Mobilität auf Eis gelegt: Bringen Sie Ihr Unternehmen wieder auf Kurs und sorgen Sie für die Eliminierung mobiler Risiken

Eine integrierte, anpassungsfähige mobile Risiko-Engine verringert Sicherheitsrisiken im Mobile-Banking-Kanal

Inhalt

Einleitung

Mobile Banking nimmt kontinuierlich an Bedeutung zu und wächst schneller als jeder andere Banking-Kanal. Viele Finanzinstitute erwägen den Ausbau ihrer Funktionen im mobilen Kanal, sorgen sich jedoch um die Sicherheit.

Zum Glück gibt es neue Sicherheitsverfahren, mit denen sich Risiken im Zusammenhang mit erweiterten Mobile-Banking- und Zahlungsfunktionen reduzieren lassen. Mobile Geräte müssen umfassend vor modernen Bedrohungen geschützt werden. Der Schlüssel zum Schutz des mobilen Kanals liegt in der Erkenntnis, dass dieser eng mit dem Online-Kanal verbunden ist. Für maximale Sicherheit müssen also Risikoindikatoren berücksichtigt werden, die sich über beide Kanäle erstrecken.

Der neue mobile Kanal

Über die enorm schnelle Verbreitung des Mobile Banking wurde bereits viel geschrieben. Branchenanalysten schätzen, dass der Kanal von über einem Drittel der erwachsenen US-Amerikaner genutzt wird.[1] Neben der beeindruckenden Akzeptanz steht fest, dass sich der durchschnittliche Mobile-Banking-Benutzer fast vier Mal pro Woche einloggt.[2]

Aktuelle Studien haben gezeigt, dass Mobile-Banking-Nutzer zu den profitabelsten Banking-Kunden gehören. Im Rahmen einer Präsentation auf der BAI Retail Delivery 2012 berichtete die Zions Bank zum Beispiel, dass Online-Banking-Kunden, die auch Mobile Banking nutzen, 29 Prozent rentabler sind als Online-Banking-Kunden, die kein Mobile Banking verwenden. Kunden, die den Online- und Mobile-Banking-Kanal nutzen, wiesen zudem eine um 63 Prozent niedrigere Fluktuationsrate auf als Kunden, die ausschließlich Online Banking betreiben.[3] Egal ob rentablere Kunden zur Verwendung von Mobile Banking tendieren oder Mobile Banking zu einer höheren Kundenrentabilität führt, ist eines klar: Die Banken müssen sich um mobile Kunden und den mobilen Kanal kümmern.

Leider jedoch gehen viele Funktionen im Mobile Banking noch nicht über „Online Banking Light“ hinaus. Die meisten Banken stellen im Mobile Banking lediglich eine eingeschränkte Auswahl der im Online Banking verfügbaren Funktionen bereit. Einige Finanzinstitute haben damit begonnen, Anmeldungen für das Mobile Banking über mobile Geräte zu ermöglichen. Das bedeutet, dass sich Kunden nicht mehr im Online Banking anmelden müssen. Außerdem können sie neue Zahlungsempfänger direkt über den mobilen Kanal registrieren. Bislang konnten oft nur Zahlungsempfänger ausgewählt werden, die zuvor im Online Banking registriert worden waren. Darüber hinaus unterstützen mehrere Banken nun auch mobile Zahlungen zwischen Einzelpersonen.

In der Tat ist es so, dass Anbieter von Mobile-Banking- und Zahlungsplattformen mehr mobile Funktionen entwickelt haben, als viele Finanzinstitute bereitstellen wollen. Zum Teil hängt die Zurückhaltung der Banken mit dem Akzeptanzrisiko zusammen, das stets mit neuen Funktionen verbunden ist. Entscheidend ist jedoch die Gefahr einer Bereitstellung von Funktionen, die unbekannte Betrugsrisiken aufweisen können. Selbst wenn Finanzinstitute Sicherheitsprobleme im Zusammenhang mit neuen Funktionen für Mobile Banking und mobile Zahlungen richtig erkennen können, stehen sie vor dem Problem, dass auf dem Markt erst wenige Kontrollen zur Risikominimierung verfügbar sind. Somit bremsen Sicherheitsbedenken das Wachstum und die Möglichkeiten des mobilen Kanals. Diese Bedenken sind ernst zu nehmen. Es gibt jedoch sehr wohl Sicherheitstechnologien, mit denen sich neue und verbesserte Funktionen für Mobile Banking und mobile Zahlungen schützen lassen.

