Die überarbeitete Richtlinie über Zahlungsdienste

Von Steven D'Alfonso und Assaf Regev

Einführung

In den letzten 30 Jahren gab es große technologische Veränderungen im Finanzdienstleistungssektor, und Aufsichtsbehörden hatten Mühe, damit Schritt zu halten. Anbieter elektronischer Zahlungsservices wie PayPal (später von eBay übernommen) nahmen die Herausforderung in Angriff, globale Onlinezahlungen zu erleichtern. Das Angebot von PayPal war einfach: ein benutzerfreundlicher Service für Onlinezahlungen, der als Alternative zu traditionellen papiergestützten Zahlungsmethoden wie Schecks und Geldanweisungen sowie zu teuren elektronischen Überweisungen fungierte. Dies war ein großer Durchbruch für Onlinenutzer und Händler, bereitete jedoch den Aufsichtsbehörden Kopfzerbrechen.

Ende 2007 verabschiedeten das Europäische Parlament und der Rat der Europäischen Union die Zahlungsdiensterichtlinie (Payment Services Directive, PSD). Die PSD wurde aus verschiedenen Gründen entwickelt[1]:

- Um einen stärker integrierten und effizienteren Markt für Zahlungen zu fördern
- Um die Wettbewerbsbedingungen für die verschiedenen Anbieter von Zahlungsdiensten (einschließlich neuer Anbieter) anzugleichen
- Um Zahlungen sicherer zu machen
- Um die Verbraucher zu schützen
- Um geringere Gebühren für Zahlungen zu fördern

Im Jahr 2011 wurde die Europäische Bankenaufsichtsbehörde EBA gegründet, um konsistente Regelungen im gesamten europäischen Bankensektor sicherzustellen. Das Hauptziel der EBA bestand darin, *„zur Erarbeitung des einheitlichen europäischen Regelwerks für den Finanzsektor beizutragen, das einheitliche und harmonisierte Aufsichtsregeln für Finanzinstitute in der EU bereitstellen soll"*.[2]

Im Dezember 2015 verabschiedete das Europäische Parlament die überarbeitete Zahlungsdiensterichtlinie (PSD2), die die ursprüngliche Richtlinie von 2007 ersetzen und erweitern sollte. Die überarbeitete Richtlinie war aufgrund des schnellen Wachstums und der technologischen Innovationen im Bereich von Online- und mobilen Zahlungen notwendig geworden. Die Ziele der PSD2 sind klar und im Einklang mit den Regelungen, die sie aktualisiert: Statt den Auftrag zur strikten Aufsicht von Transaktionen einzuschränken, soll die PSD2 die Transparenz erhöhen, neue Zahlungsservicemethoden ermöglichen und zur Kostensenkung durch Wettbewerb beitragen, indem der Einstieg in den Markt der Zahlungsdienste erleichtert wird.

PSD2: die nächste große Chance

Die PSD2 eröffnet neue Möglichkeiten für Banken, stellt jedoch auch neue Anforderungen an sie. Proaktive Early-Adopter-Unternehmen werden die neuen Anforderungen schnell erfüllen können. Durch die Bildung von Allianzen und die Bereitstellung innovativer Services werden sie in der Lage sein, sowohl für sich selbst als auch für ihre Kunden Wert zu schaffen.

Wenn es darum geht, neue Sicherheitsanforderungen zu erfüllen, die sich aus der PSD2 ergeben können, sollten Banken und andere Finanzinstitute über eine Aktualisierung ihrer Geschäfts- und Sicherheitsstrategien nachdenken, um Umsätze beizubehalten und Kunden zu binden.

Zu beachten ist, dass Banken und andere Finanzinstitute in Europa nur begrenzt Zeit haben, um sich auf die anstehenden Veränderungen vorzubereiten, da die PSD2 Anfang 2018 von staatlichen Aufsichtsbehörden umgesetzt wird.

