seine Daten geben. So fordert es die PSD2, deren zweite Stufe am 14. September 2019 in Kraft getreten ist. Durch dieses „Open Banking“ sollen Wettbewerb und Service beim Onlinebanking erhöht werden. Die neue Schnittstelle bietet aber auch einen neuen Angriffspunkt für Hacker, sagt Daniel Heck von Rohde & Schwarz Cybersecurity im FLF-Gespräch. (Red.)

FLF Die BaFin hat überraschend ja nochmal einen Aufschub bei der Umsetzungsfrist angekündigt – was bedeutet das konkret für die Banken?

Die Ausweitung der Frist betrifft das Identitätsmanagement von Internetdiensten. Der Aufschub hat keine Auswirkungen auf die Übertragung der Kundendaten an Drittanbieter. Seit dem 14. September müssen Banken sicherstellen, dass Kontoinformations- und Zahlungsauslösedienste per PSD2-Application Programming Interfaces (API) auf die Kontodaten des Nutzers zugreifen und Transaktionen durchführen können. Banken sollten diese APIs ab sofort gegen Angreifer absichern.

Daniel Heck, Vice President Marketing, Rohde & Schwarz Cybersecurity GmbH, München

FLF Herr Heck, die Banken benötigen also Ihrer Meinung nach dringend neue Sicherheitskonzepte, um die Kundendaten vor Missbrauch zu schützen. Warum ist PSD2 hier ein Auslöser?

PSD2 öffnet mit ihrer zweiten Stufe den Zahlungsverkehr gegenüber Drittparteien. Durch dieses „Open Banking“ können Kunden beispielsweise beim Einkauf im Internet Zahlungsauslösedienste (ZAD) beauftragen. Das ermöglicht eine Bezahlung per Sofort-Überweisung. Die ZAD lösen bei dem kontoführenden Kreditinstitut eine Überweisung aus und schicken dem Verkäufer eine Zahlungsbestätigung. Für Kunden soll das Bezahlen im Internet dadurch genauso schnell und einfach werden, wie bar an der Kasse.

Zudem können Kunden, die Konten bei verschiedenen Banken haben, durch die neuen Regularien Kontoinformationsdienste (KID) nutzen: Diese zeigen alle Umsätze und Kontostände in einer zentralen Übersicht an. Für die Kunden bedeutet Open Banking also mehr Komfort, für Fintechs bedeutet es einen besseren Zugang in den Markt. Damit ZAD und KID ihre Dienstleistungen anbieten können, benötigen sie Zugriff auf die Daten der Kunden. Die PSD2 definiert daher sogenannte Application Programming Interfaces (APIs). Mit diesen Schnittstellen lassen sich die Onlineservices verbinden und Daten übertragen. Die APIs bieten aber auch neue Einfallstore für Hacker.

FLF Technische Regulierungsstandards müssen selbstverständlich berücksichtigt werden. Was ist konkret anders und gegebenenfalls gefährlicher geworden?

Onlinebanking soll nicht nur bequemer, sondern auch sicherer werden. Aus diesem Grund verpflichtet die PSD2 Zahlungsdienstleister dazu, eine sogenannte starke Kundenauthentifizierung – abgekürzt SCA – zu entwickeln. In den technischen Regulierungsstandards (RTS) wird dafür eine Kombination aus mindestens zwei voneinander unabhängigen Elementen vorgegeben: Kombiniert werden kann beispielsweise etwas, das der Kunde weiß, also ein Passwort, mit etwas, das er besitzt – also zum Beispiel einer Tan – oder mit einem biometrischen Merkmal, wie einem Fingerabdruck. Für Banken ist die technische Umsetzung dieser neuen Vorgaben eine enorme Herausforderung. Sie müssen gewährleisten, dass die neuen Authentifizierungsverfahren bei der Anbindung der Drittparteien umgesetzt werden.

Insbesondere benötigen sie aber auch neue Schutzmechanismen, da APIs einer Vielzahl von Angriffsszenarien ausgesetzt sind.

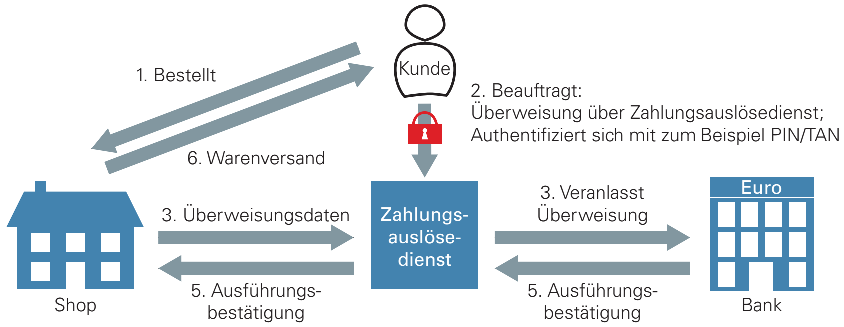
FLF Was sind die wichtigen Aspekte beim Absichern von Open Banking, auf die zu achten ist?