Finanzinstitute müssen zunächst die realen Sicherheitsrisiken bekämpfen, die mit dem mobilen Kanal verbunden sind. Anschließend können sie sich den berechtigten Sicherheitsbedenken von Kunden zuwenden, um den Bereich mobiler Banking- und Zahlungsservices erfolgreich ausbauen zu können.

Die mobile Bedrohungslandschaft

Finanzinstitute sind zu Recht besorgt wegen mobiler Bedrohungen. Cyberkriminelle wenden schon heute verschiedene Taktiken im mobilen Bereich an und werden in Zukunft ihre Angriffe und Angriffsmethoden sicherlich weiter ausbauen. Wenn Finanzinstitute umfassendere Funktionen zur Bewegung von Geld über den mobilen Kanal bereitstellen, werden Cyberkriminelle ihre Angriffe intensivieren, neue Verfahren entwickeln und somit Betrugserkennungsexperten, die den Kanal sichern müssen, immer wieder herausfordern.

Auch wenn die meisten mobilen Bedrohungen bislang nur wenigen Kategorien angehören, können wir davon ausgehen, dass der mobile Kanal ein ähnliches Muster von eskalierenden Bedrohungen aufweisen wird wie der Online-Kanal.

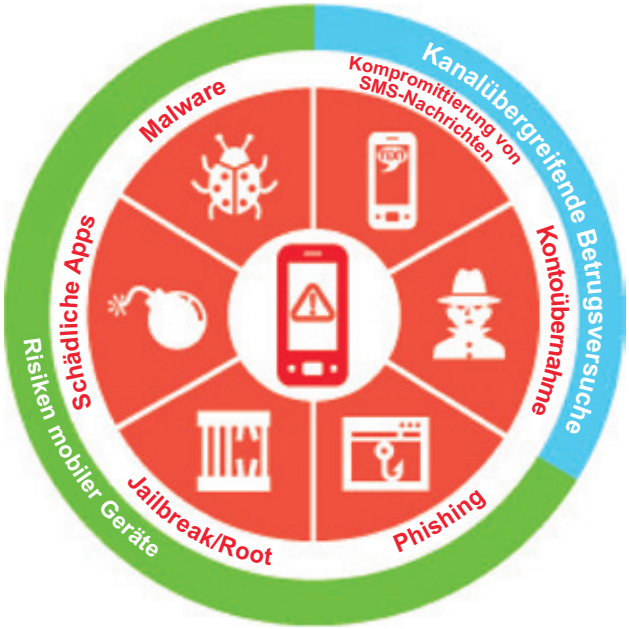

Abbildung 1: Die mobile Bedrohungslandschaft

Risiken mobiler Geräte

Cyberkriminelle greifen Schwachstellen mobiler Geräte an, um sich über den mobilen Browser Zugriff auf mobile Banking- und Zahlungskonten sowie auf Online-Banking-Konten zu verschaffen. Anders als Benutzer im ausgereifteren Online-Kanal kennen die meisten Mobile-Banking-Benutzer nicht die Bedrohungen des mobilen Kanals. Und Anbieter mobiler Plattformen und Anwendungen beginnen gerade erst mit der Entwicklung intelligenter Lösungen zur Gewährleistung der Sicherheit im mobilen Kanal. Darum unterscheiden sich mobile Angriffsvektoren deutlich von jenen im Online-Kanal.

