Risikomanagement für digitale Channels für Privatanwender

RSA Fraud & Risk Intelligence Suite

Übersicht

Die Welt der Privatanwender befindet sich an einem historischen Wendepunkt, da sie auf vielfältigere Weise interagieren und handeln als je zuvor. Die Unternehmen befinden sich gerade in einer digitalen Transformation und stellen Privatanwendern dabei immer mehr digitale Channels zur Verfügung, um deren Bedürfnis nach mehr Komfort zu erfüllen. Dies konfrontiert sie allerdings auch mit ganz neuen Geschäfts- und Sicherheitsrisiken, z. B. durch strenge gesetzliche Auflagen oder neue Mitstreiter am Markt bis hin zur einer steigenden Anzahl potenzieller Sicherheitslücken, die von Betrügern und Cyberkriminellen ausgenutzt werden könnten.

Diese Veränderungen aufseiten der Privatanwender haben Auswirkungen auf ganz unterschiedliche Arten von Unternehmen, vom Gesundheitswesen über Versicherungen bis hin zu Einzelhändlern und insbesondere Finanzinstituten, die vor gewaltigen Umbrüchen stehen wie z. B.:

- **Steigende Erwartungen der Kunden an Komfort und Tempo** – Kunden haben die Erwartungshaltung, dass sie jederzeit von jedem Gerät aus auf Informationen zugreifen und digitale Transaktionen schnell, reibungslos, individuell, kanalunabhängig und sicher durchführen können.
- **Innovationen im FinTech-Bereich** bringen neue Wettbewerber auf den Plan, die digitale Services anbieten, was die Unternehmen zwingt, ihre Strategie zu überdenken und neue Partnerschaften gestützt auf die API-Economy einzugehen. Dies schafft aber auch Risiken durch Drittanbieter, die gemanagt werden müssen.
- **Weitreichende globale Vorschriften** verlangen mehr Verantwortlichkeit für Datenschutz, Sicherheit und Privatsphäre von Privatanwendern, darunter z. B. **PSD2, GDPR, SEPA** und **FFIEC**.
- **Innovationen bei Zahlungen**, z. B. **EMV 3D-Secure**, das den Geschäftsverkehr über die 3DS-Umgebung ankurbeln soll, „**Faster Payments**“ (in seinen unterschiedlichsten Formen auf der ganzen Welt), Crowd-Payment- sowie und

RSA Fraud & Risk Intelligence Suite

- ***Vertrauen schaffen*** *– ohne Komfortverluste*
- ***Weniger Betrug****, nicht Kunden oder Umsatz*
- ***Aufdeckung der Risiken*** *bei jeder digitalen Interaktion*
- ***Optimierte Einblicke*** *mit kollektiver Intelligenz*
- ***Höhere Effizienz*** *bei der Betrugsbekämpfung*
- ***Schneller sein als Cyberkriminelle***

andere FinTech-Anwendungen, sorgen für einen drastischen Anstieg digitaler Zahlungen. Folglich steigt auch der Gesamtwert der Gelder, die über digitale Channels übertragen werden, was die Unternehmen weiteren Risiken von Betrugsverlusten aussetzt.

