SAS Studie: Coronakrise lässt Betrug mit digitalen Zahlungsmitteln explodieren

Coronakrise lässt Betrug mit digitalen Zahlungsmitteln explodieren

Heidelberg, 5. November 2020 - COVID-19 hat mit Lockdown und Social Distancing nicht nur dem E-Commerce Auftrieb gegeben - sondern auch den Betrügern, die digitale Zahlungsmittel missbrauchen. Eine globale Studie, die Javelin Strategy & Research gemeinsam mit SAS, einem weltweit führenden Anbieter von Lösungen für Analytics und künstliche Intelligenz (KI), durchgeführt hat, belegt, dass kriminelle Aktivitäten im Zusammenhang mit digitalem Bezahlen und Online-Shopping zunehmen und immer raffinierter werden - inzwischen in einem globalen Kontext und mit Milliarden-Schäden.

"Wir sehen 2020 einen Anstieg der Betrugsversuche um fast 35 Prozent. Das ist ein Hinweis darauf, dass sich Kriminelle immer häufiger auf die boomenden digitalen Kanäle konzentrieren. Sie profitieren davon, dass sich Strategien zur Betrugsbekämpfung auf normales Käuferverhalten beziehen -, aber im Hinblick auf Zahlungstransaktionen ist 2020 nichts normal", sagt ein Fraud Management Executive eines globalen Kartenanbieters, der für die Studie befragt wurde.

Wichtigste Ergebnisse

Digitales Bezahlen stellt ein globales Risiko dar. Die Nutzung von Bezahltechnologien variiert zwar hinsichtlch der Region, dennoch gibt es übergreifende Betrugstendenzen. Das lässt darauf schließen, dass sich Kriminelle besser koordinieren und austauschen, als es Finanzinstitute tun. Damit haben sie gute Karten, Kontrollmechanismen zu unterwandern. Grenzüberschreitender Betrug ist inzwischen allgegenwärtig.

Digitaler Betrug nimmt zu - an Häufigkeit und Raffinesse. Betrüger und kriminelle Netzwerke setzen inzwischen Techniken ein, die genauso fortschrittlich sind wie die Technologien zu ihrer Abwehr. Social Engineering, Phishing, Identity Schemata und die Bandbreite an Methoden zur digitalen Bezahlung spielen Verbrechern in die Hände. Dabei sind gerade neue Methoden ein dankbares Ziel, da diese anfangs in der Regel noch nicht von ausgereiften Risikokontrollmechanismen begleitet werden.

Finanzinstitute brauchen einen speziellen Technologie-Layer und Analytics zur Echtzeit-Erkennung von Bedrohungen. Die Komplexität der Angriffe erfordert den Einsatz einer eigenen Technologie-Schicht in der IT-Infrastruktur, um Betrugsversuche rechtzeitig zu erkennen und zu vermeiden sowie gleichzeitig Strategien und Untersuchungen zentral zu steuern. Automatisierte Maßnahmen und prädiktives Fall-Management, unterstützt von KI und Machine Learning, können Mitarbeiter beim Monitoring betrügerischer Aktivitäten entlasten und somit helfen, die Effizienz zu steigern.

Daten sind essenziell. Datenbasierte Echtzeitanalysen und automatisierte Maßnahmen sind die Voraussetzung, um im "New Normal" Betrügern auf die Spur zu kommen. Inwieweit Unternehmen dazu schon in der Lage sind, hängt von ihrer technologischen Reife ab. Gemeinsam ist ihnen der Bedarf an maximal umfassenden Echtzeitdaten, um fundierte Entscheidungen treffen zu können. Die Implementierung von Cloud-Infrastrukturen ist ebenfalls ein wichtiger Faktor, um die erforderliche Menge an Daten für die Fraud-Management-Systeme verarbeiten zu können.

"Die Auswirkungen dieser Betrugswelle haben eine ganz neue Dimension - und zwar aufgrund der rasanten Verbreitung digitaler Bezahlmethoden in der ganzen Welt", sagt Stu Bradley, Vice President der globalen Fraud and Security Intelligence Division bei SAS. "Um das Problem effektiv zu lösen, brauchen Unternehmen eine breite Palette an Daten und einen hybriden Multilayer-Ansatz. Denn nur auf dieser Basis können sie Entscheidungen treffen - und das auch über die Pandemie hinaus. Advanced Analytics ist der gemeinsame Nenner, der die nötige Agilität schafft, um für die Zukunft vorbereitet zu sein."

Für die Studie The Escalation of Digital Fraud: Impacts of the Coronavirus on Global Fraud Challenges wurden Payment- und Security-Entscheidungsträger in 20 Ländern weltweit zwischen Januar und September 2020 befragt. Der Report steht hier zum Download bereit. Weitere Ergebnisse sowie Möglichkeiten, diesen Betrugsversuchen entgegenzutreten, werden in einem On-Demand-Webinar diskutiert.

Weitere Informationen zu den SAS Lösungen für Betrugsbekämpfung gibt es unter https://www.sas.com/de_de/solutions/fraud-security-intelligence.html.

Pressekontakt

Dr. Haffa & Partner GmbH

Herr Philipp Moritz
Karlstraße 42
80333 München

haffapartner.de
postbox@haffapartner.de

Firmenkontakt

SAS Institute GmbH

Herr Thomas Maier
In der Neckarhelle 162
69118 Heidelberg

https://sas.com/de_de/home.html
thomas.maier@sas.com

SAS ist Marktführer im Bereich Analytics und mit mehr als drei Milliarden US-Dollar Umsatz einer der größten Softwarehersteller. Kunden weltweit setzen innovative Software und Services von SAS ein, um Daten in Wissen zu verwandeln und intelligente Geschäftsentscheidungen zu treffen. Seit 1976 verschafft SAS Kunden THE POWER TO KNOW.

Mit SAS entwickeln Unternehmen Strategien und setzen diese um, messen den eigenen Erfolg, gestalten ihre Kunden- und Lieferantenbeziehungen

profitabel, steuern in Echtzeit die gesamte Organisation und erfüllen regulatorische Vorgaben.

Firmensitz der US-amerikanischen Muttergesellschaft ist Cary, North Carolina. SAS Deutschland hat seine Zentrale in Heidelberg und weitere Niederlassungen in Berlin, Frankfurt, Hamburg, und München. Weitere Informationen unter http://www.sas.com/de_de/company-information.html.

Anlage: Bild