Mobile Lösungen von IBM Trusteer

Erweiterung der Betrugsprävention für Ihre Mobile-Banking-Plattform durch eine dedizierte IBM Lösung, die Betrugsrisiken auf Basis von Risikofaktoren für Geräte und Konten kanalübergreifend erkennt.

Highlights

- Korrelation von Risikofaktoren für Geräte und Konten auf allen Online- und mobilen Kanälen.
- Vermeidung von Kontoübernahmen-attacken über mobile Geräte durch gestohlene Zugangsdaten.
- Erfassung persistenter Geräte-IDs, Geoortungsdaten und detaillierter Risikofaktoren bei Geräten.

Sicherheitsrisiken im mobilen Umfeld

Die Verbraucher von heute nutzen unterschiedliche Smartphones und Tablets, können zwischen verschiedenen Betriebssystemen wählen und müssen sich mit zahlreichen Sicherheitsrisiken befassen. Durch diese Vielzahl an Wahlmöglichkeiten wächst auch die Wahrscheinlichkeit, dass Benutzer eine verdächtige App installieren, Malware herunterladen und installieren (beispielsweise bei einem Drive-by-Download) oder einfach nur durch eine Social Engineering-Kampagne attackiert werden.

Internetkriminelle haben ihre Attacken mittlerweile auf mobile Geräte ausgedehnt. Sie umgehen dabei die ID des mobilen Geräts und kanalübergreifende Attacken mithilfe des Kennworts für einmaliges Anmelden (OTP, z. B. TAN) und konzentrieren sich mehr auf mobiles Phishing und Malware, um mobile Plattformen anzugreifen. Die Vorgehensweisen und Verfahren bei den Sicherheitsbedrohungen im mobilen Umfeld richten sich mittlerweile sowohl gegen Geräte als auch Benutzer. Verfahren wie kanalübergreifende Attacken, SMS-Weiterleitung, Malware und Phishing sind besonders im mobilen Umfeld zu finden, da es durch die Betriebssysteme der mobilen Geräte und Benutzerfehler zahlreiche Schwachstellen gibt.

Die hohe Zunahme bei den Betrugsmethoden im Mobilbereich und fehlende Sicherheitsmechanismen auf mobilen Geräten sind Anzeigen dafür, dass sich Internetkriminelle immer mehr auf diesen Bereich konzentrieren. Es steht also außer Frage, dass neue Verfahren zur Minderung dieser Betrugsrisiken im mobilen Umfeld zwingend erforderlich sind. Nur so ist ein ausreichender Schutz vor aufkommenden Bedrohungen in diesem nach wie vor schnell wachsenden Segment möglich.

Betrugsrisiken im Mobilbereich und deren Hintergründe

Mit der zunehmenden Anzahl an lohnenden Zielen und den eingeschränkten Möglichkeiten zur Betrugserkennung und -prävention ist der Mobilbereich für Internetkriminelle ein hoch interessantes Gebiet. Einige der Gründe hierfür sind nachfolgend aufgeführt:

- Mobile-Banking-Anwendungen verfügen nur über begrenzte Sicherheitsmechanismen, bei denen das Risiko durch Geräte nicht berücksichtigt wurde.
- Nicht ausgereifte Betrugserkennungssysteme im Mobilbereich erhöhen die Wahrscheinlichkeit von Attacken.
- Durch die weite Verbreitung der Mobile-Banking- und Zahlungs-möglichkeiten wird der Mobilbereich zu einem attraktiven Ziel.

IBM Security Trusteer Mobile Risk Engine

Die Trusteer Mobile Risk Engine bietet eine zusätzliche Sicherheitsebene mit zahlreichen Schutzmechanismen und umfassenden Informationen zur Internetkriminaltität für die adaptive Malware-Prävention. Die IBM Lösungen lassen sich sehr schnell in bestehende Systeme integrieren, um innerhalb kürzester Zeit auch aktuelle Attacken erkennen und sich darauf einstellen zu können. Malware hat so praktisch keine Chance, Schaden anzurichten.

Betrugsgefahren im mobilen Umfeld nahezu in Echtzeit beurteilen

Mit der Trusteer Mobile Risk Engine wird das mobile Umfeld ausreichend geschützt, indem Risikobeurteilungen auf Basis von Risikofaktoren bei Geräten und Konten nahezu in Echtzeit vorgenommen werden. So können Unternehmen mithilfe präziser und zuverlässiger Empfehlungen, anhand derer der Endbenutzerzugriff eingeschränkt oder sogar verweigert werden kann, Risiken deutlich minimieren. Auf der Grundlage dieser Empfehlungen können Unternehmen zudem Authentifizierungen oder Transaktionsprüfungen in Bezug auf Endbenutzer, Sitzungen und Transaktionen mit erhöhtem Risiko ausweiten und intensivieren.