Auswirkungen auf PISPs

Zahlungsauslösedienstleister (Payment Initiation Service Providers, PISPs) sind Dritte, die eine Onlinezahlung zwischen Endverbrauchern und Onlinehändlern erleichtern. Ein PISP stellt eine Plattform bereit, die bestätigt, dass die erforderlichen finanziellen Mittel auf dem Bankkonto des Endverbrauchers vorhanden sind (siehe Abbildung 1). Der Endverbraucher muss den PISP gegenüber der Bank oder einem kontoführenden Zahlungsdienstleister (Account Servicing Payment Service Provider, ASPSP) vor der ersten Zahlungsauslösung autorisieren. Der PISP fungiert dann als Mittler, über den Endverbraucher auf ihre Bankkonten zugreifen und Zahlungen anweisen. Alle Kommunikations- und Authentifizierungsanforderungen entfallen jetzt auf die PISPs, wenn sie einen ASPSP kontaktieren.

Voraussichtlicher Zeitrahmen für die Umsetzung der überarbeiteten Payment Services Directive (PSD2)

Abbildung 1. Reihenfolge der wichtigsten Ereignisse bei der Umsetzung der überarbeiteten Zahlungsdiensterichtlinie (Payment Services Directive, PSD2) der Europäischen Union.

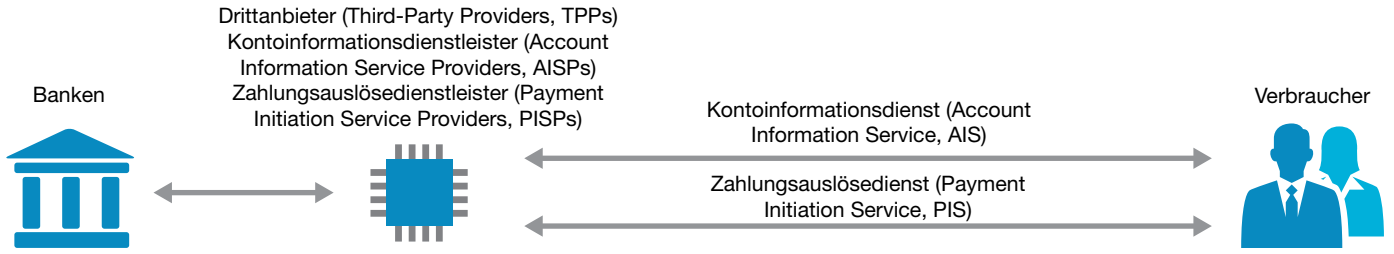

Abbildung 2. PSD2 ermöglicht Drittanbietern (TPPs) den Zugang zu den Zahlungsverarbeitungssystemen und Kontoinformationen von Banken.

Laut einem vor Kurzem von Accenture Consulting veröffentlichten Update[3] werden sich die neuen Anforderungen sehr wahrscheinlich auf fast jeden Aspekt des Unternehmens eines Zahlungsdienstleisters (Payment Service Provider, PSP) auswirken: Produkte, Services, Betriebsabläufe, Kooperationen und Bereiche mit Kundenkontakt. PSPs müssen möglicherweise ihr Geschäftsmodell und ihre Geschäftsstrategie insgesamt neu ausrichten – darunter Fach-, Risiko-, Compliance- und IT-Abteilungen –, um sich schnell und effektiv an die erforderlichen Änderungen anzupassen. Im Folgenden sind einige der möglichen Herausforderungen für bestehende Marktteilnehmer zusammengefasst:

- Potenziell höheres **Sicherheitsrisiko** durch Einschaltung eines Dritten zwischen Finanzinstitut und Verbraucher
- **Datenschutzbedenken** aufgrund der Tatsache, dass der Schutz personenbezogener Daten hohe Priorität für europäische Aufsichtsbehörden hat und besonderer Aufmerksamkeit bedarf; hier ein aktuelles Beispiel der Intervention europäischer Aufsichtsbehörden im Bereich Social Media
- **Haftungsansprüche** im Fall von nicht autorisierten Transaktionen und Datendiebstählen

