



KURZLEITFADEN · RISIKO · IDENTITÄTSBETRUG

Neuer Kunde, falsche Identität? Signale geprüft, bevor Sie zusagen.

Wer sich anmeldet oder einen Vertrag beantragt, behauptet zunächst, wer er ist. Dieser Kurzleitfaden zeigt, wie PaperOffice E-Mail-Adresse, IP-Adresse, Gerät und Ausweis als prüfbare Signale liefert. Für Shops, Plattformen, Vermieter und Händler mit Ratenkauf.

WAS SIE MITNEHMEN

Jede Prüfung liefert Felder, auf die Ihre Regel reagiert: eine Empfehlung zur E-Mail, Kennzeichen für VPN und Tor, eine Geräteerkennung und Ausweisfelder mit Fundstelle. Die Entscheidung trifft Ihr Team.

01 · DAS PROBLEM

Der Name stimmt. Die Person dahinter nicht.

Ein neuer Kunde schließt online einen Vertrag ab, das Smartphone geht per Ratenkauf raus. Name, Anschrift und E-Mail-Adresse wirken echt. Erst wenn die Raten ausbleiben, zeigt sich: Die Daten gehören einer anderen Person, oder es gibt sie gar nicht.

WARUM ES PASSIERT

Gestohlene und erfundene Daten

Betrüger nutzen echte Namen und Anschriften aus Datenlecks oder mischen sie mit erfundenen Angaben. Im Formular sieht beides gleich aus.

Tarnung im Netz

Wegwerf-Adressen, VPN, Tor und gemietete Server verbergen, wer bestellt. Dieselbe Person legt so mit wenig Aufwand viele Konten an.

Ausweise im Eiltempo

An der Theke wird die Ausweiskopie kurz angesehen und abgetippt. Ein Tippfehler oder ein fehlendes Feld fällt dabei leicht durch.

WORAN SIE ES MERKEN

- Die E-Mail-Adresse stammt von einem Wegwerf-Dienst, oder ihre Domain hat keinen Mailserver.
- Die Anmeldung kommt über VPN, Tor oder ein Rechenzentrum statt über einen normalen Anschluss.
- Das Land der IP-Adresse passt nicht zur angegebenen Anschrift.
- Dasselbe Gerät taucht bei mehreren Anmeldungen mit verschiedenen Namen auf.
- Angaben im Formular und auf dem Ausweis weichen voneinander ab.

02 · DER WEG MIT PAPEROFFICE

Vom Signal zur Entscheidung.

PaperOffice liefert Signale zu E-Mail, Netz, Gerät und Dokument, per REST-API, SDK und in der App. Was daraus folgt, legt Ihre Regel fest: durchlassen, nachfragen, prüfen lassen oder ablehnen.

1

E-Mail-Adresse bewerten

POST /fakeemail/check prüft Wegwerf-Domains, MX-Einträge, SPF und DMARC und liefert risk_score sowie die Empfehlung ACCEPT, REVIEW oder REJECT.

MODUL: [FAKE-E-MAIL-ERKENNUNG](#)

2

Netz und Standort prüfen

/ip2location/full liefert Land, Region und Provider, dazu is_vpn, is_proxy, is_tor und is_datacenter. Das Feld type nennt die Liste mit dem Treffer.

MODUL: [VPN-ERKENNUNG](#)

3

Gerät wiedererkennen

Das Browser-SDK liefert je Gerät eine visitor_id. /fingerprint/verify prüft beim nächsten Login, ob es dasselbe Gerät ist, risk.factors nennt Auffälligkeiten.

MODUL: [DEVICE FINGERPRINT](#)

4

Ausweis lesen

Ein IDP Agent liest Name, Geburtsdatum, Anschrift, Ausweisnummer und Gültigkeit aus Foto oder Scan, jeden Wert mit Fundstelle im Original.

MODUL: [IDP AGENT](#)

5

Entscheiden

Ihre Anwendung verbindet die Felder zu einer Regel, etwa: Wegwerf-Adresse oder Tor bedeutet Prüfung durch einen Menschen. Die Entscheidung trifft Ihr Team.

03 · IN DER APP

Schlüssel, SDK, Agent: so richten Sie es ein.

Die Signal-Prüfungen laufen über REST-API und SDK, der Ausweis über einen IDP Agent in der App. Die Bezeichnungen entsprechen der App.

