RSA® Adaptive Authentication for eCommerce

Risikobasiertes 3-D Secure für Kreditkartenaussteller

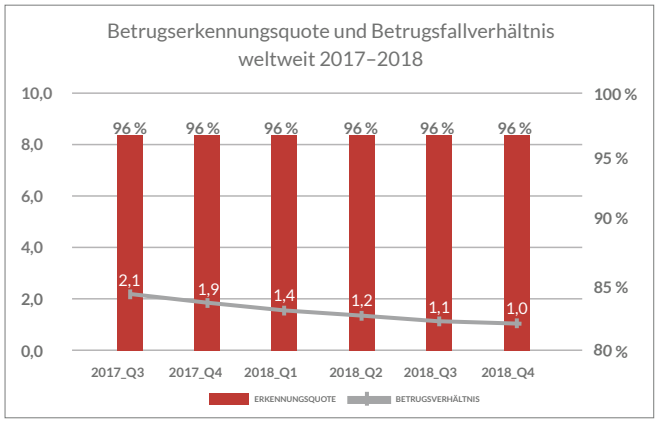
Bei 3-D Secure handelt es sich um ein Protokoll zur Betrugsbekämpfung, das von MasterCard, American Express, Visa und JCB International eingeführt wurde und eine weitere Schutzebene für Onlinezahlungen bietet. Jedes Mal, wenn ein registrierter Karteninhaber bei einem teilnehmenden Händler eine angemeldete Kreditkarte verwendet, wird der Karteninhaber im 3-D Secure-Protokoll authentifiziert, bevor die Transaktion fortgesetzt werden kann. Die Authentifizierung in einer herkömmlichen 3-D Secure-Umgebung basiert auf einem Kennwort, das die Karteninhaber bei der Anmeldung ihrer Kreditkarte erstellen. Bei jeder Transaktion erfolgt dann eine entsprechende Aufforderung zur Authentifizierung.

Die Aufforderungsquote beim herkömmlichen 3-D Secure von 100 % wirkt sich negativ auf Aussteller, Händler und Karteninhaber aus. Jede Aktivität, die den Einkaufsfluss unterbricht, erhöht die Wahrscheinlichkeit, dass der Einkauf abgebrochen wird. Und dies führt zu Umsatzeinbußen beim Aussteller wie auch beim Händler. Die negative Erfahrung, die entsteht, wenn Karteninhaber ihr Kennwort vergessen, erhöht ebenfalls die Wahrscheinlichkeit eines Abbruchs. Außerdem wird die betreffende Karte dann weniger genutzt, was den Umsatz des Ausstellers weiter schmälert.

Das risikobasierte 3-D Secure bietet eine hohe Betrugserkennungsquote durch eine starke Authentifizierung. Darüber hinaus machen Karteninhaber weniger schlechte Erfahrungen, die sich negativ auf die Umsätze des Ausstellers auswirken könnten. Mit dem risikobasierten 3-D Secure können Kreditkartenaussteller Betrugsfälle reduzieren und zugleich ihre Einnahmen sichern.

Hohe Betrugserkennung, wenig Eingriffe

Adaptive Authentication for eCommerce ist der 3-D Secure Access Control Server von RSA für Kreditkartenaussteller und -verarbeiter. Die RSA Risk Engine ist das Herzstück der Lösung und ermöglicht es Adaptive Authentication for eCommerce, Karteninhaber automatisch im Hintergrund zu authentifizieren und nur Kunden mit hohem Risiko zur Authentifizierung aufzufordern (im globalen Durchschnitt etwa 5 % aller Transaktionen). Die hohe Genauigkeit der Risk Engine fördert eine sehr hohe Betrugserkennungsquote und bedeutet zugleich eine sehr niedrige Anzahl falsch positiver Ergebnisse.



Die obige Grafik zeigt für RSA Adaptive Authentication for eCommerce eine durchschnittliche Betrugserkennungsquote von 96 % sowie ein niedriges Verhältnis zwischen legitimen und betrügerischen Transaktionen (Anzahl der legitimen Transaktionen mit Authentifizierungsaufforderung je bestätigter betrügerischer Transaktion). Mit RSA Adaptive Authentication for eCommerce lassen sich Verluste durch betrügerische Transaktionen erheblich reduzieren. Zudem werden sehr wenige legitime Kunden zur Authentifizierung aufgefordert. Dies verbessert nicht nur die Erfahrung des Karteninhabers und schützt den Umsatz von Kreditkartenausstellern, sondern senkt auch die Betriebskosten für die Überprüfung von Transaktionen und die Bearbeitung von Anfragen legitimer Kunden.

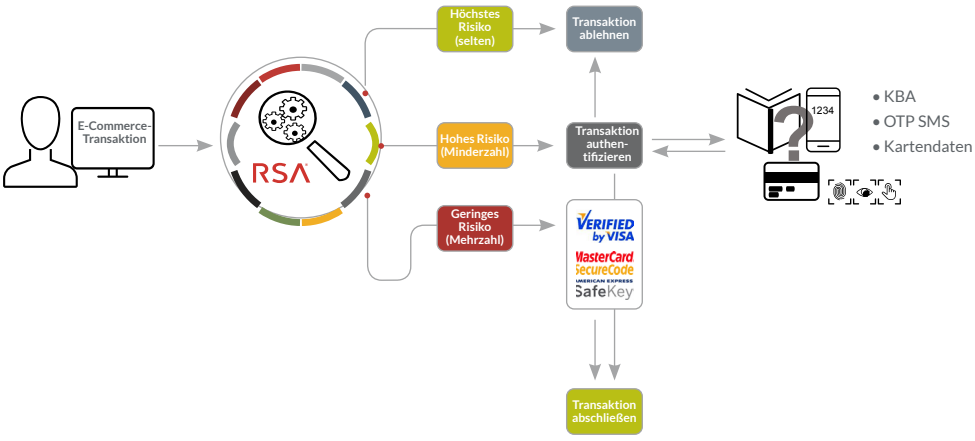
Transparente Authentifizierung für ein nahtloses Erlebnis der Karteninhaber