Auswirkungen auf die Endverbraucher

Die größten Nutznießer der geänderten Regelungen sind die Endkunden einer Bank (d. h. die Verbraucher), vor allem, da sie alle ihre bestehenden Zahlungskonten konsolidieren können. Dadurch haben sie die Möglichkeit, die bequemste Web- oder anwendungsbasierte Schnittstelle zur Prüfung ihrer Onlinedaten auszuwählen. Darüber hinaus profitieren die Verbraucher von einer direkten Verknüpfung ihrer Bankkonten mit den Websites von Onlinehändlern (z. B. Amazon) und damit von einem komfortablen, nahtlosen Kundenerlebnis beim Onlineeinkauf.

Die geänderten Regelungen können auch zu einer Stärkung von Sicherheitsmaßnahmen, d. h. „starker Kunden-authentifizierung“ führen, um das Nutzererlebnis ohne sicherheitsbedingte Komplikationen zu verbessern. Ein verbesserter Prozess für die Kundenauthentifizierung erfordert die Nutzung von zwei oder mehr Elementen, die sich in folgende Kategorien unterteilen lassen:

- **Wissen:** etwas, das nur der Nutzer *weiß*, z. B. ein Kennwort oder persönliche Informationen
- **Besitz:** etwas, das nur der Nutzer *besitzt*, z. B. ein Token oder Artefakt (Smartphone), das der Nutzer nachweislich zum Zeitpunkt der Anmeldung (gewöhnlich über ein Einmalkennwort) in seinem Besitz hatte
- **Inhärenz:** etwas, das der Nutzer *ist*. Hierbei kann es sich um unverwechselbare physische Merkmale wie den Fingerabdruck oder die Iris des Nutzers oder Verhaltensbiometrie wie Browsing-Muster oder andere Eigenschaften handeln

Diese Elemente müssen unabhängig voneinander sein, damit eine mögliche Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht beeinträchtigt. Sie müssen außerdem dafür ausgelegt sein, die Vertraulichkeit der Authentifizierungsdaten zu schützen.

Weniger positiv ist: Im Fall eines Betrugs oder finanziellen Verlusts herrscht bei Verbrauchern, die Entschädigung verlangen, Unsicherheit hinsichtlich der Beziehungen zwischen PSIPs, Händlern und Banken oder anderen ASPSPs und hinsichtlich deren Verantwortlichkeiten.

Herausforderungen für Finanzorganisationen

Für kommerzielle Organisationen, insbesondere Banken und andere Finanzinstitute, zeichnet sich eine Reihe von Herausforderungen ab.

Im Rahmen der PSD2 sollten Banken und andere Finanzinstitute ihre bestehenden Geschäftsmodelle anpassen und neue Beziehungen eingehen, um neue, innovative Services zu entwickeln, die anfängliche und fortlaufende Investitionen ausgleichen. Hinzu kommt: Auch wenn die Richtlinie die Bereitstellung von Anwendungsprogrammierschnittstellen (APIs) nicht vorschreibt, um diese neuen Modelle zu ermöglichen, ist die API-basierte Kommunikation möglicherweise der logische Weg, den Banken einschlagen werden. Banken und andere Finanzinstitute sollten die Entwicklung neuer technischer Standards in Erwägung ziehen, um Interoperabilität zu ermöglichen.

PSD2 und Betrüger

Cyberkriminelle sind Meister darin, Technologien und Prozesse auszunutzen, von denen Finanzinstitute und Nutzer profitieren sollen. Die Einführung neuer Zahlungsmodelle unter der PSD2 kann Akteuren mit bösen Absichten Möglichkeiten eröffnen, sich in Zahlungssysteme einzuschleusen. Externe Sicherheitsbedrohungen können APIs von Banken, PISPs und ASPSPs direkt attackieren. Betrüger sind Experten darin, solche Schwachstellen ausfindig zu machen.