1

API-Schlüssel für Ihr Backend

Unter **API & Entwickler** > **API-Keys** mit **Neuen Key erstellen** einen **API-Key** anlegen. Ihr Backend prüft damit E-Mail und IP. Kopieren können Sie den Schlüssel dort jederzeit.

2

Schlüssel für das Browser-SDK

Unter **API & Entwickler** > **API-Keys** mit **Neuen Key erstellen** den Typ **Veröffentlichter Schlüssel** wählen und die Domains Ihrer Website eintragen. Damit lädt Ihre Seite das Fingerprint-SDK.

3

IDP Agent für Ausweise anlegen

Ein Beispielfoto markieren, dann **Aktionen** > **Agents & Workflows** > **IDP** und **Neuen Agent erstellen**. Eine Vorlage für Ausweise wählen oder die Felder in eigenen Worten beschreiben.

4

Werte mit Fundstelle prüfen

Im Reiter **Datenfelder** steht jeder Wert neben dem Ausschnitt aus dem Ausweis. Die Ansicht **IDP Review** zeigt alle Dokumente mit offenen Feldern.

5

Prüfaufgaben abarbeiten

Fehlt ein Pflichtfeld, entsteht eine Aufgabe in der gewählten Prüfwarteschlange. Unter **Workflow AI** > **Human In The Loop Aufgaben** sieht eine Person Ausweis und Felder und schließt die Prüfung ab.

TIPP AUS DER PRAXIS

Mehrere Signale zusammen werten Ein VPN allein hat oft harmlose Gründe. Aussagekräftig wird es zusammen mit einer Wegwerf-Adresse oder einem Gerät, das in Ihrem System schon an anderen Konten hängt. Legen Sie fest, ab wann ein Mensch prüft.

04 · EIN BEISPIEL

Ein Handyhändler. Verträge mit Ratenkauf.



Ein Mobilfunkhändler mit sechs Filialen und einem Onlineshop verkauft Smartphones mit Vertrag und Ratenzahlung. Im Laden kopiert das Team den Ausweis und tippt die Daten ab, online genügt ein Formular. Immer wieder bleiben Raten aus, und die Kunden sind unerreichbar.

VORHER

- Im Laden wird der Ausweis kopiert und Feld für Feld ins Vertragsformular getippt.
- Online wird jede E-Mail-Adresse übernommen, auch von Wegwerf-Diensten.
- Anträge über VPN oder Rechenzentren sehen aus wie alle anderen.
- Dass ein Gerät schon mehrere Anträge gestellt hat, merkt niemand.

MIT PAPEROFFICE

- Das Onlineformular prüft die E-Mail-Adresse, bei REVIEW geht der Antrag in die Prüfung.
- Die IP-Prüfung meldet VPN, Tor und Rechenzentrum, die Anwendung vergleicht das Land mit der Anschrift.
- Jeder Antrag speichert die visitor_id, mehrfach genutzte Geräte fallen so auf.
- Im Laden liest ein IDP Agent den Ausweis vom Foto, das Team prüft die Werte mit Fundstelle.

Beispiel zur Veranschaulichung, Firma und Ablauf sind erfunden. Prüfen Sie mit Ihrem Datenschutz, welche Ausweis- und Gerätedaten Sie erheben und wie lange Sie sie speichern.

05 · CHECKLISTE

Zehn Punkte für Ihre Kundenaufnahme.

Gehen Sie die Punkte mit Vertrieb, IT und Datenschutz durch. Jeder Punkt lässt sich im eigenen Betrieb prüfen.

- | | |
|--|---|
| ☐ Jede Registrierung prüft die E-Mail-Adresse, bevor das Konto freigeschaltet wird. | ☐ Für REVIEW und REJECT ist festgelegt, was passiert: nachfragen, prüfen lassen oder ablehnen. |
| ☐ Ihr Backend sendet die IP-Adresse des Kunden im Parameter ip an die API. | ☐ VPN, Tor und Rechenzentrum sind einzeln bewertet, mit einer Regel für jeden Fall. |
| ☐ Das Land der IP-Adresse wird mit der angegebenen Anschrift verglichen. | ☐ Die visitor_id wird zu jedem Konto und jedem Antrag gespeichert. |
| ☐ Meldet sich ein bekanntes Konto von einem fremden Gerät an, fragt Ihre Anwendung einen zweiten Faktor ab. | ☐ Ausweise liest ein IDP Agent, die Pflichtfelder sind festgelegt. |
| ☐ Für Löschanfragen ist der Weg über POST /privacy/forget beschrieben. | ☐ Zweck, Rechtsgrundlage und Speicherdauer der Gerätedaten sind mit dem Datenschutz geklärt. |

06 · HÄUFIGE FRAGEN

Was Teams vor dem Start wissen wollen.