Jailbreaks und Roots bei Geräten

Jailbreaks (bei Apple iOS-Geräten) und Roots (bei Android-Geräten) sind zwar miteinander verwandt, stellen jedoch unterschiedliche Ansätze zur Beseitigung von Einschränkungen bei der Softwareinstallation auf mobilen Geräten dar. Ein Grund, warum Gerätehersteller diese Einschränkungen durchsetzen, ist die Verbesserung des Sicherheitsstatus von Geräten: Zugriffe nicht vertrauenswürdiger Anwendungen (bei Apple) bzw. Zugriffe auf der Root-Ebene (bei Android) sollen verhindert werden. Damit sollen unerwünschte Zugriffe auf Geräte und Daten unmöglich werden. Benutzer wollen jedoch beliebige Anwendungen installieren und ihre mobilen Geräte modifizieren können. Viele von ihnen kennen die Risiken nicht, die mit Jailbreaks und Roots verbunden sind. Hacker nutzen die verbesserten Zugriffsmöglichkeiten modifizierter Geräte, um unbemerkt schädliche Anwendungen zu installieren und sensible Daten zu extrahieren.

Bösartige mobile Anwendungen

Bislang wurden bei Apple fast 50 Milliarden Apps heruntergeladen, bei Android waren es 48 Milliarden.[4] Das ist Cyberkriminellen natürlich nicht entgangen. Immer wieder werden über App Stores manipulierte mobile Spiel- oder Sicherheitsanwendungen angeboten, die mit Malware infiziert sind. Nach der Installation kann Malware sensible Informationen wie Anmeldedaten für Mobile Banking, SMS-Nachrichten und andere Daten abfangen.
Das Verfahren einer Infektion und Extrahierung von Daten wird erleichtert, wenn Endbenutzer ein Gerät mit Jailbreak oder Root verwenden. Die Ermittlung des Status der Geräte von Endbenutzern ist also eine entscheidende Komponente bei der Analyse mobiler Risiken.

Mobile Malware

Mobile Geräte können infiziert werden, wenn Benutzer auf Websites mit Exploit-Codes zugreifen, die Schwachstellen mobiler Browser ausnutzen (auch als Drive-by-Downloads bekannt). In diesen Fällen wird eine schädliche Anwendung heruntergeladen und heimlich ausgeführt, sodass Benutzer keinerlei verdächtige Aktivitäten bemerken. Die Malware kann Kontoanmeldedaten ausspähen oder Benutzer auf eine heimtückisch manipulierte Banking-Seite weiterleiten. Bislang wurde noch keine mobile Man-in-the-Browser-Malware entdeckt. Das ist jedoch nur noch eine Frage der Zeit.

Mobile Phishing

Mobile Benutzer tendieren stärker als Online-Benutzer dazu, auf bösartige Links zu klicken – unter anderem deswegen, weil die häufig für mobile Geräte verwendeten abgekürzten URLs nicht genügend Informationen enthalten, um Hinweise auf mögliche Risiken zu liefern. Mobile Benutzer klicken häufig rasch auf verschiedene Links. Die Persistenz mobiler Geräte sorgt dafür, dass mobile Benutzer mit einer höheren Wahrscheinlichkeit mit Phishing-Sites in Kontakt kommen als Online-Benutzer. Da die Erfolgswahrscheinlichkeit besonders hoch ist, wenden sich immer mehr Cyberkriminelle mobilen Benutzern zu. Mobile Phishing kann zum direktem Diebstahl von Anmeldedaten, Drive-by-Downloads von Malware oder der Installation von Social-Engineering-Malware führen.

Kanalübergreifende Risiken

Cyberkriminelle haben erkannt, dass Finanzinstitute Probleme damit haben, kanalübergreifende Betrugsversuche zu erkennen. Dies hat mit der siloartigen Natur von Bereitstellungskanälen, Betrugserkennungssystemen und Support-Abteilungen zu tun. Die Zahl der kanalübergreifenden Angriffe im Online-Kanal von Finanzinstituten nimmt genauso zu wie die Zahl der kanalübergreifenden Online-/Mobilangriffe.