Während PSPs relativ neu im Finanzdienstleistungssektor sind, bekämpfen Banken Betrug schon lange und haben enorme Summen in die Prävention und Erkennung von Betrug investiert.

Doch trotz all ihrer Anstrengungen hat die Häufigkeit von Betrug gegen Banken und ihre Kunden nicht nachgelassen. Zwar hat Technologie dazu beigetragen, bestimmte Probleme zu verringern, aber insgesamt verlagern sich Betrugsversuche einfach in andere, weniger gut geschützte Bereiche.

Die Betrugsbekämpfung ähnelt dem Arcade-Spiel Whack-a-Mole, bei dem man Maulwürfe, die aus ihren Löchern hervorkommen, treffen muss, damit sie wieder in die Löcher verschwinden – wenn man einen Maulwurf trifft, taucht sofort ein anderer auf. Angesichts neuer Marktteilnehmer, die unter der PSD2 auf den Markt kommen, können für jeden außer Gefecht gesetzten Betrüger mehrere neue auftauchen. Neue oder auch bestehende Drittanbieter verfügen möglicherweise nicht über die ausgefeilte Sicherheitsinfrastruktur, die Banken haben. Branchenexperten gehen davon aus, dass die Mehrfaktorauthentifizierung, wie wir sie kennen, bis zur Durchsetzung der PSD2 2018 bis 2019 eine große Veränderung durchlaufen wird.[4]

Seit die Anbieter elektronischer Zahlungsservices vor mehr als 15 Jahren auf dem Markt auftauchten, haben Betrüger in der Regel die schwächsten Glieder der Kette ins Visier genommen – normalerweise Menschen statt Systeme und insbesondere Verbraucher. Das Risiko eines Datendiebstahls besteht auch weiterhin. Am einfachsten für Betrüger, die sich in den Zahlungsprozess einschleusen wollen, ist es jedoch, sich Zugang zu den Geräten der Endverbraucher zu verschaffen oder die Endverbraucher selbst zu täuschen.

Eine weit verbreitete Angriffsmethode kombiniert Social Engineering und Malware auf dem Gerät eines Verbrauchers. In diesem Szenario entwickeln Cyberkriminelle akribisch Malware, um einen Web-Injection-Angriff auf einen Onlinehändler auszuüben und den Zahlungsprozess zu kompromittieren. Der Injection-Angriff erfolgt im Normalfall während des Bezahlvorgangs an der Kasse. Dabei wird eine gefälschte Seite angezeigt, die den Nutzer zur Eingabe zusätzlicher Sicherheitsinformationen auffordert, um Sicherheitseinstellungen „zu bestätigen“ oder eine zusätzliche Aufgabe auszuführen. Geht der Kunde darauf ein, erhält der Betrüger wichtige Sicherheitsdaten im Zusammenhang mit dem PISP.

Wie viele Nutzer werden Opfer dieses Angriffstyps und geben sensible Informationen an die Betrüger weiter? Die Antwort ist: sehr viele. Die gefälschte Seite wird am Ende der Onlinesitzung eines Kunden angezeigt, wenn dieser sich in Sicherheit wiegt, da das Einkaufserlebnis bislang ganz normal war.

Wir können nur spekulieren, wie Cyberkriminelle und Betrüger den Prozess als Nächstes ausnutzen werden, aber es gibt wahrscheinlich mindestens einen Weg, den niemand in Betracht gezogen hat. Das Gesetz der unbeabsichtigten Folgen ist bei neuen Technologien oder Finanzdienstleistungsangeboten fast immer präsent.