Prüft PaperOffice Ausweise biometrisch?

PaperOffice arbeitet ohne Gesichtsabgleich. Ein IDP Agent liest die Felder des Ausweises mit Fundstelle, die übrigen Prüfungen liefern Signale zu E-Mail, Netz und Gerät. Ob eine Identität bestätigt ist, entscheidet Ihr Team.

Was ist mit Menschen, die aus guten Gründen ein VPN nutzen?

Ein VPN ist ein Signal, das Ihre Regel gewichtet. Die Antwort trennt VPN, Proxy, Tor und Rechenzentrum und nennt im Feld type die Liste mit dem Treffer. Auch Adressen aus Sperrlisten erscheinen unter is_vpn.

Wie kommen die Prüfungen in unser Portal?

Über die REST-API aus Ihrem Backend, über das Fingerprint-SDK mit einem **Veröffentlichter Schlüssel**, der an Ihre Domains gebunden ist, und über MCP. Ausweise laden Sie in einen Workspace, in dem ein IDP Agent läuft.

Woher kommt der Risikowert?

Aus der E-Mail-Prüfung: risk_score von 0 bis 100, risk_level von MINIMAL bis CRITICAL und die Empfehlung ACCEPT, REVIEW oder REJECT. Die Geräteprüfung liefert eigene Risikofaktoren, etwa VPN oder eine unmögliche Reisegeschwindigkeit.

Erkenne ich dasselbe Gerät hinter mehreren Konten?

Ja, wenn Sie die visitor_id zu jedem Konto speichern. Dann steht dieselbe Kennung an mehreren Konten. /fingerprint/similar findet Geräte mit ähnlichen Merkmalen, /fingerprint/linked Geräte aus demselben Netz.

Wie gehe ich mit Löschanfragen um?

POST /privacy/forget löscht Geräteprofil, Verknüpfungen, Verlauf und Warnungen zu einer Kennung in Ihrer Organisation. Ein Sperrvermerk verhindert, dass dieselbe Kennung erneut erfasst wird.

07 · SO STARTEN SIE

Prüfen Sie die nächste Anmeldung mit echten Signalen.

Konto auf app.paperoffice.ai anlegen, unter **API & Entwickler > API-Keys** einen API-Schlüssel erstellen und die erste Adresse mit POST `/fakeemail/check` prüfen. Abgerechnet wird nach Verbrauch, Details stehen auf der Preisseite.

E-Mail-Prüfung einbauen

Ihr Anmeldeformular sendet die Adresse über Ihr Backend an `/fakeemail/check` und reagiert auf das Feld `recommendation`.

IP und Gerät dazunehmen

`/ip2location/full` für Netz und Standort, das Fingerprint-SDK für die `visitor_id`. Beides zum Antrag speichern.

Ausweise lesen lassen

Einen IDP Agent mit einer Ausweisvorlage anlegen und im Workspace für Anträge nach der Verarbeitung automatisch laufen lassen.

DATENBLÄTTER ZUM THEMA

Fake-E-Mail-Erkennungpaperoffice.ai/downloads/paperoffice-ai-datenblatt-api-fake-mail.pdf**VPN-Erkennung**paperoffice.ai/downloads/paperoffice-ai-datenblatt-api-vpn.pdf**IP-Standort-API**paperoffice.ai/downloads/paperoffice-ai-datenblatt-api-ip-standort.pdf**Device Fingerprint**paperoffice.ai/downloads/paperoffice-ai-datenblatt-api-fingerprint.pdf**IDP Agent**paperoffice.ai/downloads/paperoffice-ai-datenblatt-idp-agent.pdf

MEHR ZUM THEMA

Identitätsbetrugpaperoffice.ai/de/loesungen/risiko/ki-identitaetsbetrug-erkennung-praevention

MEHR ZUM THEMA

paperoffice.ai/de/loesungen/risiko/ki-identitaetsbetrug-erkennung-praevention

PREISE

paperoffice.ai/de/preise

KONTAKT

paperoffice.ai/de/kontakt