- Das Internet der Dinge (**IoT**), das es unterschiedlichen Geräten ermöglicht, im Namen des Privatanwenders verschiedene Aktionen auszuführen (man nehme nur *Alexa* als Beispiel) – mit der Folge, dass die Identität des Kontoinhabers quasi verschwindet. Und doch müssen auch hier die Unternehmen in der Lage sein, eine legitime digitale Interaktion von einer betrügerischen zu unterscheiden.
- Es mehren sich also die Möglichkeiten der Kompromittierung und Sicherheitslücken, wenn Unternehmen ihre **Omnichannel-Strategien** ausweiten. Jeder neue Channel bietet zwar mehr Effizienz und einen optimierten Zugriff auf die Finanzdaten, er schafft aber auch potenzielle Sicherheitslücken.
- **Der drastischen Zunahme der digitalen Aktivitäten und Transaktionsvolumina** steht nur ein minimaler (oder gar kein) Anstieg der Ressourcen gegenüber, die in den Unternehmen zur Verfügung stehen, um Betrug einzudämmen und zu untersuchen. Dies könnte dazu führen, dass die Betrugsteams **gar keine Fälle mehr markieren**, weil sie die große Flut an Fällen gar nicht mehr analysieren können. Dies ist sehr gefährlich, da die Analysten ohnehin Schwierigkeiten haben, zu verstehen, welche Fälle am wichtigsten sind und was prioritär behandelt werden sollte. Diese mangelnde Transparenz für eine rasche Identifizierung betrügerischer Aktivitäten – damit sie noch verhindert werden können – kann dazu führen, dass Betrugsfälle auch dann noch unbemerkt bleiben, nachdem sie Verluste verursacht haben. Und die Verluste können sehr dramatisch sein. Außerdem sind die Sicherheitsteams möglicherweise gar nicht in der Lage, Fragen der Geschäftsführung zur Art der Angriffe, der Gefährdung des Unternehmens oder den allgemeinen geschäftlichen Auswirkungen zu beantworten.

Diese Zunahme der digitalen Interaktionen zwischen Privatanwendern und Unternehmen eröffnet zwar einerseits neue Umsatzchancen, andererseits erhöht sich jedoch auch die Gefahr potenzieller Beeinträchtigungen und Sicherheitslücken. Die Unfähigkeit, digitale Betrugsversuche in Echtzeit zu identifizieren oder zwischen legitimen Websitenutzern und Cyberkriminellen zu unterscheiden, kann für die Unternehmen schwerwiegende Folgen haben. Daher ist eine ordnungsgemäße Planung erforderlich. Onlinebetrug schmälert das Umsatzvolumen jährlich um Milliarden von US-Dollar. Dies betrifft sowohl die direkten als auch die indirekten finanziellen Verluste. Außerdem wird ein Markenschaden verursacht, der die Fähigkeit der Unternehmen weiter einschränkt, Kunden zu gewinnen und zu halten. Betrüger versuchen zunehmend, nicht autorisierte Konten zu eröffnen und bestehende Konten zu übernehmen.

Folglich müssen die Unternehmen auch in der Lage sein, Betrug in Echtzeit zu erkennen und die richtigen Kontrollen zu implementieren, um betrügerische Transaktionen – ebenfalls in Echtzeit – abzuwehren. Sie benötigen einen umfassenden Überblick darüber, was die Nutzer in ihren digitalen Channels zu jeder Zeit tun, damit böswilliges Nutzerverhalten wie Kontoübernahmen und betrügerische Geldtransaktionen offengelegt werden können. Sie müssen jedoch auch in der Lage sein, auf Betrugsfälle entsprechend ihrer Risikotoleranz, ihren Ressourcen und ihren strategischen Prioritäten zu reagieren.

Obwohl die meisten Unternehmen mehr als ein halbes Dutzend unabhängiger Betrugsbekämpfungstools nutzen, die allerdings nur jeweils ein spezifisches Problem lösen, fehlt es vielen an der Möglichkeit, diese miteinander in Bezug zu bringen. Wenn die Unternehmen nun Omnichannel-Strategien umsetzen, wird es umso notwendiger sein, Daten aus den verschiedenen Betrugsbekämpfungstools zu korrelieren, um die Betrugserkennung kanalübergreifend zu verbessern und das Fallmanagement zu zentralisieren.

In den vergangenen Jahren wurde Betrug in erster Linie als ein Technologieproblem und die Maßnahmen zur Betrugsprävention als reine Kostenstelle betrachtet. Dies trifft jedoch kaum noch zu. Die Unternehmen sehen die Maßnahmen zur Betrugsbekämpfung nun aus dem Blickwinkel der geschäftlichen Auswirkungen und stellen die Sicherheit der Dinge an oberste Stelle, die für das Unternehmen am wertvollsten sind. Hierzu gehören der Schutz ihrer Einnahmequellen sowie die Bereitstellung einer sicheren und reibungslosen digitalen Erfahrung für die Privatanwender.