Im Folgenden finden Sie eine kurze Liste der Taktiken, die Cyberkriminelle und Betrüger anwenden, um den Zahlungsprozess auszunutzen. Die Liste erhebt keinen Anspruch auf Vollständigkeit, sondern hebt nur einige der häufigsten Methoden hervor:

- **Datendiebstahl:** Das Risiko einer direkten Cyberattacke auf eine Bank oder einen Drittanbieter ist immer vorhanden. Banken haben kontinuierlich Maßnahmen zur Reaktion auf solche direkten Angriffe entwickelt. PISPs und ASPSPs dagegen verfügen möglicherweise nicht über eine so ausgereifte Infrastruktur und stellen damit ein höheres Risiko dar. Einige bekannte Datendiebstähle bei Finanzunternehmen waren das Ergebnis erfolgreicher Spear-Phishing-Attacken. Banken haben ihre Mitarbeiter geschult, wachsam gegenüber Phishing-Mails und ähnlichen Social-Engineering-Taktiken zu sein. Cyberkriminelle könnten ihre Aufmerksamkeit daher auf neuere Anbieter konzentrieren.
- **API-Sicherheitsverletzung:** API-Banking und -Zahlungen sind ein neuer Bereich, den Betrüger erkunden könnten. API-Zugriff ohne ausreichende Authentifizierung oder ausreichenden Schutz kann Betrügern direkten Zugang zu verschiedenen Systemen des Service-Providers verschaffen. So können große Mengen von Zahlungsanweisungen eingeschleust werden.
- **Kompromittierung von Nutzern:** Ob Kontoinformationsdienstleister (Account Information Service Providers, AISPs) neue Banking-Services und Kundenerlebnisse bereitstellen oder PISPs vereinfachte Zahlungsmöglichkeiten in ihren E-Commerce- oder Mobile-Commerce-Anwendungen anbieten, der Benutzerzugriff auf die Services kann mit verschiedenen Methoden kompromittiert werden. Deren Ziel ist es, die Zugangsdaten des Nutzers zu erhalten. Dazu zählen folgende Methoden:
  - *Phishing:* Phishing-Attacken wollen Verbraucher dazu verleiten, sensible Zugangsdaten für den Kontozugriff preiszugeben. Auch wenn die Nutzung der Mehrfaktorauthentifizierung zunimmt, waren versierte Angreifer bereits erfolgreich darin, die Mehrfaktorauthentifizierung und die Verwendung von Einmalkennwörtern mit den per Phishing erhaltenen Informationen zu umgehen.
  - *Malware:* Malware kann dafür entwickelt werden, PISPs und ASPSPs – genau wie bislang Banken – ins Visier zu nehmen und zu infiltrieren, um Kundendaten von ihren Systemen zu stehlen. Ein wahrscheinlicheres Szenario ist jedoch Malware, die Endverbraucher attackiert. In diesem Fall wird der Malware-Code für mehrere Organisationen geschrieben und auf die Mobilgeräte von Verbrauchern verteilt. Die Malware bleibt dann so lange inaktiv, bis ein Nutzer auf eine Website oder Anwendung zugreift, die Ziel des Angriffs ist. Diese Angriffsmethode umfasst den Diebstahl von Zugangsdaten durch Man-in-the-Browser- und Overlay-Attacken, durch den Diebstahl von Tokens für die Mehrfaktorauthentifizierung und sogar durch Angriffe mittels der kompletten Übernahme per Remote-Zugriff, die Transaktionen vom Gerät des Nutzers selbst in betrügerischen „Shops“ durchführen.
  - *Social Engineering:* Social Engineering ist häufig keine Betrugstaktik an sich. Vielmehr kombiniert ausgefeiltes Social Engineering heute zwei oder mehr Elemente, die Technologie, Kommunikationskanäle und reine Täuschung beinhalten. Phishing-Kampagnen können einfache E-Mails mit schädlichem Anhang oder komplexere Modelle nutzen. Letztere verleiten Kunden dazu, den „Kundenservice“ anzurufen, um eine dringende Angelegenheit zu klären. An diesem Punkt versucht der Betrüger, den Anrufer zur Preisgabe sensibler Informationen oder zur Ausführung einer zusätzlichen Maßnahme zu überreden. Jeder Schritt im Prozess soll dem Verbraucher ein stärkeres Gefühl der Sicherheit vorgaukeln, damit er letztendlich die Informationen preisgibt, die der Betrüger benötigt, um einen Angriff auf das Konto des Verbrauchers zu starten.