Aus meiner Sicht sind das drei wichtige Dinge: Erstens muss eine Nichterreichbarkeit verhindert werden, zweitens müssen die Daten geschützt und selbstverständlich die Vorgaben der Datenschutzgrundverordnung eingehalten werden. Und drittens muss die IT-Sicherheit gleichzeitig Ressourcen schonen.

FLF Gehen wir auf die Punkte ein. Was würde aus einer „Nichterreichbarkeit“ folgen und wie könnte sie ausgelöst werden?

Sind Onlinefinanzdienste nicht erreichbar, erleidet der Finanzdienstleister einen enormen Imageschaden. Ausgelöst werden kann die Verweigerung des Dienstes durch einen Distributed Denial of Service (DDoS)-Angriff auf die API. Angreifer senden dabei sintflutartige Anfragen an das Netzwerk des jeweiligen Opfers. Die Masse eingehender Nachrichten erzwingt ein Abschalten des Systems und aller über dieses System bereitgestellten Dienste. Häufig werden diese Angriffe mit Lösegeldforderungen verbunden. Die Hacker senden dann zunächst eine Nachricht an das jeweilige Finanzinstitut und drohen mit einer Anfragenattacke, sollte ein bestimmter Geldbetrag nicht gezahlt werden. Eine Drohung, die ernst zu nehmen ist. Schließlich haben DDoS-Attacken in der Vergangenheit bereits schwerwiegende Schäden ausgelöst. Die Bewältigung eines solchen Ransom-DDoS-Angriffs kann eine Bank mehrere Hunderttausende Euro kosten.

Abbildung 1: Zahlungsauslösedienst



Quelle: Deutsche Bundesbank

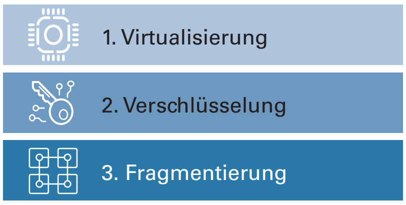
Gegen diese Attacken können herkömmliche Netzwerk-Firewalls wenig ausrichten. Da Firewalls in der Regel die erste Verteidigungslinie gegen Attacken aus dem Internet darstellen, sollten sie zwar beim Sicherheitskonzept auf keinen Fall fehlen. Da APIs jedoch auf Web-Ebene kommunizieren, sind zusätzliche Schutzmechanismen erforderlich.

Kern dieses Schutzes ist eine sogenannte „Web Application Firewall“. Diese kann – im Unterschied zu herkömmlichen Firewalls – Daten überprüfen, die im HTTP- beziehungsweise HTTPS-Protokoll verkehren. Sobald bestimmte Inhalte als verdächtig eingestuft werden, verhindert die Web Application Firewall den Zugriff. Im Falle von DDoS- oder DoS-Attacken greift ein Scoring-Modell: Nimmt man als Schwellenwert zum Beispiel die Anzahl der Anfragen, die eine einzelne IP innerhalb eines festgelegten Zeitraums übermitteln darf, werden Anfragen gestoppt, die über diese Anzahl hinausgehen. Auf diese Weise sind Finanzinstitute geschützt und brauchen Attacken dieser Art nicht zu fürchten.

FLF Der Datenschutz ist bei unseren Finanzdienstleistern schon auf einem hohen Niveau. Daten schützen und die EU-DSGVO einhalten sollte kein neues Thema sein?

Abbildung 2: Sicherheitskonzept

Mehrstufiges Sicherheitskonzept als Schutz vor Cyberangriffen auf die Cloud



Quelle: Rohde & Schwarz Cybersecurity

Daten, die über APIs in Web- und Cloud-Anwendungen bereitgestellt werden, lassen sich nicht mit klassischen Sicherheitssystemen vor Angriffen schützen. Denn die Verarbeitung und Speicherung der Daten verlagert sich aus dem eigenen Netzwerk auf externe Systeme. Die herkömmliche „Perimetersicherheit" reicht nicht mehr aus. Hinzu kommt, dass nicht nur Benutzer und Administratoren Zugriff auf die Daten haben. Auch Cloud-Provider oder Hacker können sich Zugriff verschaffen, wenn Daten ungeschützt und unverschlüsselt abliegen.

Die Lösung für dieses Problem liegt in der „datenzentrischen Sicherheit". Dabei werden ausschließlich die Metadaten eines Dokuments als Platzhalter in die Cloud geladen. Das Originaldokument wird hingegen in einem Streaming-Verfahren verschlüsselt. Die Fragmentierung der Dokumente in mehrere kleine Teile, den sogenannten Chunks, sowie die konfigurierbare verteilte Speicherung bieten weiteren Schutz.

