DE RICHTLINIE ZUM SCHUTZ VON KUNDENDATEN

230 Route des Dolines, 06560 VALBONNE
Tel : +33(0)9 72 10 05 90 - E-Mail : solutions@my-travelplanet.com
www.my-travelplanet.com

TRAVEL PLANET France SAS mit einem Kapital von 3.000.000 €
SIRET 384 221 925 00116 - APE 7911Z - IM62100003

1.Governance der Datensicherheit
1.1 Ein engagierter Ansatz für die Sicherheit von Kundendaten
Travel Planet verpflichtet sich, alle notwendigen Maßnahmen zum Schutz der Kundendaten zu ergreifen.
Im Streben nach Spitzenleistungen in der Cybersicherheit arbeitet Travel Planet mit einem spezialisierten Dienstleister zusammen, der 2017 folgende Aufgaben durchgeführt hat:
Sicherheitsprüfung des Informationssystems (Arbeitsumgebung der Mitarbeiter, Infrastruktur des Rechenzentrums, Anwendungsarchitektur)
Umsetzung von Compliance-Maßnahmen
Schulung der Entwicklungsleiter in sicheren Programmierpraktiken

1.1.1 Einhaltung der DSGVO
Die Einhaltung der Datenschutz-Grundverordnung (DSGVO) wurde mit ihrem Inkrafttreten formalisiert.

1.2 Risikobasiertes Sicherheitsmanagement
Um einen effektiven und fundierten Sicherheitsansatz sicherzustellen, führt Travel Planet regelmäßig Sicherheitsprüfungen seines Informationssystems durch.
Darüber hinaus werden Investitionsentscheidungen im Bereich Sicherheit auf Grundlage einer Risikoanalyse getroffen, die sich an den spezifischen Merkmalen der Geschäftstätigkeit von Travel Planet orientiert. Diese Risikoanalyse wird alle zwei Jahre überprüft.
Überblick über das risikobasierte Management:
Kartierung der digitalen Vermögenswerte
• IT-Systeme, in denen Daten gespeichert sind oder durch die sie übertragen werden
Bewertung potenzieller Bedrohungen
• Externe und internetbasierte Bedrohungen
• Bewertung verfügbarer Ressourcen
Risikoanalyse
• Steuerung von Sicherheitsinvestitionen zur Bewältigung der bedeutendsten Risiken
• Systematische Priorisierung der Sicherheit von Kundendaten

1.3 Richtlinien für Travel Planet Mitarbeiter:
1.3.1 Beschränkungen des Datenzugriffs
Jeder Mitarbeiter von Travel Planet hat innerhalb des Unternehmens eine oder mehrere Rollen. Je nach Rolle hat ein Mitarbeiter nur Zugriff auf die Informationen, die zur Ausübung seiner Aufgaben erforderlich sind. Darüber hinaus werden die Mitarbeiter auf die Bedeutung hingewiesen, nicht auf interne oder externe Anfragen zur Offenlegung von Kundendaten zu reagieren.
1.3.2 Sicherung von Konten und Zugang zum Informationssystem
Der Zugang zum Informationssystem von Travel Planet wird namentlich einzelnen Personen zugewiesen, um die Nachverfolgbarkeit des Zugriffs zu gewährleisten. Mitarbeiterkonten werden deaktiviert, wenn ein Mitarbeiter das Unternehmen verlässt oder seine Rolle wechselt.
Es werden keine Kundendaten auf den Arbeitsplätzen der Mitarbeiter gespeichert; diese dienen ausschließlich als Zugangspunkte zu den Webanwendungen des Informationssystems.
Die Sicherheit privilegierter Konten (Administratoren) wird durch eine Zwei-Faktor-Authentifizierung verstärkt.
1.3.3 Mitarbeiterschulungen
Die Travel Planet Academy ist ein internes Schulungsprogramm, das neuen Mitarbeitern eine auf ihre Tätigkeit zugeschnittene Ausbildung bietet. Im Rahmen dieses Programms wird eine Schulung zu bewährten Praktiken im Bereich Datenschutz sowie zur Sensibilisierung für Cyberhygiene durchgeführt.
Zudem führen wir regelmäßig interne Kommunikationskampagnen zu Datenschutz- und Cyberhygiene-Themen durch.
Speicherung und Nutzung personenbezogener Daten
2.1 Speicherung personenbezogener Kundendaten
Travel Planet verwendet Kundendaten weder direkt noch indirekt für andere Zwecke als die Erfüllung seiner Rolle als Travel Management Company (TMC). Wir kaufen oder verkaufen keine Kundendaten.
2.1.1 Gespeicherte Daten
Travel Planet speichert nur die für die Vertragsausführung mit dem Kunden erforderlichen Daten. Im Hinblick auf personenbezogene Daten handelt es sich hauptsächlich um Identitätsinformationen, die für die Organisation von Reisen notwendig sind. Zahlungsinformationen werden nicht gespeichert.
2.1.2 Ausdrucke
Reisepläne werden vollständig im digitalen Format verarbeitet. Es werden keine Ausdrucke erstellt.

Nur die Bearbeitung außergewöhnlicher Anfragen kann gelegentlich die Erstellung einer Papierakte erforderlich machen. In solchen Fällen werden die Akten in verschlossenen Schränken an einem der gesicherten Standorte von Travel Planet aufbewahrt, wobei der Zugang durch ein Badgesystem beschränkt ist.