IBM Trusteer-Lösungen für den Schutz vor Betrug

IBM Trusteer-Lösungen helfen Unternehmen mit Funktionen, zu denen die Überprüfung von Kundenberechtigungen und Online-Identitäten gehört, ihre Sicherheitsanforderungen zu erfüllen.

IBM Trusteer Pinpoint Detect stellt Empfehlungen nahezu in Echtzeit zu Anmeldeversuchen, überschrittenen Sitzungszeitlimits und der Gültigkeit der Authentifizierung bereit. Mit diesen Funktionen können Unternehmen Onlinenutzer auf verschiedenen Geräten überprüfen – präzise und ohne den Nutzer zu frustrieren. Diese passive und nahtlose Analyse macht es zudem sehr viel schwieriger für Betrüger, den Sicherheitsprozess zu umgehen, da es schwieriger für sie ist, etwas zu bekämpfen, das sie gar nicht sehen.

Durch die Aggregation und Korrelation von evidenzbasierten Informationen zu Sicherheitsbedrohungen, risikobasierten Indikatoren, Verhaltensanalysen und detaillierten Informationen über Betrug liefert Trusteer umsetzbare Empfehlungen zur Betrugs- und Identitätserkennung. Damit können Unternehmen die richtige Balance von Sicherheit und Nutzerkomfort schaffen und sich auf ihr Kerngeschäft konzentrieren.

- **IBM Trusteer Pinpoint Detect** erstellt zwei unabhängige Ebenen zur Beurteilung der Identitätsprüfung innerhalb einer einzelnen Lösung. Trusteer Pinpoint kann einen PSP warnen, wenn ein unterstütztes Gerät, das einem kompromittierten Nutzer gehört – oder sich in den Händen eines Betrügers befindet –, versucht, auf eine geschützte Anwendung (darunter Website-basierte und mobile Anwendungen) zuzugreifen. Um einen betrügerischen Kontozugriff zu erkennen, erfasst die Lösung Informationen zur Erstellung eines Gerätefingerabdrucks und kennzeichnet die Geräte von Betrügern. Unabhängig davon beobachtet die Lösung auch das Nutzerverhalten, erkennt Fälle von Device-Spoofing oder das Verstecken hinter Proxys und identifiziert Tools für den Remote-Zugriff. Sie bietet die Möglichkeit, die Sitzung und das Verhalten des Nutzers mit früheren Interaktionen zu vergleichen, und erstellt ein persistentes Verhaltensprofil, das verwendet werden kann, um den Benutzerzugriff auf die Services zu vereinfachen.
- **IBM Trusteer Mobile SDK** stellt eine eindeutige Geräte-ID bereit, mit der Systemanbieter besser zwischen verschiedenen Geräten, die demselben Nutzer gehören, unterscheiden können. Dies schließt neu erkannte Geräte und Geräte im Zusammenhang mit verschiedenen Konten ein. Darüber hinaus kann Trusteer Mobile SDK eine Vielzahl von Risiken für Geräte mithilfe von Trusteer Pinpoint Detect und Langzeitdaten zum Benutzerzugriff auf allen Geräten erkennen.
- **IBM Trusteer Rapport** schützt das Gerät eines Endanwenders vor komplexen Malware- und Phishing-Attacken, die versuchen, Nutzerdaten zu stehlen. Solange Trusteer Rapport auf dem Gerät eines Endanwenders installiert ist, erstellt es eine starke, persistente Geräte-ID, die Kompromittierungs- oder Replay-Versuchen standhält. Diese starke Geräte-ID wird auch von Trusteer Pinpoint Detect verwendet, um die Verbindung des Geräts zum Nutzer weiter zu stärken.