Mit RSA Adaptive Authentication for eCommerce, aufsetzend auf dem 3-D Secure-Protokoll und der zugehörigen Infrastruktur, können Händler und Aussteller Karteninhabern ein einheitliches, sicheres Shopping-Erlebnis im Internet bieten und zugleich das Risiko von Verlusten durch Rückbelastungen minimieren.

RSA Adaptive Authentication for eCommerce ermöglicht es Kreditinstituten, Verified by Visa® (VbV), Mastercard SecureCode® und Identity Check® sowie American Express SafeKey® bereitzustellen, ohne dass sich dies negativ auf das Einkaufserlebnis ihrer Karteninhaber auswirkt. Mithilfe der RSA Risk Engine bewertet Adaptive Authentication for eCommerce jede Transaktion auf transparente Weise und in Echtzeit. Dabei wird die Wahrscheinlichkeit ermittelt, dass mit der Transaktion eine betrügerische Handlung verfolgt wird. Es werden nur Karteninhaber zur Authentifizierung aufgefordert, die Transaktionen mit hohem Risiko durchführen. Dies bedeutet, dass etwa 95 % der Transaktionen der teilnehmenden Händler vom sicheren 3-D Secure-Verifizierungsprozess gar nicht beeinträchtigt werden. Aufgrund der transparenten Authentifizierungsebene müssen Karteninhaber keinen VBV-, SecureCode-, Identity Check- oder SafeKey-Anmeldeprozess mehr durchlaufen (alle BIN-Bereiche werden vom Aussteller im Voraus registriert) oder sich ein Kennwort merken (es stehen verschiedene zusätzliche Authentifizierungsmethoden zur Verfügung, z. B. Einmalkennwort und Biometrieverfahren). So können legitime Karteninhaber ihren Online-Einkauf ohne Unterbrechungen fortsetzen.

Für uns bemisst sich der Erfolg wie folgt: Wir können viel mehr Verkaufstransaktionen verarbeiten, wir haben unsere Verluste durch Betrugsfälle im Griff und unsere Kunden sind mit der Lösung zufrieden.

Verantwortlicher für die Überwachung des Betrugsrisikos einer großen Bank



Die Analyseanwendung

Die Analyseanwendung von RSA Adaptive Authentication for eCommerce bietet Kartenausstellern lückenlose Einblicke in ihre 3-D Secure-Transaktionsdaten. Die Analyseanwendung stellt den Ausstellern tägliche und monatliche Überwachungskennzahlen, Betrugserkennungsquoten und Regelleistungsdaten bereit, sodass sie die Lösungen an ihre Risikotoleranzwerte und Geschäftsprioritäten anpassen können.

Das Dashboard mit den entsprechenden Berichten bietet folgende Optionen:

- Visualisierung und Hervorhebung von Trends und Ausreißern
- Anzeige von Daten auf verschiedenen Granularitätsebenen
- Flexible und dynamische Oberfläche für schnelle Änderungen

Aussteller können Informationen aus dem Dashboard auch in verschiedene Formate exportieren, um sie über externe Anwendungen zu nutzen.

Die Analyseanwendung bietet Ausstellern mehr Einblicke in ihre Bedrohungslandschaft, sodass sie fundiertere Entscheidungen zu Regeln der Richtlinienverwaltung, Schwellenwerten für die Risikobewertung und anderen konfigurierbaren Variablen treffen können.

3-D Secure 2.0 – die nächste Generation

Das 3-D Secure-Protokoll wird ständig weiterentwickelt. Von EMVCo, das mit der Entwicklung des neuen Protokolls beauftragte Normungsgremium, wurde im Oktober 2016 die nächste Generation von 3-D Secure (EMV 3-D Secure, 3-D Secure 2.0 oder einfach „3DS 2.0“) veröffentlicht. Mit dem 3DS 2.0-Protokoll soll durch den Einsatz risikobasierter Authentifizierungstechnologien ein nahtloses Kauferlebnis der Karteninhaber gefördert werden, ein Ansatz, bei dem RSA bereits im Jahre 2008 Vorreiter war. Als EMVCo Technical Associate lieferte RSA einen wichtigen Beitrag zu 3DS 2.0, was sich auch in den Spezifikationen widerspiegelte.

RSA freut sich darauf, auf unserer Plattform neue Funktionen zu unterstützen, und wird auch weiterhin direkt mit Kunden und EMVCo an Initiativen arbeiten, die Kartenausstellern eine transparente, kennwortlose Authentifizierung ermöglichen.

Informationen über RSA

Mit den Lösungen von RSA® Business-Driven Security™ können Unternehmen einen einheitlichen Ansatz für das Management digitaler Risiken nutzen, der auf integrierter Sichtbarkeit, automatisierten Einblicken und koordinierten Aktionen basiert. Dank der Lösungen für schnelle Erkennung und Reaktion, Nutzerzugriffskontrolle, Verbraucherschutz und integriertes Risikomanagement können RSA-Kunden erfolgreich sein und sich kontinuierlich an Transformationsänderungen anpassen. Weitere Informationen finden Sie unter rsa.com/de-de.