# Étude de cas : La brèche des données de British Airways (2018)

La brèche des données de **British Airways** en 2018 est l'une des violations de données les plus importantes en matière de cybersécurité, impliquant l'exposition d'informations personnelles et financières de centaines de milliers de clients. Cette attaque a mis en évidence des lacunes importantes dans la gestion des données, la sécurité des systèmes, et a entraîné des conséquences juridiques et financières importantes pour la compagnie aérienne.

## Contexte de l'incident

En septembre 2018, British Airways a révélé que son site web et son application mobile avaient été compromis par des attaquants. Cette brèche de sécurité a conduit à l'exfiltration de données personnelles et financières appartenant à environ **380 000 clients**, incluant des noms, des adresses, des informations de carte de crédit, et des informations de voyage.

- **Période de la brèche** : L'attaque a duré du **21 août 2018 au 5 septembre 2018**.
- **Nature des données compromises** : Les attaquants ont accédé aux informations personnelles, y compris les noms, adresses de facturation, adresses email, ainsi que les détails complets des cartes bancaires (numéros de carte, dates d'expiration, codes CVV).

## Mode opératoire de l'attaque

L'attaque a été attribuée à un groupe de cybercriminels utilisant la technique de **Magecart**, une méthode d'**injection de code malveillant** dans des sites e-commerce pour collecter en temps réel les informations de paiement des utilisateurs.

#### Injection de script malveillant sur le site web :

- Les attaquants ont exploité une vulnérabilité sur le site web de British Airways, leur permettant d'injecter un **script JavaScript malveillant** dans les pages de paiement du site et de l'application mobile.
- Ce script capturait les données saisies par les utilisateurs lorsqu'ils remplissaient les formulaires de réservation et de paiement, et les envoyait à un serveur contrôlé par les attaquants. Les données étaient volées à la volée, c'est-à-dire au moment même où elles étaient entrées par les utilisateurs.

#### Redirection vers des serveurs malveillants :

- Le script malveillant était hébergé sur un serveur tiers, créé pour ressembler à un domaine de confiance. En réalité, il redirigeait les données collectées vers les cybercriminels.
- Le script malveillant utilisé par les attaquants ne modifiait pas l'apparence du site web ou de l'application mobile, rendant l'attaque indétectable pour les utilisateurs.

#### Absence de détection rapide :

- Le système de détection de British Airways n'a pas identifié rapidement l'activité malveillante. L'attaque s'est poursuivie pendant plus de deux semaines avant que la compagnie ne la découvre et ne la stoppe.

## Conséquences pour British Airways

La brèche de données a eu des conséquences importantes à la fois pour les clients et pour British Airways, tant sur le plan financier que sur le plan de la réputation de l'entreprise.

#### Impact financier

- **Amende record** : En vertu du **Règlement Général sur la Protection des Données (RGPD)**, l'Information Commissioner's Office (ICO) du Royaume-Uni a infligé à British Airways une amende de **183 millions de livres sterling** (environ 204 millions d'euros) en juillet 2019. Cette amende a été plus tard réduite à **20 millions de livres sterling** en raison de la pandémie de COVID-19, mais elle reste l'une des amendes les plus importantes infligées sous le RGPD.

#### Impact sur la réputation

- **Perte de confiance des clients** : La brèche a gravement affecté la confiance des clients dans la capacité de British Airways à protéger leurs informations. Les clients lésés ont exprimé leur frustration face au manque de transparence initial et à la gestion de la crise par la compagnie.
- **Répercussions à long terme** : L'atteinte à la réputation de British Airways a également entraîné une perte de clients potentiels et a affecté ses relations commerciales, notamment avec les partenaires financiers tels que les banques et les processeurs de paiement.

#### Recours légaux et poursuites

- **Actions en justice** : En plus de l'amende infligée par l'ICO, British Airways a dû faire face à plusieurs poursuites en justice intentées par des clients et des groupes de consommateurs pour manquement à la protection des données.
- **Dédommagement des clients** : British Airways a été contraint de dédommager les clients affectés par la fuite de leurs données personnelles et financières.

## Failles de sécurité identifiées

L'incident de British Airways a révélé plusieurs faiblesses dans la gestion de la sécurité des systèmes informatiques de la compagnie :

#### 1. Absence de surveillance proactive et de détection

- Le système de surveillance de British Airways n'a pas détecté l'injection du script malveillant. Une surveillance proactive plus robuste des scripts tiers et une analyse des logs auraient pu alerter l'équipe de sécurité de l'anomalie bien plus tôt.

#### 2. Mauvaise gestion des scripts tiers

- Les attaquants ont pu injecter un script malveillant dans le site web de British Airways en exploitant des vulnérabilités dans les bibliothèques JavaScript tierces. Il semble que la gestion des scripts tiers n'ait pas été rigoureusement contrôlée ou mise à jour.

#### 3. Manque de chiffrement complet

- Les données sensibles saisies par les utilisateurs (numéros de carte de crédit, CVV, etc.) n'étaient pas correctement protégées contre l'exfiltration. Même si les données étaient transférées de manière sécurisée via HTTPS, l'injection de script a permis de capturer ces données avant qu'elles ne soient chiffrées et envoyées au serveur.

#### 4. Absence d'audit régulier de la sécurité

- Un audit de sécurité régulier aurait pu identifier les failles dans la gestion des bibliothèques JavaScript et la vulnérabilité exploitée. L'absence d'un tel audit a permis à cette attaque de passer inaperçue pendant des semaines.

### Leçons à tirer et bonnes pratiques à adopter

L'attaque de British Airways a mis en lumière l'importance de la protection des données et la vigilance nécessaire pour sécuriser les applications web et les systèmes informatiques. Voici les principales leçons à en tirer et les bonnes pratiques que les entreprises devraient adopter :

#### 1. Surveillance continue des scripts et des applications

- **Supervision des scripts tiers** : Toute entreprise utilisant des scripts ou des bibliothèques JavaScript tiers devrait surveiller activement ces scripts pour détecter toute modification non autorisée. Des outils comme les **Content Security Policy (CSP)** peuvent être utilisés pour empêcher le chargement de scripts malveillants.

#### 2. Audit de sécurité régulier

- **Évaluation des vulnérabilités** : Effectuer des audits de sécurité réguliers pour identifier et corriger les vulnérabilités, en particulier dans les composants tiers (comme les bibliothèques JavaScript). Des outils de gestion des dépendances et des scanners de vulnérabilités peuvent identifier les failles connues dans les bibliothèques utilisées.

#### 3. Chiffrement de bout en bout des données

- **Protection des données en temps réel** : Les informations sensibles comme les données de paiement doivent être chiffrées dès leur saisie dans les formulaires, avant même leur envoi vers le serveur, pour éviter les attaques qui interceptent les données avant qu'elles ne soient chiffrées.

#### 4. Détection des anomalies en temps réel

- **Analyse des comportements anormaux** : Mettre en place des systèmes de détection d'anomalies basés sur le machine learning ou d'autres techniques qui peuvent identifier des comportements suspects dans les interactions des utilisateurs avec le site web (par exemple, des scripts inconnus ou des requêtes inhabituelles).

#### 5. Respect du RGPD et des réglementations

- **Conformité avec les réglementations** : La brèche de British Airways montre l'importance de respecter les réglementations comme le RGPD, qui impose des règles strictes sur la protection des

données personnelles et la gestion des brèches de sécurité.

---