Sicherheit versus Komfort – warum nicht beides?

IBM Security-Lösungen, insbesondere Trusteer Pinpoint Detect, helfen Banken und anderen Finanzinstituten, den Zugang neuer Marktteilnehmer zu ihren Systemen zu kontrollieren. Sie nutzen starke Sicherheitsmaßnahmen, um die Infrastruktur sowohl des Zahlungsempfängers als auch des Zahlungsdienstes zu schützen.

Fazit

Häufig studieren Hacker das Nutzer- und Kontoverhalten genau, bevor sie ihre Angriffe starten. Sie sind versiert darin geworden, Sicherheitsmaßnahmen wie risikobasierte Kontrollen und strikte Authentifizierungsmethoden zu umgehen. Daher können statische Sicherheitskontrollen Online-Finanzbetrug nicht effektiv verhindern.

Trusteer-Entwickler setzen auf die folgenden grundlegenden Methoden, um Kunden zu schützen:

- **Risikobewertung auf der Basis von Echtzeitdaten zu Sicherheitsbedrohungen.** Die Früherkennung von Änderungen in der Bedrohungslandschaft ist entscheidend für eine effektive Risikobewertung und die Bereitstellung von Sicherheitsmaßnahmen, die Kunden vor Onlinebetrug schützen. Das Forschungs- und Entwicklungsteam der IBM X-Force passt seinen Threat-Intelligence-Index kontinuierlich an und aktualisiert Sicherheitswarnstufen, um Risiken in Echtzeit zu mindern.
- **Mehrstufige Sicherheit für Online-Banking und -Zahlungen.** Die Nutzung mehrerer Ebenen der Sicherheit für Endgeräte und Webanwendungen ermöglicht einen leistungsfähigen und flexiblen Schutz. Die Endgerätesicherheit bildet eine Ebene der Abwehr, Informationserfassung und Abhilfemaßnahmen. Die clientlose Malware-Erkennung ist die nächste Ebene. Sie deckt Endbenutzersysteme mit geringen Auswirkungen auf die Implementierung ab. Die Verbindung von Trusteer Rapport oder Trusteer Mobile SDK (für die Endgerätesicherheit) mit Trusteer Pinpoint (für die clientlose Erkennung) bietet Unternehmen die Möglichkeit, die Infrastruktur von Zahlungsempfänger und Zahlungsdienst zu schützen. Beide Lösungen können starke Funktionen für einen Gerätefingerabdruck nutzen, um zu verifizieren, dass sich ein bestimmtes Gerät im Besitz des Endanwenders befindet.

- **Schutz von Kundengeräten.** In den letzten Jahren haben Cyberkriminelle Malware eingesetzt, die in der Lage ist, viele Sicherheitskontrollen zu umgehen. Indem verhindert wird, dass solche Malware das Endgerät infiziert und den Browser oder die Webanwendung attackiert, kann Betrug verhindert werden. Trusteer Rapport bietet mehrstufigen Schutz. Die Lösung schützt das Gerät des Endanwenders vor Malware-Infektionen und Phishing-Attacken und schützt gleichzeitig Web-Browser-Sitzungen, um eine Manipulation von Kundentransaktionen zu verhindern.
- **Erkennung von Anomalien.** Die Früherkennung und Abwehr von Malware-Angriffen trägt dazu bei, die Anzahl an verdächtigen Transaktionen, die von den für Betrugsbekämpfung und Support verantwortlichen Teams untersucht werden müssen, und den damit verbundenen Betriebskosten- und Personalaufwand zu reduzieren. Trusteer nutzt Funktionen für maschinelles Lernen und erstellt transparent umfangreiche, personalisierte Verhaltensbeschreibungen auf der Basis früherer Sitzungen. Dadurch ist ein Vergleich des aktuellen Verhaltens mit früheren Interaktionen möglich. So können Anomalien festgestellt werden, die auf eine Malware-Infektion hindeuten könnten.
- **Minimierung der Auswirkungen auf die Endanwender.** Die richtige Balance von Sicherheit, Benutzerfreundlichkeit und Interoperabilität sorgt für größere Akzeptanz bei Endanwendern und minimiert die Auswirkungen auf tägliche Abläufe, ohne dass Abstriche bei der Sicherheit gemacht werden müssen.
- **Zusammenarbeit mit einem bewährten Anbieter von Lösungen für die Betrugsbekämpfung im Onlinebanking.** Letztendlich ist die Betrugsbekämpfung Teamwork. Finanzdienstleister sollten bei der Wahl eines geeigneten Anbieters darauf achten, ob dieser ihre eigenen Mitarbeiter um das Know-how und die Fähigkeiten ergänzen kann, die für einen effektiven Schutz vor Cyberkriminellen erforderlich sind.

