Un mystérieux expert trouve une faille aux CFF

Cyberincident

Un million de données ont fuité. C'est un spécialiste externe qui a découvert la brèche. Il faut un audit indépendant, clament les experts.

Les CFF l'ont annoncé ce lundi: un spécialiste externe est parvenu à accéder à la plateforme de vente de billets pour les transports publics pour télécharger des données, lesquelles ont ensuite été effacées «de manière irréversible». C'est grave docteur? «La fuite a été colmatée, indiquent les CFF et Alliance SwissPass. Les clients n'ont subi aucun dommage.»

Mais de quelles données parle-t-on au juste? Le transporteur se veut rassurant. D'abord, ce million de données correspond à 0,2% de tous les enregistrements. Il s'agissait d'informations sur les billets achetés et/ou la durée de validité des abonnements. Environ la moitié des données étaient exclusivement liées aux noms, prénoms et dates de naissance des clients. Et rien d'autre? L'ex-régie fédérale dit que non: aucune information n'a été fournie sur le lieu de résidence, les moyens de paiement, les mots de passe et les adresses courriels.

Un gentil hacker?

Pour expliquer le couac, il faut remonter à la fin de l'année 2020 quand les CFF ont modifié la sécurité du processus de renouvellement des abonnements via cette plateforme. Fin 2021, on est revenu à l'ancien mécanisme. Et cela a créé une brèche. Qui a décelé la fuite? Un spécialiste informatique externe serait parvenu à siphonner les données en quelques jours au mois de janvier, répondent en chœur les CFF et Alliance SwissPass. Cet homme a-t-il été mandaté ou s'agit-il d'un gentil hacker bien intentionné? Les CFF ne donnent pas de détail. De son côté, Stéphane Koch, vice-président d'ImmuniWeb et spécialiste des questions numériques, livre son analyse à chaud: «Ce que cette personne a fait, c'est une divulgation responsable. Il a contacté l'entreprise plutôt que de le faire publiquement, dans une démarche éthique.»

«Il est courant, dans le monde de la cybersécurité, appuie Solange Ghernaouti, experte en la matière et professeure à l'Université de Lausanne, que des acteurs qui découvrent des failles et des vulnérabilités les rapportent aux propriétaires des systèmes, sur une base volontaire, parfois gratuitement. Par analogie, c'est le cas de quelqu'un qui trouve un portefeuille avec de l'argent et les coordonnées de son propriétaire et lui restitue le tout, sans contrepartie.» Stéphane Koch évoque l'importance de mettre en place des programmes où, selon un cadre précis, on rend le hacking légal. «C'est une couche de sécurité supplémentaire qui permettra à des personnes de chercher et de trouver les failles, moyennant des récompenses pouvant se monter à plusieurs milliers de francs.»

Une analyse nécessaire

«Dans le cas d'espèce, note Stéphane Koch, rien ne dit qu'une personne autre que celle qui a averti les CFF n'ait pas accédé à ces données. Et rien ne nous dit, dans le cas présent, que d'autres périmètres n'aient pas pu être atteints.» Solange Ghernaouti développe: «De l'extérieur, il est toujours difficile de pouvoir estimer l'ampleur des problèmes dont la connaissance dépend pour l'essentiel de la stratégie de communication de l'organisation victime.» Et pourquoi? «Selon sa stratégie de défense de ses intérêts et de sa réputation, celle-ci peut souhaiter minimiser les effets d'un cyberincident, notamment pour ne pas inquiéter ses partenaires et ses clients.» D'où la nécessité d'un audit à mener rapidement. «Pour l'heure, une faille a été annoncée, résume Stéphane Koch. Elle doit être analysée de près pour savoir si d'autres données sont sorties. La question est primordiale. On ne peut pas se contenter de la seule communication des CFF, car on n'est sûr de rien. Lorsqu'ils parlent de 0,2% du total des informations, c'est une manière de minimiser et de rassurer. Si cette faille est récente, il faudra un peu de temps. Par ailleurs, à mon sens, les CFF devraient aussi informer les personnes concernées.»

À noter que les CFF ont contacté le préposé fédéral à la protection des données et à la transparence ainsi que les entreprises publiques concernées. Une enquête interne a aussi été ouverte.

Sébastien Jubin