Die Trusteer Mobile Risk Engine bietet im Detail Folgendes:

- Webbasierter Service
- IBM Security Trusteer Mobile SDK
- IBM Security Trusteer Mobile Browser
- Angepasste, auf Daten abgestimmte Anwendungs-programmierschnittstelle (API)

Erkennung von Geräten mit hohem Risikopotenzial auf Basis mehrerer Datenquellen

Über die Trusteer Mobile Risk Engine werden präzise Sicherheitsempfehlungen auf Basis verschiedener geräte-spezifischer Risikofaktoren generiert. Um gezielt auf Einschränkungen bei der Bereitstellung und Integration eingehen zu können, kann die Lösung Risikodaten aus dem Trusteer Mobile SDK und dem Trusteer Mobile Browser (d. h. Komponenten auf dem Gerät) oder aus der Webanwendung des Kunden über die API verarbeiten. IBM pflegt hierfür eine globale Datenbank für kriminelle Geräte, die Unternehmen zur Verfügung steht. Über die Trusteer Mobile Risk Engine lässt sich zudem auf Risikodaten aus folgenden Quellen zugreifen:

- IBM Security Trusteer Pinpoint Malware Detection
- IBM Security Trusteer Pinpoint Criminal Detection
- IBM Security Trusteer Rapport

Korrelation von Risikodaten zum Online- und Mobile-Banking für eine zuverlässigere Risikoerkennung im Mobilbereich

Um auch komplexen Attacken in Online- und Mobilkanälen Paroli bieten zu können, lassen sich in der Trusteer Mobile Risk Engine kontenspezifische Risikofaktoren einbinden wie Malware-Infizierungen und Phishing-Incidents. Dieses erweiterte Datenspektrum wird über IBM Lösungen für die clientbasierte oder clientunabhängige Betrugsprävention – Trusteer Rapport bzw. Trusteer Pinpoint Malware Detection – erfasst. Mithilfe der Risikodaten lassen sich ganz präzise Kontoübernahmeversuche von mobilen Geräten aus erkennen, bei denen gefährdete Berechtigungsnachweise aus anderen Kanälen verwendet werden.

Ein Beitrag zu sicherem und störungsfreiem Mobile-Banking

Durch die Berücksichtigung verschiedener Risikofaktoren in unterschiedlichen Kanälen lässt sich mit der Trusteer Mobile Risk Engine praktisch der gesamte Lebenszyklus von Attacken ganz präzise verfolgen. Dabei kommen verschiedene, auf den Mobilbereich ausgerichtete Risikoerkennungsregeln zum Einsatz. Bei diesen werden aktuelle Angriffsmuster abgebildet und basierend auf dem weltweiten IBM spezifischen Wissen aktualisiert.

Trusteer Mobile SDK

Erkennung von Zugriffsversuchen mit hohem Risiko

Das Trusteer Mobile SDK wird gestartet, sobald die mobile Anwendung geöffnet wird, und erfasst verschiedene geräte-spezifische Risikofaktoren. Die Risikodaten werden dann an die Mobile-Banking-Anwendung übergeben und können verwendet werden, um die Funktionalität auf Basis der Risikostufe des Geräts einzuschränken. So kann beispielsweise die Nutzung bestimmter Anwendungsfunktionen eingeschränkt werden – z. B. Hinzufügen eines Zahlungsempfängers oder Überweisung von Geldbeträgen über ein per Jailbreak oder Rooting verändertes Gerät. Die Risikodaten können auch mit weiteren geräte- und kontenspezifischen Risikofaktoren korreliert werden, beispielsweise Malware-Infizierungen und Phishing-Incidents, um Zugriffsversuche und Transaktionen mit hohem Risiko-potenzial zu markieren.

Über das Trusteer Mobile SDK kann ein breites Spektrum an Daten ermittelt werden:

- Risikodaten
  - Jailbreak/Rooting
  - Jailbreaking-/Rooting-Hider
  - Finanzspezifische Malware
  - Betriebssystempatching
  - WiFi-Sicherheit
  - Verdächtige Apps
- Gerätedaten
  - Persistente Geräte-ID
  - WiFi-Verbindung oder Verbindungen zum Telekommunikationsnetzwerk
  - SIM-Daten (Subscriber Identity Module)
  - Anwendungs-ID
  - Logischer Name des Geräts
  - Datum/Uhrzeit vs. Zeitzone
  - Geoortung
  - Gesamtrisikobewertung pro WiFi-Name (auf Anforderung)
- Kontodaten
  - Benutzer-ID
  - Hashverschlüsselt für IBM
- Verschlüsselt für Bankzwecke
  - Sitzungs-ID