Übernahme von Konten

Die Hauptsorge im mobilen Kanal gilt koordinierten Angriffen zur Kontoübernahme, die den Online- und mobilen Kanal umfassen. Cyberkriminelle stehlen per Malware oder Phishing die Anmeldedaten vom Computer eines Opfers, um mithilfe des mobilen Browsers das Konto zu übernehmen. Diese Methode wird dadurch erleichtert, dass viele Banken für den Online- und mobilen

Kanal die gleiche Kombination aus Benutzername und Kennwort verwenden sowie die gleichen Sicherheitsfragen zur Kennworterinnerung stellen.

Je nach Land werden mobile Angriffe zur Kontoübernahme auf verschiedene Weise durchgeführt. In den USA werden beim Mobile Banking mit einer mobilen Banking-App oder der mobilen Website einer Bank im Allgemeinen keine Zahlungen an neue Empfänger unterstützt. Kriminelle können jedoch die mobile Website umgehen und über den mobilen Browser auf die komplette Online-Banking-Site zugreifen, um alle Online-Banking-App-Funktionen der Bank zu nutzen – inklusive Hinzufügen neuer Zahlungsempfänger. Die Durchsetzung von Sicherheitskontrollen für die mobile App und die mobile Webseite ist sinnlos, wenn die gleichen Kontrollen nicht auch für den mobilen Browser durchgesetzt werden.

Es gibt einen wesentlichen Grund, warum Cyberkriminelle über den mobilen Kanal auf Konten zugreifen: die Einschränkungen bei den IDs mobiler Geräte. Eine der grundlegendsten Authentifizierungsmethoden, die Finanzinstitute für den Online- und mobilen Kanal nutzen, beinhaltet die Geräte-ID. Ein Krimineller, der sich mit einem neuen Gerät anmeldet, sollte einen Betrugsalarm auslösen, woraufhin der Zugriff auf das Konto eingeschränkt oder ganz unterbunden wird. Mobile Geräte (vor allem iPhones) haben jedoch eine gefährliche Eigenschaft: Für Systeme zur Erkennung der Geräte-ID sehen sie alle gleich aus. Wenn ein Benutzer mit seinem nativen mobilen Browser (zum Beispiel über ein iPhone mit Safari) auf eine Website zugreift, sind die Eigenschaften des Geräts identisch mit denen fast aller anderen iPhones: Sie verfügen über die gleiche Hardware, den gleichen Browser und die gleichen Schriftarten.

Bei diesem Angriffsschema verwenden Kriminelle Phishing-Methoden und Malware, um Anmeldedaten von den Computern ihrer Opfer zu stehlen. Denken Sie daran, dass die meisten Banken für den Online- und mobilen Kanal die gleichen primären und sekundären Authentifizierungsdaten verwenden. Als nächstes loggen sich die Kriminellen über ein mobiles Gerät und einen nativen mobilen Browser bei der Bank ein (ohne Mobile-Banking-App). Die Bank kann das Gerät nicht eindeutig identifizieren, da das iPhone des Kriminellen genauso aussieht wie das iPhone des Opfers (oder jedes andere iPhone). Der Anmeldeversuch des Kriminellen löst keine Risikoindikatoren aus, sodass der Weg frei ist für betrügerische Transaktionen. Hier versagen Sicherheitssilos.

Gefahren für mobile SMS-Nachrichten

Cyberkriminelle haben nicht lange gebraucht, um die Out-of-Band-Authentifizierung per SMS, die von vielen internationalen Banken genutzt wird, zu umgehen.[5] Der Angriff besteht aus zwei Teilen: Zuerst werden Online-Benutzer dazu gebracht, die Nummer ihres Mobiltelefons einzugeben, damit auf ihren Geräten eine neu erforderliche Sicherheitsanwendung installiert werden kann. Als nächstes werden Benutzer dazu angeleitet, die manipulierte Anwendung über einen per SMS versendeten Link zu installieren und den von der Malware bereitgestellten Aktivierungscode einzugeben. Nach der Installation erfasst die mobile Malware den gesamten SMS-Verkehr, darunter auch Einmal-Kennwörter, welche die Bank per SMS an das Opfer versendet, und leitet diese an die Betrüger weiter. Nun können die Kriminellen betrügerische Überweisungen vornehmen und die erforderlichen Einmal-Kennwörter abfangen, um SMS-basierte Out-of-Band-Autorisierungssysteme zu umgehen.