Geschäftsorientierte Omnichannel-Betrugsmanagementstrategie

Legacy-Betrugsbekämpfungstools können Unternehmen nicht ausreichend vor Angriffen neuer und sich ständig weiter entwickelnder Betrugsrisiken schützen. Es ist Zeit für einen neuen Ansatz, der die Stärke der Partnerschaft zwischen technischen und geschäftlichen Führungskräften nutzt.

Das geschäftsorientierte Omnichannel-Betrugsmanagement bietet ein mehrstufiges Modell zum Schutz des Zugriffs und der Transaktionen von Privatanwendern über alle digitalen Channels hinweg und ermöglicht es den Unternehmen, ein ausgewogenes Verhältnis zwischen Umsatz, Risiken, Kosten und Benutzerfreundlichkeit zu schaffen.

Ziel einer geschäftsorientierten Omnichannel-Betrugsmanagementstrategie ist, dass die gewünschten Geschäftsergebnisse korrekt umgesetzt werden. Die Betrugs- und Sicherheitsteams müssen die Geschäftsziele verstehen, und jede Entscheidung muss mit dem gewünschten Geschäftsergebnis übereinstimmen.

Diagramm 1: Betrugsprävention für alle Channels

Die Einrichtung simpler KPIs wie Umsatzziele, Transaktionsabbruchsraten, Kundeneingriffe, Betrugserkennungsraten oder Vorbeugung von Verlusten durch Betrug ist ein Anfang. Wenn diese KPIs von der Geschäftsführung definiert werden, können die Betrugsmanagement-Teams eine geschäftsorientierte Betrugsmanagementstrategie wie folgt entwickeln und umsetzen:

- **Schaffung eines Gleichgewichts zwischen dem Privatanwendererlebnis in den digitalen Channels auf der einen und dem Risiko von Betrugsverlusten auf der anderen Seite:** Die Nutzer von heute fordern einen schnellen und einfachen Zugriff auf Konten, Produkte und Services in digitalen Channels und wollen nicht, dass ihre Erfahrung unterbrochen wird. Jede erfolgreiche geschäftsorientierte Betrugsmanagementstrategie muss die Sicherheitsanforderungen des Unternehmens mit dem Bedürfnis nach einem bequemen Nutzerzugriff und reibungslosen Nutzererlebnis in Einklang bringen.

- **Auswahl der richtigen Authentifizierungsmethoden für Privatanwender:** Dies kann ebenfalls von entscheidender Bedeutung sein, denn es gibt kein Authentifizierungsmodell, dass für alle gleich gut geeignet ist. Die Unternehmen sollten verschiedene Authentifizierungsmethoden anbieten, die in den unterschiedlichen digitalen Channels bequem verwendet werden können. Die Unternehmen sollten nach Methoden Ausschau halten, die korrekt arbeiten und wenig falsch positive und negative Ergebnisse aufweisen, da sich dies direkt auf das Nutzererlebnis und die Betrugspräventionsrate auswirkt. Die Bereitstellung eines reibungslosen Nutzererlebnisses für die Mehrzahl der Endnutzer ist ein wichtiger Faktor für die Kundenzufriedenheit. Da die Privatanwender erwarten, dass sie jederzeit und von jedem Gerät aus auf sichere, bequeme Weise digital mit dem Unternehmen interagieren können, kann es zu einer Zunahme der Transaktionsabbruchraten oder zu einer Abwanderung von Kunden führen, wenn diese Erwartungen nicht erfüllt werden. Und dies wiederum mindert die Einnahmen des Unternehmens.
- **Korrekte Bewertung des Risikos im Zusammenhang mit der digitalen Interaktion von Privatanwendern:** Dies ist wichtig, um zu entscheiden, welcher Nutzer transparent authentifiziert werden kann und wer zu einer zusätzlichen Authentifizierung aufgefordert werden sollte. Eine hochpräzise risikobasierte Authentifizierungslösung mit hohen Betrugserkennungsraten und wenig falsch positiven Ergebnissen ist unerlässlich, um dieses Ziel zu erreichen.
- Überprüfen, ob **vollständige Transparenz dahingehend besteht, wie die Privatanwender über all ihre digitalen Channels hinweg interagieren:** Dies ist besonders wichtig, da die Unternehmen mehr digitale Channels für die Interaktion mit ihren Kunden öffnen möchten. Betrüger suchen stets nach dem schwächsten Glied und greifen weniger geschützte Channels an. Die Unternehmen sollten sich nach Lösungen umsehen, die ihnen Transparenz und Einblicke dahingehend liefern, wie sich die Privatanwender in ihren digitalen Channels verhalten. Nur so können sie einen Betrüger von einem legitimen Nutzer unterscheiden.
- Einsicht, dass sie Betrug nicht allein bekämpfen können: Um die Betrugsprävention und -minimierung erfolgreich zu bewältigen, sollten Unternehmen **zusammenarbeiten und Erkenntnisse zu bestätigten betrügerischen Aktivitäten austauschen**, damit ein betrügerischer Angriff mit ähnlichen Attributen in anderen Unternehmen verhindert werden kann. Durch die Macht einer Gemeinschaft, die gemeinsam gegen Betrug vorgeht, lassen sich Verluste durch Betrug deutlich reduzieren.