Generierung einer persistenten ID für das mobile Gerät für eine eindeutige Geräteidentifikation

Über das Trusteer Mobile SDK wird eine persistente ID für das mobile Gerät generiert. So können Unternehmen gezielt jedes Gerät identifizieren, das auf die native Mobile-Banking-Anwendung zugreift. Diese persistente Geräte-ID wird dem Konto des Endbenutzers zugeordnet, sodass jedes Gerät erkannt werden kann – auch dann noch, wenn für das Telefon ein neues Image eingespielt wurde. So wird sichergestellt, dass neue Geräte identifiziert, Anmeldeversuche durch bekannte Geräte ausgenommen und potenzielle Geräte mit betrügerischen Absichten sofort markiert werden.

Erweiterte Sicherheit bei Zertifizierungsstellen

Eine Möglichkeit, um viele Arten von Man-in-the-Middle-Attacken (MITM) zu erkennen und zu blockieren, ist das Certificate Pinning, das auch als SSL Pinning bezeichnet wird. Nach Erhalt des Serverzertifikats überprüft das Trusteer Mobile SDK das Serverzertifikat auf vertrauenswürdige Validierungsdaten. In der Regel sind diese Daten in Form einer vertrauenswürdigen Kopie dieses Zertifikats mit der App verbunden. Darüber hinaus können diese Daten in einem vertrauenswürdigen Hash oder elektronischen Fingerabdruck dieses Zertifikats oder dem öffentlichen Schlüssel des Zertifikats bereitgestellt werden.

Erweiterter aktiver Schutz

Per Rooting veränderte mobile Geräte machen es Internet-kriminellen noch leichter, eine Attacke über ein solches Gerät durchzuführen. Beim Rooting wird der standardmäßige Sandboxschutz innerhalb des Betriebssystems durchbrochen, sodass der Angreifer weitere betriebssystemspezifische Zugriffsberechtigungen erhält und weitere Angriffsvektoren freigesetzt werden. Mit dem Trusteer Mobile SDK lassen sich Rooting-Evasion-Verfahren auf Android-Geräten wie Rooting-Hider und aktive Hiding-Techniken erkennen.

Trusteer Mobile Browser

Sicherer mobiler Zugriff beim Online-Banking

Der Trusteer Mobile Browser ist ein sicherer Mobile-Browser, mit dem Endbenutzer auf sichere Weise auf Online-Banking-Websites zugreifen können. Finanzinstitute können festlegen, dass der Zugriff auf ihre Online-Banking-Websites nur über den Trusteer Mobile Browser erfolgen kann. Sobald der Zugriff auf eine geschützte Website erfolgt, wird auf dem Gerät eine umfassende Beurteilung des Sicherheitsniveaus vorgenommen. Der Trusteer Mobile Browser erfasst alle Risiko-faktoren in Bezug auf das mobile Gerät und eine persistente ID des mobilen Geräts. Diese Daten werden dann an die Online-Banking-Website und die Trusteer Mobile Risk Engine gesendet. Dort wird dann anhand der Daten eine Beurteilung des mobilen Risikos vorgenommen.

Benachrichtigung des Benutzers über Sicherheitsrisiken durch das Gerät

Benutzer des Trusteer Mobile Browsers können den Sicherheitsstatus ihres Geräts über ein entsprechendes Dashboard anzeigen. Sobald es Anzeichen für Malware-Infizierungen gibt, werden nicht gesicherte Mobilverbindungen und andere Sicherheitsrisiken ermittelt. Der Endbenutzer kann diese Risiken dann schrittweise anhand vorgegebener Korrekturmaßnahmen in der Anwendung beheben.

Schutz des Benutzers vor falschen Bankwebsites

Der Trusteer Mobile Browser schützt den Benutzer auch vor Pharming-Attacken. Durch die Überprüfung der IP-Adresse und des SSL-Zertifikats beim Zugriff auf eine geschützte Website können sowohl Session-Hijacking (d. h. Man-in-the-Middle-Attacken) als auch Umleitungsattacken verhindert werden.