Mobile Bedrohungen der Zukunft

Wir wissen, dass sich mobile Bedrohungen weiterentwickeln werden. Dafür wissen wir aber noch nicht, welche mobilen Bedrohungen die Zukunft bringen wird. Unerlässlich ist jedoch eine zuverlässige, flexible und anpassungsfähige Plattform zur Abwehr von Betrugsversuchen. Ähnlich wie im Online-Kanal ist auch im mobilen Kanal die Fähigkeit zur umgehenden Erkennung neuer Betrugsrisiken und zur Implementierung von Maßnahmen zur Risikominderung entscheidend. Cyberkriminelle können sich sofort anpasssen, wodurch der Bedarf für einen Schutz entsteht, der ihrer List und Geschwindigkeit gewachsen ist.

Minimierung mobiler Betrugsrisiken

Da mobile Umgebungen besondere Risiken aufweisen, ist ein neuer Ansatz zur Betrugsverhinderung erforderlich. Die Plattform muss extrem flexibel sein, um gegen sich schnell verändernden Bedrohungen in diesem stetig wachsenden Kanal schützen zu können.

Die Sicherheit im mobilen Kanal setzt einen ganzheitlichen Ansatz voraus, der Schutz vor allen kanalübergreifenden und mobilspezifischen Angriffsvektoren bietet.

Mobile Risiko-Engine

Angesichts der aktuellen Bedrohungslage mit kanalübergreifenden Kontoübernahmeangriffen ist klar, dass Daten im Mobil- und Online-Kanal berücksichtigt werden müssen, wenn mobile Risiken konsistent und präzise ermittelt werden sollen. Eine mobile Risiko-Engine, die alle Risiken richtig identifizieren kann, muss geräte- und kontobezogene Risikofaktoren im Online- und mobilen Kanal erkennen, um mobile Risiken in nahezu Echtzeit bewerten zu können. Für einen optimalen Schutz vor mobilen Betrugsversuchen müssen diese Informationen miteinander verknüpft werden. Lösungen, die nur eine Art von Risikofaktoren berücksichtigen, sind nicht dazu geeignet, alle Betrugsversuche im mobilen Kanal zuverlässig zu erkennen.

- **Gerätebasierte Risikofaktoren:** Bestimmte Bedingungen auf der Geräteebene geben Auskunft über die Gesamtwahrscheinlichkeit, dass ein Gerät sicher genug ist, um Zugriffe über die spezielle Banking-App oder einen mobilen Browser zulassen zu dürfen.
- **Kontobasierte Risikofaktoren:** Hierzu gehören spezifische Sitzungs- und Kontoindikatoren wie Online-Erkennung von Malware und Phishing, ein Verlauf der Kontotransaktionen, Zugriffsmuster von Benutzern und die Korrelation von Benutzergeräten und Konten. Wenn diese Faktoren mit gerätebasierten Risikofaktoren verknüpft werden, ist eine effektive Betrugserkennung möglich. Ein Beispiel hierfür wäre die Korrelation eines untypischen Gerätestandorts (gerätebasierter Risikofaktor) mit einem kürzlichen Online-Phishing-Vorfall (kontobasierter Risikofaktor). Gemeinsam liefern die Faktoren deutliche Hinweise auf einen Betrugsversuch.
- **Gerätebasierte Risikofaktoren:** Bestimmte Bedingungen auf der Geräteebene geben Auskunft über die Gesamtwahrscheinlichkeit, dass ein Gerät sicher genug ist, um Zugriffe über die spezielle Banking-App oder einen mobilen Browser zulassen zu dürfen.
- **Kanalübergreifende Korrelation:** Durch die Korrelation von geräte- und kontobasierten Risikofaktoren mit sämtlichen Kanalinteraktionen und -transaktionen kann die mobile Risiko-Engine Risiken präzise vorhersagen. Der Schutz sollte auf alle Mobile-Banking- und Zahlungsmethoden ausgeweitet werden, darunter auch auf die native Mobile-Banking-App sowie den mobilen Webzugriff. Außerdem müssen alle kritischen Transaktionen geprüft und gesichert werden, darunter Zahlungen, Out-of-Band-Autorisierungen und doppelte Autorisierungen.

