Kaspersky®
Fraud Prevention

# Kontobasierte Betrugserkennung für Online- und mobile Plattformen

## Angriffsflächen nehmen zu, Betrugsprävention muss kontobasiert und plattformübergreifend stattfinden

**Kaspersky Fraud Prevention Cloud:**
Analysiert die Kombination der Parameter und Ereignisse von allen Benutzergeräten, mit denen auf das entsprechende Konto zugegriffen wird.

Trifft Entscheidungen basierend auf der allgemeinen Risikobewertung der Geräte und Konten.

Ermöglicht die effiziente Erkennung komplexer Betrugsversuche auf Kontoebene und unterstützt Sie dabei, die Erkennungsgenauigkeit ständig zu verbessern.

Kundengeräte befinden sich außerhalb Ihres Sicherheitsperimeters und somit auch außerhalb Ihrer Kontrolle und sind oft nicht ausreichend oder sogar gar nicht geschützt. Trotzdem dürfen entsprechende Geräte auf vertrauliche digitale Banking-Apps zugreifen und eine Reihe risikoreicher Aktivitäten durchführen. Da die meisten Kunden mehrere Plattformen nutzen, um auf Ihre Banking-Services zuzugreifen, wird der Aufbau einer umfassenden Schutzstrategie für all diese Plattformen schnell zur Herausforderung.

Darüber hinaus greifen Betrüger oft eine Plattform an, um einen plattformübergreifenden Betrug durchführen zu können. So könnte ein Angreifer beispielsweise verhältnismäßig ungesicherte Banking-Anmeldedaten von Mobilgeräten stehlen, um diese für die Anmeldung beim Online-Banking zu nutzen und das Konto zu übernehmen. Dies führt unweigerlich zu dem Schluss, dass Schutz, der auf einzelnen Geräten oder Plattformen beruht, nicht ausreicht. Stattdessen ist ein ganzheitlicher Ansatz erforderlich. Eine solche Strategie muss das Konto in den Mittelpunkt rücken und sämtliche Plattformen abdecken.

**Kaspersky Fraud Prevention Cloud** kann Angriffe auf Benutzerkonten und Banking-Sitzungen erkennen:

- Kontoübernahme
- Betrug mit neuem Konto
- Phishing/Pharming
- Bots/Kartentests/Gegenprüfung von Anmeldedaten
- Angriffe mit Remote-Verwaltungstools
- Man-in-the-Browser-Angriffe

Kaspersky Fraud Prevention Cloud kombiniert vier wichtige Technologien zur Betrugsprävention, die auf lernfähigen Systemen basieren:

- **Clientless Malware Detection** überprüft, ob der Rechner des Kunden mit Malware infiziert ist, ohne auf Benutzerseite zusätzliche Software zu installieren. Diese Daten werden dann für die risikobasierte Authentifizierung (RBA), die Modellierung der lernfähigen Systeme und die Bestimmung der Legitimität von Transaktionen verwendet.
- **Verhaltensbiometrie:** Analysiert die Interaktion des jeweiligen Kunden mit seinem Gerät. Hierzu zählen Mausbewegungen, Klicks, Display-Berührungen, Wischgeschwindigkeit und mehr, um zu erkennen, ob das Gerät von einem legitimen Benutzer verwendet wird oder nicht. Diese Technologie erkennt auch Bots und Remote-Verwaltungstools.
- Die **Verhaltensanalyse** analysiert, worauf der Benutzer klickt und wie er sich bei der Anmeldung und in der Sitzung verhält. Darüber hinaus werden typische Navigations- und Zeitmuster sowie andere Aspekte untersucht. Mithilfe dieser Daten lässt sich ein Profil des normalen Verhaltens erstellen, um anormales Verhalten und verdächtige Aktivitäten zu erkennen.
- Die **Geräte- und Umgebungsanalyse** nutzt die globale Präsenz von Kaspersky Lab, um legitime Geräte zu erkennen, und verwendet diese Informationen für die Benutzerauthentifizierung. Basierend auf einer globalen Geräte-ID werden IP-Adresse, Standortreputation und viele weitere Eigenschaften von Geräten, die an betrügerischen Aktivitäten beteiligt waren, frühzeitig erkannt und als verdächtig angezeigt.

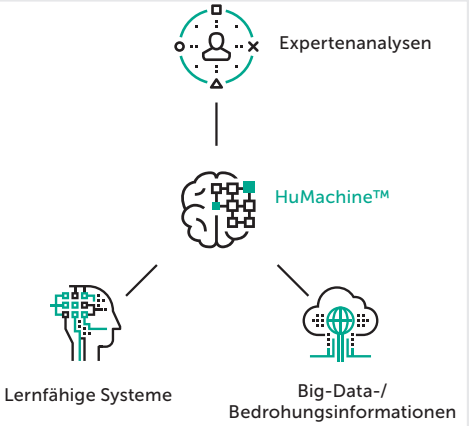
Lernfähige Systeme, die einen wichtigen Teil des Systems darstellen, erweitern diese Technologien und ermöglichen so zusätzliche Ebenen der Betrugserkennung:

Die **risikobasierte Authentifizierung** ermöglicht eine dynamische Bewertung des Risikos, wenn sich ein Benutzer beim System anmeldet. Basierend auf dieser Bewertung und den Echtzeiteinschätzungen von Kaspersky Fraud Prevention Cloud kann Ihr Unternehmen Entscheidungen dazu treffen, wie die Transaktion verarbeitet werden soll: Zugriff gewähren, zusätzliche Authentifizierung anfordern oder verfügbare Services einschränken. Hieraus ergeben sich völlig neue Möglichkeiten in der Betrugsprävention. So vermeiden Sie beispielsweise zusätzliche Authentifizierungsschritte für legitime Benutzer und können in Echtzeit auf Betrugsversuche reagieren.

**Continuous Session Anomaly Detection** bietet eine kontinuierliche Bewertung des Sitzungsrisikos, die auf der Analyse von Verhalten, Gerät und Umgebung, Biometriedaten und mehr basiert. Mithilfe dieser Informationen können interne Systeme zur Transaktionsüberwachung Betrugsversuche frühzeitig erkennen, entsprechende Reaktionen automatisieren und die Erkennungsrate steigern. Risikoreiche Transaktionen können als solche markiert und manuell verarbeitet werden, während die Verarbeitung legitimer Anfragen automatisch und somit ohne Verzögerungen erfolgt.

Kaspersky Fraud Prevention Cloud soll Ihre interne Überwachungslösung nicht ersetzen. Sie soll sie ergänzen, indem sie Ihren Teams dauerhaft die erforderlichen Daten bereitstellt, um betrügerische Aktivitäten frühzeitig zu erkennen, noch bevor eine Transaktion stattfindet. So können Ihre aktuellen Systeme den zusätzlichen Kontext für eine schnellere und präzisere Entscheidungsfindung sowie für den intelligenten und flexiblen Einsatz einer beschleunigten Authentifizierung nutzen.

**Kontaktieren Sie uns, um mehr zu erfahren: kfp@kaspersky.com**




Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **https://de.securelist.com/**
IT-Sicherheitsnachrichten: **business.kaspersky.com**

#truecybersecurity
#HuMachine

**www.kaspersky.de**