

Die Audit-Checkliste für Betrugsprävention ohne Reibungsverluste

Schützen Ihre Sicherheitskontrollen den Umsatz oder stoppen sie Ihre Kundschaft?

Es ist schon schwer genug, Benutzer:innen in Ihren Online-Shop zu bringen. Wenn Sie legitime Käufer:innen beim Checkout durch aufdringliche CAPTCHAs, fälschliche Ablehnungen und unerwartete Anmeldehürden blockieren, ist das schmerzhaft und teuer.

Die meisten Führungsteams verfolgen Chargeback-Kosten genau, aber nur wenige messen die unbemerkten Umsatzverluste durch fälschliche Ablehnungen und Sicherheitsbarrieren, die die Konversion erschweren.

Verwenden Sie diese Checkliste, um Ihr aktuelles Setup für Betrugs- und Identitätsschutz zu überprüfen. Damit erkennen Sie, wo starre Sicherheitsbarrieren den Verkaufsprozess behindern und wo einfache, moderne Threat Intelligence Betrugsversuche unbemerkt im Hintergrund blockieren kann.

Anleitung: Kreuzen Sie jedes Kästchen an, das Ihrem aktuellen Setup entspricht. Wenn Sie sich nicht sicher sind oder wissen, dass Sie eine statische, pauschale Regel verwenden, betrachten Sie diesen Punkt als offene Lücke.

1. Bot-Abwehr und Perimetersicherheit

- ☐ Filtern Sie automatisierten Bot-Traffic und Credential-Stuffing-Skripte am Perimeter heraus, bevor diese Ihre Login-Box oder Ihre APIs erreichen?
- ☐ Können echte Kund:innen den Kaufvorgang abschließen, ohne durch störende CAPTCHAs unterbrochen zu werden?
- ☐ Nutzen Sie Edge-Rate-Limiting und IP-Reputationsfilterung, um Brute-Force-Angriffe automatisch zu stoppen?
- ☐ Ist Ihr Anti-Bot-Schutz intelligent genug, um schädliche Skripte zu blockieren, ohne legitime menschliche Käufer:innen bei stark nachgefragten Verkaufsaktionen auszubremsen?

2. Sicherheit von Anmeldedaten und Schutz vor Kontoübernahmen

- ☐ Gleichen Sie übermittelte Passwörter in Echtzeit automatisch mit Datenbanken für kompromittierte Anmeldedaten ab, um kompromittierte Logins zu blockieren?
- ☐ Bieten Sie biometrische Passkeys (Touch ID, Face ID, Windows Hello) an, um Passwort-Schwachstellen vollständig zu beseitigen?
- ☐ Können Benutzer:innen kompromittierte Accounts sicher zurücksetzen, ohne beim Checkout auf langsame, umständliche E-Mail-Reset-Schleifen warten zu müssen?
- ☐ Verwenden Sie kryptografische Hash-Abfragen (z. B. k-Anonymity), damit vertrauliche Benutzeranmeldedaten bei Prüfungen auf Sicherheitsverletzungen niemals offengelegt werden?

3. Hintergrund-Risikotelemetrie

- ☐ Wertet Ihr System Hintergrundsignale (z. B. Geräte-Fingerprinting, Browser-Status und IP-Reputation) in weniger als 50 Millisekunden aus?
- ☐ Können Sie nicht plausible Ortsveränderungen erkennen, z. B. eine Anmeldung in Chicago, auf die wenige Minuten später eine API-Anfrage aus Frankfurt folgt?
- ☐ Durchlaufen mehr als 90 % Ihrer legitimen, risikoarmen Benutzer:innen Login und Checkout ohne jegliche Sicherheitsabfragen?
- ☐ Werden Session-Token unbemerkt im Hintergrund ausgestellt, sobald das kontextabhängige Risiko als gering eingestuft wird?

4. Adaptive Verifizierung und Step-up-Sicherheit

- ☐ Werden zusätzliche Sicherheitsprüfungen (z. B. die Multi-Faktor-Authentifizierung) ausschließlich dann ausgelöst, wenn der Risiko-Score einer Session tatsächlich stark ansteigt?
- ☐ Werden Wiederholungskäufe mit geringem Risiko auf bekannten Geräten zugelassen, ohne dass zusätzliche Verifizierungsschritte erzwungen werden?
- ☐ Behalten Sie die Step-up-Authentifizierung risikoreichen Aktionen vor, z. B. der Aktualisierung von Lieferadressen oder dem Einlösen wertvoller Treuepunkte?
- ☐ Bieten Sie nahtlose Optionen für Push-Benachrichtigungen oder biometrische Verifizierung an, anstatt sich ausschließlich auf verzögerte SMS-Einmalpasswörter zu verlassen?