Schutz auf der Ebene mobiler Geräte

Die mobile Risiko-Engine nutzt Daten auf der Geräteebene zur Optimierung der Risikoanalyse. Ähnlich wie im Online-Kanal wird die Betrugserkennung deutlich genauer, wenn entscheidende gerätebasierte Daten in den Betrugsanalyseprozess integriert werden. Ohne diese Daten kann die Risiko-Engine Betrugsversuche nicht zuverlässig erkennen. Das Ergebnis: unentdeckte Betrugsfälle, eine hohe Zahl an falsch positiven Fällen sowie unnötige Unannehmlichkeiten für Kunden.

Eindeutige Geräte-IDs lassen sich auf mobilen Geräten deutlich schwerer erzeugen als auf einem Computer, da viele mobile Geräte extrem ähnlich erscheinen. Durch den Einsatz von Software auf dem Gerät oder ein integriertes Software Development Kit (SDK), das Geräte auch noch nach Entfernung und Neuinstallation einer mobilen Anwendung erkennen kann, ist es möglich, persistente IDs für mobile Geräte zu erzeugen. Außerdem gibt es Verfahren, mit denen sich genügend Eigenschaften zur Identifizierung eines Geräts ermitteln lassen, um eine eindeutige Geräte-ID zu generieren – besonders dann, wenn weitere sitzungs- und kontobasierte Faktoren berücksichtigt werden.

Gerätebasierte Risikofaktoren können verschiedenste Aspekte umfassen, darunter Geräte-IDs, Standort, IP-Adressen, Gerätezeiten, fehlende Sicherheitspatches in Betriebssystemen, Geräte mit Jailbreak/Root, riskante Konfigurationseinstellungen im System, Malware-Infektionen oder die Verwendung einer ungesicherten WLAN-Verbindung. Mit gerätebasierten Risikodaten lassen sich Funktionen je nach Geräterisiko einschränken, zum Beispiel durch die Beschränkung bestimmter Anwendungsfunktionen (wie Hinzufügen von Empfängern oder Überweisen von Geld) an Geräten mit Jailbreak.
In der Regel kann kein gerätebasierter Risikofaktor allein zuverlässige Hinweise auf Betrugsversuche liefern. Wenn jedoch verschiedene gerätebasierte Risikofaktoren mit weiteren kontobasierten Risikofaktoren korreliert werden, lässt sich die Betrugserkennung deutlich wirksamer gestalten.

Gerätebasierte Risikofaktoren sind eine wichtige Komponente der Analyse durch mobile Risiko-Engines und bieten bereits vor einer solchen Analyse Schutz auf der Geräteebene. Egal ob gerätebasierte Risikofaktoren einzeln oder in Kombination verwendet werden, kann ihre Analyse ein Finanzinstitut dazu veranlassen, Kontozugriffe zu unterbinden, bestimmte Kontofunktionen einzuschränken oder eine zusätzliche Authentifizierung zu verlangen. Außerdem können Banken sich und ihre Kunden noch besser schützen sowie den Kundendienst optimieren, wenn sie eine Option zur Selbstkorrektur bereitstellen.