Die geschäftsorientierten Omnichannel-Betrugsmanagementlösungen von RSA

Die RSA Fraud & Risk Intelligence Suite wurde für Unternehmen entwickelt, die ihre Bemühungen in der Betrugsprävention mit ihrer Risikotoleranz und ihren strategischen Prioritäten abstimmen möchten, damit sie Betrug – und nicht ihren Kundenstamm – reduzieren können. Die Suite bietet mit einer zentralisierten Strategie für die Betrugserkennung und -minimierung einen umfassenden Überblick über digitale Channels und kombiniert auf einzigartige Weise eine risikobasierte Entscheidungsfindung, vorausschauende Analysen, tiefgreifende Entitätsprofilerstellung, flexibles regelbasiertes Richtlinienmanagement und gemeinsame globale Betrugserkenntnisse mit der Fähigkeit, Einblicke aus anderen Betrugsbekämpfungstools zu integrieren, um Risikobewertungen anzureichern und Kunden besser vor Cyberangriffen zu schützen.

Durch die Analyse jeder Interaktion zwischen Endnutzern und dem digitalen Channel deckt die Suite Betrug auf, der andernfalls unentdeckt bleiben würde. Darüber hinaus unterstützt die RSA Fraud & Risk Intelligence Suite die risikobasierte Entscheidungsfindung an wichtigen Punkten einer Sitzung wie z. B. Anmeldungen und Transaktionen. Die selbstlernende Risiko-Engine erstellt detaillierte Entitätsprofile und errechnet eine Risikobewertung, die die Wahrscheinlichkeit darstellt, dass die Aktivität von einem Betrüger durchgeführt wird.

Die RSA Fraud & Risk Intelligence Suite schützt jeden Schritt bei der digitalen Transformation für Privatanwender:

- **RSA FraudAction™** ist ein externer Bedrohungsmanagementservice, der Angriffe abwehrt und Informationen zur Betrugsaufklärung bietet. Von der Erkennung bis zur Sperrung bietet RSA FraudAction 360 einen lückenlosen Schutz vor Phishing- und Trojaner-Angriffen sowie nicht autorisierten mobilen Apps und Social Media-Seiten. Der FraudAction Cyber Intelligence-Service bietet umfassende Einblicke in die Cyberkriminalität, die Ihre Marken betreffen könnte. Der Service greift auf seine in vielen Jahren gewonnenen Erkenntnisse aus dem Dark Web kombiniert mit umfassenden Recherchen in Social Media-Foren zurück.
- **RSA Adaptive Authentication** ist ein fortschrittlicher Hub für die Omnichannel-Betrugserkennung, der eine risikobasierte mehrstufige Authentifizierung für Unternehmen bietet, die ihre Kunden vor Betrug durch digitale Channels schützen möchten. Gestützt auf die RSA Risk Engine analysiert RSA Adaptive Authentication das mit den Aktivitäten eines Nutzers während und nach der Anmeldung verknüpfte Risiko durch die Bewertung verschiedener Risikoindikatoren. Unter Verwendung leistungsstarker ML-Funktionen und Optionen für differenzierte Richtlinienkontrollen fordert der RSA Adaptive Authentication-Hub nur dann zusätzliche Sicherheit an (z. B. eine zusätzliche Authentifizierung), wenn ein hohes Risiko vorliegt und/oder die vom Unternehmen festgelegten Regeln verletzt werden. Diese Methode ermöglicht für die Mehrzahl der Nutzer eine transparente Authentifizierung und sorgt so für ein reibungsloses Nutzererlebnis und hohe Betrugserkennungsraten.
- **RSA Adaptive Authentication for eCommerce** ist die EMV 3-D Secure-Lösung von RSA für Kreditkartenaussteller und -verarbeiter. Mit Adaptive Authentication for eCommerce, das auf dem 3-D Secure-Protokoll und der zugehörigen Infrastruktur aufsetzt, können Händler und Aussteller Karteninhabern ein einheitliches, sicheres Shopping-Erlebnis im Internet bieten und zugleich das Risiko von Verlusten durch Rückbelastungen minimieren. Gestützt auf die RSA Risk Engine ermöglicht RSA Adaptive Authentication for e-Commerce ein reibungsloses Einkaufserlebnis, indem legitime Karteninhaber nahtlos authentifiziert und nur wenig Endnutzer, nämlich die mit hohem Risiko, zu einer zusätzlichen Authentifizierung aufgefordert werden. Die Fähigkeit der Lösung, nur in der richtigen Situation weitere Authentifizierungen anzufordern, Betrug zu eliminieren und zugleich „guten“ Kunden ein reibungsloses Einkaufserlebnis zu bieten, ist in der Branche einmalig.

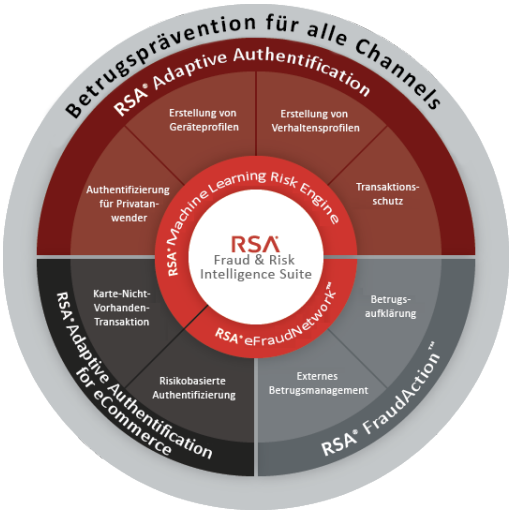

Diagramm 2: RSA Fraud & Risk Intelligence Suite – Schutz des digitalen Lebenszyklus der Privatanwender

Bewährter Schutz vor Privatanwenderbetrug

- ***Mehr als 2 Milliarden*** *Privatanwender sind geschützt*
- ***Mehr als 4 Milliarden USD*** *Betrugsverluste werden pro Jahr verhindert*
- ***Über 1 Million*** *Cyberangriffe wurden abgewehrt*
- ***Betrugserkennungsrate von 95 %*** *bei einer* ***Interventionsrate von nur 3–5 %***

Tausende *direkte und indirekte Kunden leisten einen täglichen* ***Beitrag*** *zum* ***RSA eFraudNetwork*** *– einer Community, die gemeinsam gegen Betrug vorgeht*

Die RSA Fraud & Risk Intelligence Suite bindet isolierte Funktionen und Datenquellen ein, um einen ganzheitlichen Überblick über die einzelnen Nutzeraktivitäten und -verhaltensweisen zu bieten. Dieses produktübergreifende Vorgehen sorgt für eine genauere Betrugserkennung. Außerdem ermöglicht dies eine äußerst granulare und personalisierte Strategie zur Betrugsbekämpfung, die auf die Risikotoleranz und strategischen Prioritäten Ihres Unternehmens ausgerichtet ist.