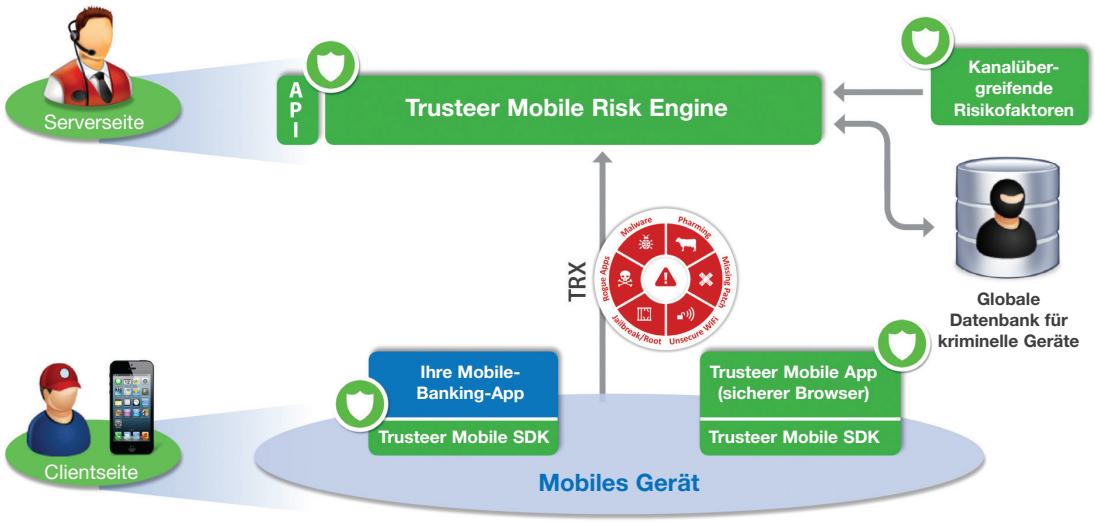

Abbildung 1: IBM Architektur für mobile Lösungen.

Warum IBM?

IBM Security-Lösungen genießen bei vielen Unternehmen in Bezug auf Betrugsprävention sowie Identitäts- und Zugriffsmanagement hohe Wertschätzung. Bewährte Technologien unterstützen Unternehmen beim Schutz ihrer Kunden, Mitarbeiter und geschäftskritischen Ressourcen vor Sicherheitsbedrohungen. Sobald neue Sicherheitsrisiken auftreten, kann IBM Unternehmen mit einem umfassenden Portfolio an Produkten, Services und Business Partner-Lösungen beim Aufbau einer zentralen Sicherheitsinfrastruktur helfen. Mit IBM Hilfe können Unternehmen Sicherheitslücken reduzieren und sich ganz auf den Erfolg ihrer strategischen Geschäftsinitiativen konzentrieren.

Weitere Informationen

Weitere Informationen zu Trusteer-Lösungen zur Vorbeugung vor Internetkriminalität erhalten Sie bei Ihrem IBM Ansprechpartner oder IBM Business Partner oder unter: **ibm.com**/security

Informationen zu IBM Security-Lösungen

IBM Security bietet beim Thema Unternehmenssicherheit eines der innovativsten Produkt- und Serviceportfolios mit dem höchsten Integrationsfaktor. Das Lösungsportfolio, das von der weltweit anerkannten IBM X-Force-Forschungs- und Entwicklungsgruppe unterstützt wird, stellt Sicherheitsdaten bereit, mit denen Unternehmen mit einem ganzheitlichen Ansatz Mitarbeiter, Infrastrukturen, Daten und Anwendungen schützen können. Hierfür steht eine große Anzahl von Lösungen für die unterschiedlichsten Bereiche zur Verfügung: Identitäts- und Zugriffsmanagement, Datenbanksicherheit, Anwendungsentwicklung, Risikomanagement, Endpunktmanagement, Netzwerksicherheit und vieles mehr. Mit diesen Lösungen können Unternehmen ihr Risikomanagement wesentlich effektiver gestalten und integrierte Sicherheitsmechanismen für Mobile-, Cloud-, Social Media- und andere Geschäftsarchitekturen implementieren. IBM betreibt eine der weltweit größten Organisationen im Bereich der Erforschung, Entwicklung und Bereitstellung von Sicherheitslösungen, verwaltet die Überwachung von 15 Mrd. Sicherheitsereignissen pro Tag in mehr als 130 Ländern und besitzt über 3.000 Sicherheitspatente. Finanzierungslösungen von IBM Global Financing können Ihnen bei der kosteneffizienten und strategisch richtigen Anschaffung von Softwarefunktionalität für Ihr Unternehmen helfen. Wir arbeiten bei der Ausarbeitung einer auf Ihre Geschäfts- und Entwicklungsziele abgestimmten Finanzierungslösung mit bonitätsgeprüften Kunden zusammen, um für Sie eine effektive Finanzdisposition und eine Reduzierung der Gesamtbetriebskosten zu erreichen. Finanzieren Sie Ihre kritischen IT-Investitionen und bringen Sie Ihr Unternehmen nach vorne mit IBM Global Financing. Weitere Informationen finden Sie unter: **ibm.com**/financing/de

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

Trusteer wurde von IBM im August 2013 übernommen.

Bitte der Wiederverwertung zuführen

WGS03025-DEDE-00