Wenn eine Bank zum Beispiel erkennt, dass auf einem Gerät eine veraltete Betriebssystemversion ausgeführt wird, die einen ungenügenden Sicherheitsstatus mit sich bringt, kann die Bank ein Verfahren unterstützen, das es Benutzern ermöglicht, das Risiko selbst zu beseitigen. Hierzu stellt die Mobile-Banking-App schrittweise Korrekturanweisungen bereit.

Wir möchten noch einmal darauf hinweisen, dass Schutz auf der Geräteebene oder Analysen auf der Kontoebene auch für sich alleine nützlich sind. Doch erst durch eine Korrelation der beiden Schutzebenen lassen sich mobile Betrugsversuche zuverlässig und genau erkennen.

Konformitätsüberlegungen

Während die Branche noch auf genaue Anweisungen für mobile Geräte seitens der Bankenaufsicht wartet, ist klar, dass vorhandene Regeln für den Online-Kanal auch für den Banking-Kanal gelten. Das steigende Volumen mobiler Zahlungen in Ländern weltweit wird früher oder später zu regulatorischen Maßnahmen führen.

Die aktuellen Authentifizierungsrichtlinien des Federal Financial Institutions Examination Council (FFIEC) in den USA zum Beispiel schreiben vor, dass Finanzinstitute eine gründliche Risikobewertung für den mobilen Kanal vornehmen und kanalübergreifende Risiken im Zusammenhang mit dem mobilen Kanal untersuchen müssen. Sie müssen Kontrollen zur Risikominderung implementieren, darunter strikte Kontrollen bei hochriskanten Transaktionen (zum Beispiel Transaktionen, bei denen Geld in das Institut gelangt bzw. Geld die Bank verlässt). Die Authentifizierungsrichtlinien des FFIEC sehen außerdem vor, dass Finanzinstitute eine kontinuierliche Risikobewertung durchführen und verschiedene Sicherheitsebenen implementieren müssen, um betrügerische Transaktionen erkennen zu können.
Eine mobile Risiko-Engine erkennt hochriskante Aktivitäten durch eine Bewertung des Risikos einzelner mobiler Geräte, mobiler Anmeldeversuche und mobiler Transaktionen.
Zu den risikobasierten Handlungsempfehlungen können eine erneute Authentifizierung des Benutzers sowie eine Beschränkung des Zugriffs auf bestimmte Transaktionen oder das Konto gehören.

Fazit

Der mobile Kanal wird für die Erfahrung von Bankkunden zu einer immer wichtigeren strategischen Komponente. Sicherheitsbedenken führen jedoch dazu, dass erweiterte mobile Funktionen nur langsam eingeführt werden. Bankexperten wissen nämlich, dass Probleme schwere Folgen für die Akzeptanz und Nutzung haben können. Ein zuverlässiger Schutz des mobilen Kanals vor aktuellen und neuen Bedrohungen ist also entscheidend für dessen Akzeptanz, Annahme und Wachstumspotenzial.

Das Risiko mobiler Betrugsversuche muss ein zentraler Bestandteil der Gesamtstrategie von Banken zur Betrugsverhinderung sein. Die Zeit ist reif für die Entwicklung und Implementierung von Strategien, mit denen sich mobile Betrugsrisiken reduzieren und benötigte Funktionen in die gesamte Betrugsverwaltungsplattform von Finanzinstituten integrieren lassen. Eine besonders effektive Methode zur Ermittlung aktueller und zukünftiger Betrugsmuster ist die Bereitstellung einer integrierten und anpassungsfähigen mobilen Risiko-Engine. So lassen sich Mobile Banking sowie mobile Zahlungen leicht wieder auf Kurs bringen.

Warum IBM?

Unternehmen auf der ganzen Welt verlassen sich auf IBM Security Lösungen, wenn es um die Verhinderung von Betrugsversuchen sowie die Identitäts- und Zugriffsverwaltung geht. Mit unseren bewährten Technologien können Unternehmen Kunden, Mitarbeiter und geschäftskritische Ressourcen vor neuesten Sicherheitsbedrohungen schützen. Angesichts der ständig neuen Risiken hilft IBM Unternehmen dabei, ihre grundlegende Sicherheitsinfrastruktur mit einem umfassenden Portfolio an Produkten, Dienstleistungen und Business Partner Lösungen spürbar zu verbessern. Mit IBM können Unternehmen Sicherheitslücken schließen und sich auf den Erfolg ihrer strategischen Initiativen konzentrieren.

