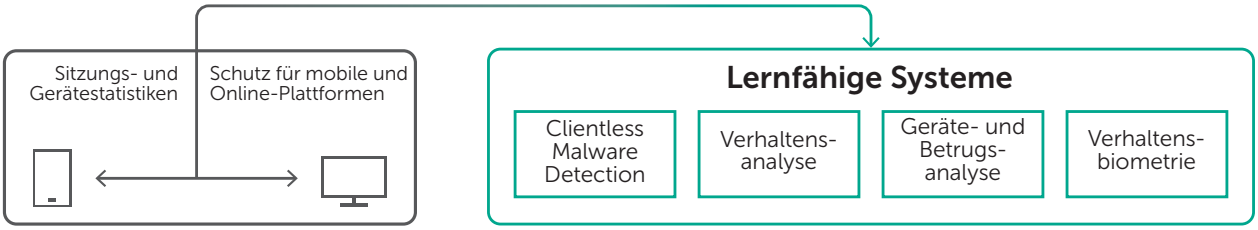
Kaspersky Fraud Prevention

Technologien für eine übergreifende Echtzeiterkennung von Betrugsversuchen

Unternehmen haben sich bereits weit über herkömmliche Services hinaus entwickelt und bieten Kunden Zugriff auf ihre persönlichen Konten über Online-Kanäle und mobile Geräte. Die digitale Transformation bringt neue Chancen, neue Kunden und natürlich auch neue Umsätze mit sich. Andererseits öffnet sie aber auch Tür und Tor für Betrüger, die neue, raffiniertere Methoden nutzen und übergreifende Angriffe auf Benutzergeräte und -konten starten.

Betrug mit neuem Konto	Kontoübernahme	Tools zur Betrugsautomatisierung
Manipulation von Transaktionen	Angriffe mit Remote-Verwaltungstools	Malware und Phishing

Kaspersky Fraud Prevention nutzt erweiterte Technologien mit lernfähigen Systemen für die schnelle Erkennung komplexer Betrugsmethoden in Online- und mobilen Kanälen – in Echtzeit, noch bevor eine Transaktion stattfindet.

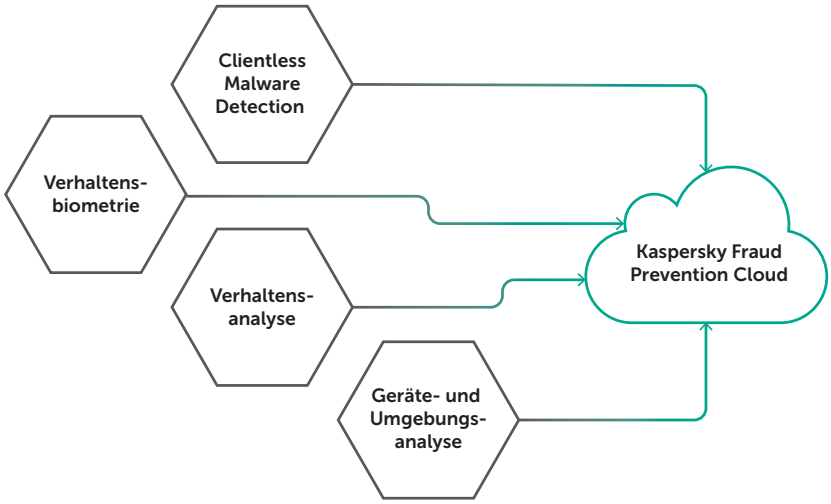


Clientless Malware Detection überprüft, ob der Rechner des Kunden mit Malware infiziert ist, ohne dass auf Benutzerseite zusätzliche Software installiert werden muss. Diese Informationen werden dann für die Bestimmung der Legitimität von Transaktionen, die risikobasierte Authentifizierung und die Modellierung der lernfähigen Systeme verwendet.

Die **Verhaltensanalyse** untersucht die Benutzeraktivität während der Anmeldung und der Sitzung, analysiert dabei typische Navigations- und Zeitmuster und ermittelt, wie der Benutzer in seinem persönlichen Konto agiert, worauf er klickt usw. Mithilfe dieser Daten lassen sich Profile des normalen Verhaltens erstellen, sodass anormales Verhalten und verdächtige Aktivitäten während der Anmeldung oder Sitzung erkannt werden.

Die **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 kann auch genutzt verwendet, um Bots oder Remote-Verwaltungstools 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.



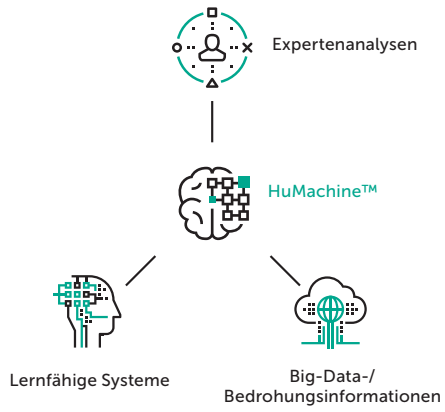
Lernfähige Systeme stellen einen wichtigen Teil der Kaspersky Fraud Prevention Platform dar. Verschiedene Methoden lernfähiger Systeme wie **Clustering, Entscheidungsbaum-Lernen und künstliche neuronale Netzwerke** steigern die Effizienz und Genauigkeit der Kaspersky Fraud Prevention-Technologien. Hieraus ergeben sich völlig neue Möglichkeiten in der Betrugsprävention. So vermeiden Sie beispielsweise zusätzliche Authentifizierungsschritte für legitime Benutzer und können während laufender Sitzungen in Echtzeit auf Betrugsversuche reagieren.

Aus der Verarbeitung anonymisierter Daten durch vier wichtige Technologien ergeben sich Echtzeiteinschätzungen in Kaspersky Fraud Prevention Cloud. Unsere Cloud-Lösung basiert auf der kontinuierlichen Analyse von Daten zur Geräte- und Sitzungsreputation in Online- und mobilen Kanälen, von Verhaltens- und Biometriedaten sowie anderen Aspekten und versorgt Ihre internen Überwachungssysteme mit Informationen, die eine frühzeitige und effiziente Betrugserkennung ermöglichen. So profitieren Ihre aktuellen Systeme vom zusätzlichen Kontext für eine rechtzeitige und präzise Entscheidungsfindung sowie die intelligente und flexible Nutzung einer beschleunigten Authentifizierung.

HAUPTVORTEILE:

- Dauerhafte Echtzeiterkennung erweiterter Betrugsversuche, bevor eine Transaktion stattfindet
- Betrugsschutz über Online- und mobile Kanäle hinweg
- Erkennung von Betrug und Geldwäsche
- Verbessertes Benutzererlebnis dank risikobasierter Authentifizierung (RBA) und damit mehr und zufriedenere Kunden
- Umfassende Sitzungsstatistiken für Forensik mit dediziertem Teamsupport
- Ergänzung bestehender Unternehmenslösungen für das Betrugsmanagement
- Produktivitätssteigerung dank Automatisierung

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



Informationen zur Internetsicherheit: **https://de.securelist.com/**
Informationen zu Partnern in Ihrer Nähe finden Sie hier:
http://www.kaspersky.com/de/partner_finden

www.kaspersky.de
#truecybersecurity