Weitere Informationen

Wenn Sie mehr über IBM Trusteer-Lösungen erfahren möchten, wenden Sie sich bitte an Ihren IBM Ansprechpartner oder IBM Business Partner oder besuchen Sie die folgende Website: **ibm.com**/software/products/de/category/advanced-fraud-protection

Glossar

AISP (Account Information Service Provider), dt. Kontoinformationsdienstleister: Eine von zwei neuen Kategorien von dritten Zahlungsdienstleistern (Third-Party Payment Providers, TPPs), die in der PSD2 eingeführt wurden. Ein AISP fasst Daten zu den Konten eines Nutzers zusammen, die dieser bei einem oder mehreren unterschiedlichen ASPSPs unterhält. AISPs müssen sich unter der PSD2 als Zahlungsinstitut registrieren.

ASPSP (Account Servicing Payment Service Provider), dt. kontoführender Zahlungsdienstleister: Eine traditionelle Form eines Zahlungsinstituts, bei dem ein Nutzer eines oder mehrere Konten unterhält.

PISP (Payment Initiation Service Provider), dt. Zahlungsauslösedienstleister: Die zweite neue Kategorie von TPPs, die mit der PSD2 eingeführt wird. PISPs erhalten die Genehmigung eines Nutzers, Zahlungen in dessen Auftrag auszulösen. Sie stellen eine „Softwarebrücke“ zwischen der Website eines Händlers und der Onlinebanking-Plattform der Bank eines Zahlungspflichtigen her, um die Zahlung auszulösen. Der PISP wird in der Regel als Zahlungsoption auf der Website eines Händlers angeboten.

PSP (Payment Service Provider), dt. Zahlungsdienstleister: Ein allgemeiner Begriff für Anbieter, die Online-Services für die Annahme elektronischer Zahlungen mittels verschiedener Methoden, darunter Kredit-/Debitkarten und Echtzeitüberweisung, anbieten. Zu traditionellen PSPs wie Banken und Finanzinstituten kommt jetzt eine immer größere Zahl und Vielfalt von TPPs hinzu.

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

Bitte der Wiederverwertung zuführen

WGW03255-DEDE-01

[1] „GREEN PAPER Towards an integrated European market for card, internet and mobile payments“, *EUR-Lex*, Dokument 52011DC0941, 11. Januar 2012. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1476195234402&uri=CELEX:52011DC0941

[2] „About Us“, *The European Banking Authority*. http://www.eba.europa.eu/about-us

[3] „Welcoming a new phase of Everyday Payments in Europe: Payment Services Directive (PSD2) enables Everyday Payments in Europe to move to the next level“, Accenture, Zugriff am 10. Oktober 2016. https://www.accenture.com/il-en/insight-everyday-payments-europe

[4] Douglas Bonderut, „SMS Two-Factor Authentication: Time to Trash the Text?“ *IBM Security Intelligence*, 28. Juli 2016. https://securityintelligence.com/news/sms-two-factor-authentication-time-to-trash-the-text/