5. Fälschliche Ablehnungen und Umsatzsteuerung

- ☐ Messen Ihre Führungs- und Risikoteams neben den herkömmlichen Betrugs-Chargeback-Kennzahlen aktiv die Raten fälschlicher Ablehnungen?
- ☐ Wird Ihre Rate fälschlicher Ablehnungen erfasst und bleibt sie unter dem Branchendurchschnitt von 1,5 %?
- ☐ Werden wiederkehrende, verifizierte Kund:innen aufgrund ihrer Identitätshistorie automatisch von aggressiven Prüfungen auf Zahlungsbetrug ausgenommen?
- ☐ Übermittelt Ihr Identity-System Echtzeit-Benutzerkontext und Risikotelemetrie direkt an nachgelagerte Zahlungs- und Betrugs-Engines?

6. Branchenspezifisches Reibungsmanagement

- ☐ **Einzelhandel und E-Commerce:** Können Käufer:innen mit hoher Kaufabsicht den Bezahlvorgang reibungslos abschließen, ohne zu obligatorischen Formularen zur Account-Erstellung oder wiederholten Verifizierungen gezwungen zu werden?
- ☐ **Streaming und Medien:** Können Benutzer:innen auf Smart-TVs und Mobilgeräten angemeldet bleiben, ohne häufige Aufforderungen zur erneuten Authentifizierung zu erhalten?
- ☐ **FinTech und iGaming:** Können Benutzer:innen sofortige Registrierungen oder Kleinbetragsüberweisungen abschließen, ohne durch eine aufwendige, vorgelagerte Verifizierung aufgehalten zu werden?
- ☐ **Reisen und Treuprogramme:** Sind Kundentreuepunkte, Geschenkkarten und VIP-Meilen vor Credential-Stuffing geschützt, ohne das tägliche Gästeerlebnis zu beeinträchtigen?

7. Bereitschaft für KI-Agenten und automatisierte Transaktionen

- ☐ Kann Ihre Sicherheitsarchitektur zwischen schädlichen Scraping-Bots und legitimen KI-Einkaufsassistenten von Kund:innen unterscheiden?
- ☐ Kann Ihr System für KI-Assistenten kurzlebige Token mit festgelegtem Berechtigungsbereich (per OAuth 2.0 Token Exchange) ausstellen, ohne Benutzeranmeldedaten preiszugeben?
- ☐ Setzen Sie feingranulare Ausgabenlimits und Aktionsgrenzen für automatisierte KI-Transaktionen durch?
- ☐ Können Kund:innen Berechtigungen, die sie persönlichen KI-Einkaufsassistenten gewährt haben, auf einfache Weise überprüfen und widerrufen?

So berechnen Sie Ihren Score

Zählen Sie Ihre angekreuzten Kästchen zusammen, um den Stand Ihres Kunden- und Sicherheits-Setups zu ermitteln:

24–28 Kästchen angekreuzt

Optimiert

Ihre Konfiguration blockiert Betrug unbemerkt im Hintergrund, während der Checkout für legitime Käufer:innen vollständig zugänglich bleibt.

16–23 Kästchen angekreuzt

Solide, aber mit Umsatz-verlusten

Ihre grundlegenden Schutzmaßnahmen funktionieren, aber statische Sicherheitshürden und fälschliche Ablehnungen kosten Sie wahrscheinlich Umsatz.

Weniger als 16 Kästchen angekreuzt

Hohes Conversion-Risiko

Veraltete Sicherheitskontrollen und pauschale Hürden treiben Käufer:innen zu Mitbewerbern und benachteiligen echte Kund:innen.

Sind Sie bereit, Reibungsverluste beim Checkout zu beseitigen, ohne das Risiko zu erhöhen?

Die Bewertung Ihrer Betrugskontrollen ist nur der Ausgangspunkt. Für die Behebung von fälschlichen Ablehnungen und Anmeldeabbrüchen müssen Sie weder Ihren kompletten Tech-Stack austauschen noch Kompromisse bei den Sicherheitsstandards eingehen. Wenn Sie kontextabhängige Risiken unbemerkt im Hintergrund bewerten, können Sie automatisierten Betrug in Echtzeit unterbinden, während der Checkout für echte Käufer:innen schnell und reibungslos bleibt.

Vereinbaren Sie eine 30-minütige Scoping-Session mit Auth0-Architekturfachleuten. Wir gehen gemeinsam die Ergebnisse dieser Checkliste durch, besprechen Ihr aktuelles Sicherheits-Setup und erstellen einen maßgeschneiderten Plan, mit dem Sie fälschliche Ablehnungen beseitigen und den Umsatz schützen können.