Trotz Rezessionsangst: Black Friday versetzt Deutschland in Konsumrausch – geringere Betrugsquote trotz mehr Bestellanfragen

Pressemeldungen (B2B) E-Commerce

06.12.2024

- 3,5 Prozent mehr Bestellanfragen als im Vorjahr. Durchschnittlicher Bestellwert steigt um 10 Prozent auf 275 €.
- Aktionswoche zieht vor allem junge Kunden an: Altersschnitt der Käufer um 1,5 Jahre jünger als im Jahresdurchschnitt
- ngere Betrugsquote durch mehr reguläre Bestellungen. Höhere ugsquote zur Weihnachtszeit erwartet.

Anbieter mit hohen Rabatten gegenseitig übertrumpfen. Immer mehr Konsumenten nutzen diesen Tag für ihre Bestellungen. So verzeichneten Online-Händler 2024 mit 198 Prozent nahezu doppelt so viele Bestellanfragen als im Jahresdurchschnitt. Das geht aus einer Auswertung des Informationsdienstleisters CRIF hervor. Im Vergleich zum Black Friday 2023 stieg das von CRIF verzeichnete Anfragevolumen damit nochmals um 3,5 Prozent. Zusätzlich stieg der durchschnittliche Bestellwert um 10 Prozent auf 275 € (vorher 250 €). Dabei nutzen vor allem junge Menschen die Rabattaktion: Der Altersschnitt war in der Rabattwoche 1,5 Jahre jünger als im übrigen Jahr.

Geringere Betrugsquote trotz mehr Bestellanfragen

Für Betrüger sind die Aktionstage hingegen kein Grund, um ihre Aktivitäten auszuweiten: Zwar ist jede 133. Bestellung (0,75 Prozent) ein potenzieller Betrugsversuch. Verglichen mit den Wochen zuvor ist dies jedoch sogar ein Rückgang von 19,5 Prozent. Im Jahresdurchschnitt ist immerhin fast jeder 100. Bestellung (0,93 Prozent) ein möglicher Betrug. „Der Preis eines Gutes ist für Betrüger nicht relevant, für ehrliche Käufer hingegen schon. Aktionstage wie der Black Friday motivieren also verstärkt ehrliche Kunden zum Kauf, wodurch das Verhältnis zwischen Betrugsversuchen und regulären Bestellungen sinkt“, ordnet Dr. Frank Schlein, Geschäftsführer von CRIF Deutschland ein. „Anders wird es in der Weihnachtswoche sein, hier gehen weniger reguläre Bestellungen ein, während Betrüger weiterhin aktiv sind. Dadurch wird die Betrugsquote steigen“, prognostiziert Schlein.

Typische Betrugsmethoden und Schutzmaßnahmen

häufig genutzte Methode ist der **Identitätsdiebstahl**, bei dem Betrüger echte Identitäten missbrauchen, um Bestellungen aufzugeben. Daneben kommt es häufig zu **Eingehungsbetrug**, bei dem Bestellungen trotz offensichtlicher Zahlungsunfähigkeit getätigt werden. Ebenso verbreitet ist die Erstellung **erfundener Identitäten**, bei der falsche Bestellerprofile konstruiert werden, um betrügerische Transaktionen zu verschleiern. Ein weiteres Problem ist der **Retourenbetrug**, bei dem Rückgaberichtlinien manipuliert oder gefälschte Quittungen verwendet werden, um unrechtmäßig Rückerstattungen oder Ersatz zu erhalten. „Diese vielfältigen Betrugsmethoden zeigen, wie wichtig es ist, gezielte Maßnahmen zur Prävention und Erkennung zu ergreifen", betont Schlein. „Händler können sich nur durch eine umfassende Risikoprüfung schützen, indem sie interne und externe Daten mit intelligenten Modellen kombinieren. Ein gezielter Einsatz von Machine-Learning-Technologien und manuellen Kontrollverfahren bietet dabei den effektivsten Schutz gegen Betrüger."

Tipps für Händler und Verbraucher

Sowohl Händler als auch Verbraucher können durch Aufmerksamkeit und gezielte Maßnahmen Betrugsversuche frühzeitig erkennen und vermeiden. Händler sollten besonders wachsam gegenüber auffälligen Bestellmustern sein. Dazu zählen ungewöhnlich hohe Bestellwerte, die von Betrügern oft bevorzugt werden, sowie wiederkehrende E-Mail-Domains, die in bestimmten Regionen gehäuft auftreten. Durch das frühzeitige Erkennen solcher Muster und eine konsequente Überprüfung verdächtiger Transaktionen können sie potenzielle Schäden minimieren.

die sie nicht getätigt haben. „Solche Anzeichen können auf den Missbrauch persönlicher Daten oder Identitäten hinweisen“, meint Schlein.

Künstliche Intelligenz ist dabei Chance und Risiko zugleich
KI spielt eine zentrale Rolle in der Betrugsprävention. Mit datenbasierten Machine-Learning-Modellen arbeitet CRIF daran, betrügerische Netzwerke und Identitätsverschleierungen zu identifizieren.

Doch KI kann auch missbraucht werden: So erleichtert sie die Erstellung täuschend echter Fakeshops oder manipulierter Produktbewertungen.

CRIF setzt auf flexible Plattformen und eine exzellente Datengrundlage. Durch die Anpassungsfähigkeit der KI-Modelle und den Einsatz bewährter Tools ist das Unternehmen in der Lage, betrugsverdächtige Anfragen mit hoher Genauigkeit zu erkennen und an neue Betrugsmuster anzupassen.
Dabei spielen auch ML-Modelle (Machine Learning) eine zentrale Rolle. Diese Modelle nutzen komplexe Entscheidungslogiken, um betrügerische Anfragen noch präziser zu identifizieren und von legitimen Bestellungen zu unterscheiden. Ihre Fähigkeit, Muster in großen Datenmengen zu erkennen und kontinuierlich aus neuen Informationen zu lernen, ermöglicht eine effektivere, trennschärfere Vorhersage von Betrugsversuchen.

Nächste Seite

CRIF GmbH Victor-Gollancz-Straße 5 76137 Karlsruhe Tel : 040 89803-0 Fax : 040 89803-777 E-Mail : info.de@crif.com
www.crif.de