Außerdem werden Papierdokumente vor der Entsorgung als Recyclingabfall vernichtet.

2.1.3 Cybersicherheitsgrundsätze im Zusammenhang mit der digitalen Speicherung personenbezogener Daten

Um die Sicherheit personenbezogener Daten innerhalb des Informationssystems von Travel Planet zu gewährleisten, haben wir die in diesem Abschnitt beschriebenen Architekturprinzipien implementiert.

2.1.3.1 Persönlicher Datentresor

Alle personenbezogenen Daten unserer Kunden werden in einem digitalen persönlichen Datentresor gespeichert.

Dabei handelt es sich um eine sichere Datenbank, die personenbezogene Daten enthält. Als personenbezogene Daten gelten alle Informationen, die eine Identifizierung eines Kunden erleichtern, wie Identitätsdaten (Vorname, Nachname usw.) oder Kontaktdaten (Telefonnummer, Postanschrift usw.). Der Zugriff auf diesen Tresor ist streng begrenzt, und die Daten werden auf Anwendungsebene verschlüsselt gespeichert (eine SQL-Abfrage an die Datenbank liefert verschlüsselte Informationen zurück).

Standardmäßig speichern und verarbeiten unsere Anwendungen anonymisierte Daten, die mit einer technischen Kennung verknüpft sind. Nur Prozesse, die den Zugriff auf personenbezogene Daten erfordern, können diese gelegentlich über die korrelierende technische ID aus dem Tresor abrufen.

2.1.3.2 Sicherheit unserer Webanwendungsentwicklung

Alle Transaktionen mit dem Webclient erfolgen innerhalb einer zeitlich begrenzten Anwendungssitzung. Die Sitzung wird mit einem standardmäßigen, selbst generierten Cookie verwaltet. Dadurch wird bei allen Client-Server-Transaktionen die Sitzungskennung übermittelt.

Um Hackingversuche auf unseren Webclient zu verhindern, führen wir systematisch Zugriffskontrollen auf alle serverseitigen APIs mit einem sicheren Token durch.

Jede anormale Situation (Timeout, mehrere gleichzeitige Verbindungen usw.) während einer Sitzung führt zur Beendigung der Sitzung, sodass sich der Benutzer erneut verbinden muss, um normale Bedingungen wiederherzustellen. Darüber hinaus behalten wir uns das Recht vor, ein Benutzerkonto, das anormales Verhalten zeigt und auf einen möglichen Kompromiss hinweist, vorübergehend zu deaktivieren.

2.2 Verarbeitung personenbezogener Daten

Wir führen keine Verarbeitung von Kundendaten durch, die über das zur Erbringung unserer Dienstleistung unbedingt erforderliche Maß hinausgeht. Es erfolgt keine Datenanreicherung oder sonstige Nutzung personenbezogener Daten.

3.1.2 Erweitertes Filtersystem

Wir verwenden eine Filtertechnologie, die für jede Maschine individuell angewendet wird. Das bedeutet, dass selbst zwei Maschinen (virtuell oder physisch) innerhalb derselben Netzwerkzone standardmäßig nicht miteinander kommunizieren können.

Für jede Maschine definieren wir spezialisierte Filterregeln basierend auf ihrer Rolle. Es ist nur der Netzwerkverkehr erlaubt, der für das ordnungsgemäße Funktionieren des Informationssystems erforderlich ist. Die Implementierung dieser Technologie erzwingt eine strenge Disziplin im Management unseres Netzwerkverkehrs.

3.2 Betriebliches Wartungs- und Sicherheitsberichtswesen

3.2.1 Verwaltung von Obsoleszenz und Patches

Die Entwicklungs- und IT-Betriebsteams arbeiten zusammen, um die betriebliche und sicherheitstechnische Integrität des Informationssystems aufrechtzuerhalten. Dieser Prozess basiert insbesondere auf dem Berichtswesen zur Verwaltung von Obsoleszenz (einschließlich Patch-Management) für Systemkomponenten (Infrastruktur, Betriebssysteme, Middleware und Anwendungslibraries).

3.2.2 Zugriff auf Verwaltungskonsolen

Auf die Produktionsumgebung kann ausschließlich über Verwaltungskonsolen zugegriffen werden. Um deren Sicherheit zu maximieren, sind diese Konsolen flüchtig: Sie werden erstellt, wenn ein Betreiber eine Wartungsaufgabe durchführen muss, und nach Abschluss der Aufgabe wieder gelöscht. Dadurch existiert unter normalen Bedingungen kein dauerhafter Zugriff auf die „Administrationsschnittstellen“ der Produktionsmaschinen.

3.3 Erkennung von Eindringversuchen

Wir haben eine Protokollierungsrichtlinie implementiert, um die Aktivitäten auf unserem Informationssystem zu überwachen. Dadurch können sowohl Leistungsdaten (Antwortzeiten usw.) als auch Sicherheitsdaten (Zugriffsprotokolle usw.) gesammelt werden. Diese Protokolle werden mithilfe eines Business-Intelligence-Tools ausgewertet.

Einige dieser Prozesse sind darauf ausgelegt, anormales Verhalten zu erkennen, das auf Eindringversuche oder Datenexfiltration hinweisen könnte.

Wenn ein anormales Verhalten festgestellt wird...