Der Vorteil: Das Originaldokument ist nie vollständig einsehbar und nur in Form von Fragmenten hinterlegt. Selbst bei einem Angriff auf die Cloud oder wenn Hacker in ein System eindringen, bleiben die vertraulichen Inhalte für Angreifer oder nicht befugte Personen unlesbar. Egal, wo ein Angreifer Zugriff erlangt: Er kann keinen großen Schaden mehr anrichten. Zudem bleiben die Daten bei dieser Methode in Deutschland und ihre Speicherung entspricht den strengen Datenschutz- und Sicherheitsvorgaben der EU-DSGVO.

FLF Das alles deutet eigentlich auf zusätzlichen Aufwand. Was meinen Sie damit, dass IT-Sicherheit Ressourcen schonen muss?

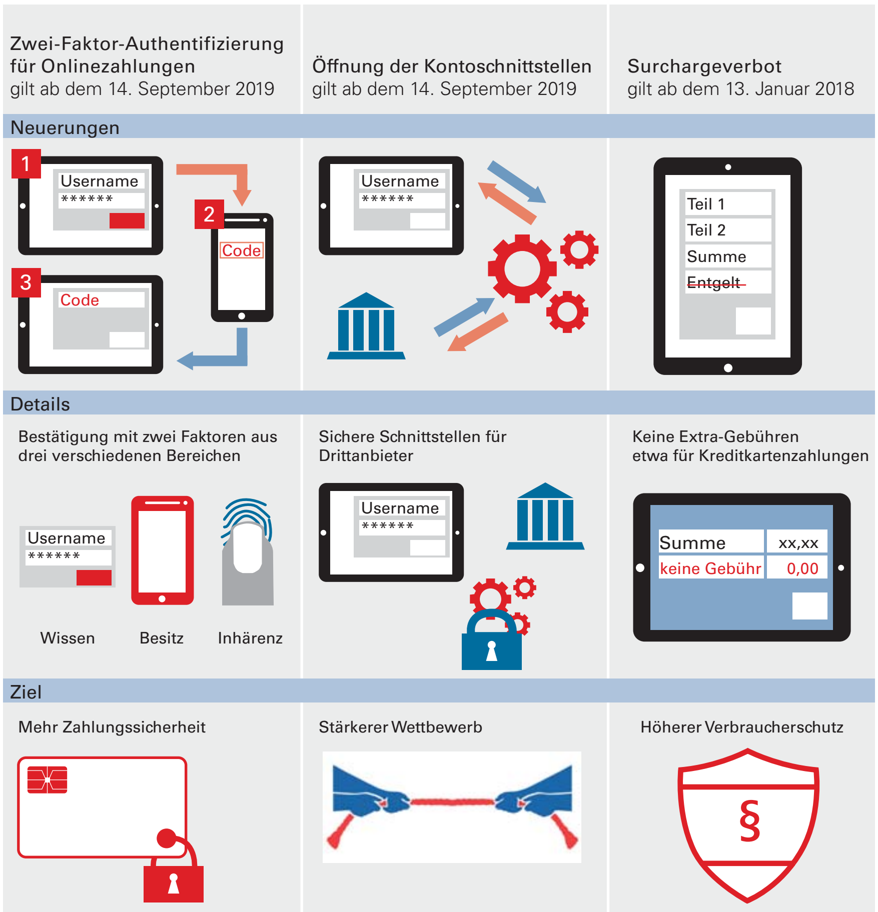
Die vor allem mittelständisch aufgestellten Banken und Sparkassen benötigen IT-Sicherheitsstrategien, die auf die vorhandenen Ressourcen zugeschnitten sind. IT-Sicherheitsanwendungen dürfen daher nicht zu komplex sein, sodass auch ein kleines Team mit wenig Manpower sie bedienen kann.

Zudem sollten die Lösungen nicht zu viel interne Rechenleistung belegen – denn das kann teuer werden. Besonders effizient sind „Software as a Service"-Lösungen. „Web Application Firewall as a Service"-Lösungen ermöglichen Finanzinstituten, ihre Webanwendungen zu schützen, ohne die gesamte erforderliche Back-end-Infrastruktur verwalten und neue Fähigkeiten erlernen zu müssen. Eine solche IT-Security aus der Cloud ist besonders nutzerfreundlich und skalierbar: Je nach Bedarf lassen sich Features an die Bedürfnisse einer Bank anpassen. Entscheidend dabei ist allerdings, dass die Daten innerhalb der EU gespeichert und so die europäischen Datenschutzvorschriften erfüllt werden.

Banken sollten jetzt aktiv werden und sich hinsichtlich der Absicherung der neuen Schnittstellen beraten lassen. Denn nur, wenn Open Banking sicher ist, kann es sich bei den Kunden durchsetzen – und damit zum Erfolg werden, für etablierte Banken und neue Dienstleister gleichermaßen.

FLF Herr Heck, herzlichen Dank für das Gespräch.

Abbildung 3: PSD2-Neuerungen im Überblick



Quelle: Deutsche Bundesbank