Weitere Informationen

Weitere Informationen zur mobilen Risikominimierung erhalten Sie von Ihrem IBM Ansprechpartner oder IBM Business Partner (BP). Oder besuchen Sie die folgende Webseite: **ibm.com**/security

Über IBM Security Lösungen

IBM Security bietet eines der modernsten und integrierten Portfolios von Sicherheitsprodukten und -services für Unternehmen an. Das Portfolio, das von der weltweit bekannten IBM® X-Force® Forschungs- und Entwicklungsabteilung unterstützt wird, umfasst umfangreiche Sicherheitsexpertise, damit Unternehmen Mitarbeiter, Infrastrukturen, Daten und Anwendungen zuverlässig schützen können. Wir bieten Lösungen für die Identitäts- und Zugriffsverwaltung, Datenbanksicherheit, Anwendungsentwicklung, Risikoverwaltung, Endpunktverwaltung, Netzwerksicherheit und vieles mehr an. Mit unseren Lösungen können Unternehmen Risiken erfolgreich verwalten und integrierte Sicherheitsverfahren für mobile und Cloud-basierte Umgebungen, soziale Medien sowie andere geschäftliche Architekturen implementieren. IBM verfügt über eine der weltweit größten Abteilungen für Forschung, Entwicklung und Bereitstellung im Bereich Sicherheit, überwacht in über 130 Ländern 13 Milliarden Sicherheitsereignisse am Tag und kann mehr als 3000 Sicherheitspatente vorweisen. Mithilfe von IBM Global Financing können Sie die für Ihr Unternehmen erforderlichen Softwarelösungen strategisch und kosteneffizient erwerben. Wir bieten kreditfähigen Kunden individuelle Finanzierungslösungen, die auf ihre Geschäfts- und Entwicklungsziele abgestimmt sind und ihnen helfen, ihre Geldmittelverwaltung zu verbessern und die Betriebskosten zu senken. Finanzieren Sie entscheidende IT-Investitionen mithilfe von IBM Global Financing, um die Geschäfte Ihres Unternehmens weiter voranzutreiben. Weitere Informationen finden Sie im Internet unter: **ibm.com**/financing/de

[1] Robin Arnfield, „Pew Survey Finds Mobile Banking on the Rise in U.S.“, Mobile Payments Today, 23. August 2013. http://www.mobilepaymentstoday.com/article/218409/Pew-survey-finds-mobile-banking-on-the-rise-in-U-S

[2] Robert McGarvey, „Study: Hard Numbers Reveal Growing Mobile Usage“, Credit Union Times, 20. August 2013. http://www.cutimes.com/2013/08/20/study-hard-numbers-reveal-growing-mobile-usage

[3] Robery McGarvey, „At BAI, Mobile Banking Rings the Cash Register: Onsite Coverage“, Credit Union Times, 10. Oktober 2012. http://www.cutimes.com/2012/10/10/at-bai-mobile-banking-rings-the-cash-register-onsi

[4] „Google I/O 2013: 900 million Android activations, 48 billion app downloads“, Examiner.com, 15. Mai 2013. http://www.examiner.com/article/google-i-o-2013-900-million-android-activations-48-billion-app-downloads

[5] George Tubin, „Is Your Risk Engine Short-sighted? Improve Its Vision with a Holistic View“, Trusteer Blog, 19. März 2013. http://www.trusteer.com/blog/is-your-risk-engine-short-sighted-improve-its-vision-with-a-holistic-view

Trusteer wurde im August 2013 von IBM übernommen.

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

Hergestellt in den Vereinigten Staaten von Amerika
August 2014

WGW03041-DEDE-01