Es gibt zahlreiche Integrationspunkte für die Lösungen der RSA Fraud & Risk Intelligence Suite, darunter:

- RSA eFraudNetwork™ – das weltweit erste und größte Repository bestätigter Betrugsdatenelemente, die von RSA Fraud & Risk Intelligence-Kunden gemeinsam genutzt werden. Durch die Nutzung der im eFraudNetwork veröffentlichten Informationen, die auf bestätigten Betrugsfällen basieren, die von anderen Unternehmen gemeldet wurden, können Kunden neue Arten betrügerischer Aktivitäten schnell aufdecken und Betrug in ihrer Umgebung verhindern.
- Der Ansatz des RSA Adaptive Authentication Eco System wurde entwickelt, um die Betrugserkennung zu optimieren, indem Daten aus unterschiedlichen Quellen herangezogen werden. Durch die Nutzung faktischer Daten von Drittanbietern, die in die Risikobewertung einfließen und den Risikofaktor bestimmen, können Kunden zusätzliche Erkenntnisse aus internen Business Intelligence- und anderen Betrugsbekämpfungstools einbringen. Derzeit haben mehr als die Hälfte der Unternehmen 4 bis 10 verschiedene Betrugsbekämpfungstools im Einsatz. Mit dem RSA Adaptive Authentication Eco System-Ansatz können die Unternehmen auf ihren vorhandenen Investitionen in verschiedene Betrugsbekämpfungstools aufbauen und die Risikobewertung und das Fallmanagement in Adaptive Authentication zentralisieren, um ihre Betriebskosten zu senken und die Betrugserkennungsrate zu erhöhen.

Die integrierten RSA Fraud & Risk Intelligence-Lösungen ermöglichen mehr Einblicke in die digitalen Channels Ihres Unternehmens und helfen Ihnen dabei, Betrug zu erkennen und zu minimieren – und zwar schneller und effizienter.

Die RSA Fraud & Risk Intelligence Suite bietet ganzheitliche Funktionen für die Betrugserkennung und -eindämmung über alle Channels hinweg. So können die Unternehmen wachsen, sich kontinuierlich an tiefgreifende Veränderungen und die zunehmenden Erwartungen der Privatanwender anpassen und zugleich Betrugsverluste und Betriebskosten reduzieren.

Mit einem geschäftsorientierten Ansatz zur Betrugsbekämpfung sind die Verantwortlichen besser gerüstet, um über die aktuellen geschäftlichen Auswirkungen von Betrugsrisiken zu diskutieren und sich auf die Zukunft vorzubereiten. Denn mit diesem Ansatz sind sie in der Lage, gemeinsam mit der Geschäftsführung sicherzustellen, dass das geschützt wird, was für das Unternehmen am wichtigsten ist: die Kunden. Stoppen Sie also Betrug, nicht Ihre Kunden!

Digitale Risiken betreffen alle
Wir helfen Ihnen, sie zu bewältigen

RSA bietet unternehmensgesteuerte Sicherheitslösungen, mit denen Unternehmen einen einheitlichen Ansatz für das Management digitaler Risiken nutzen können, der auf integrierter Sichtbarkeit, automatisierten Einblicken und koordinierten Aktionen basiert. RSA-Lösungen ermöglichen Unternehmen die effektive Erkennung und Abwehr komplexer Angriffe, das Management der Nutzerzugriffskontrolle sowie die Verringerung von Geschäftsrisiken, Betrug und Cyberkriminalität. RSA schützt Millionen Nutzer auf der ganzen Welt und trägt dazu bei, dass mehr als 90 % der Fortune-500-Unternehmen Erfolg haben und sich kontinuierlich an transformatorische Veränderungen anpassen.

Finden Sie heraus, wie Sie in einer dynamischen, hochriskanten digitalen Welt erfolgreich sein können. Besuchen Sie rsa.com/de-de.

RSA