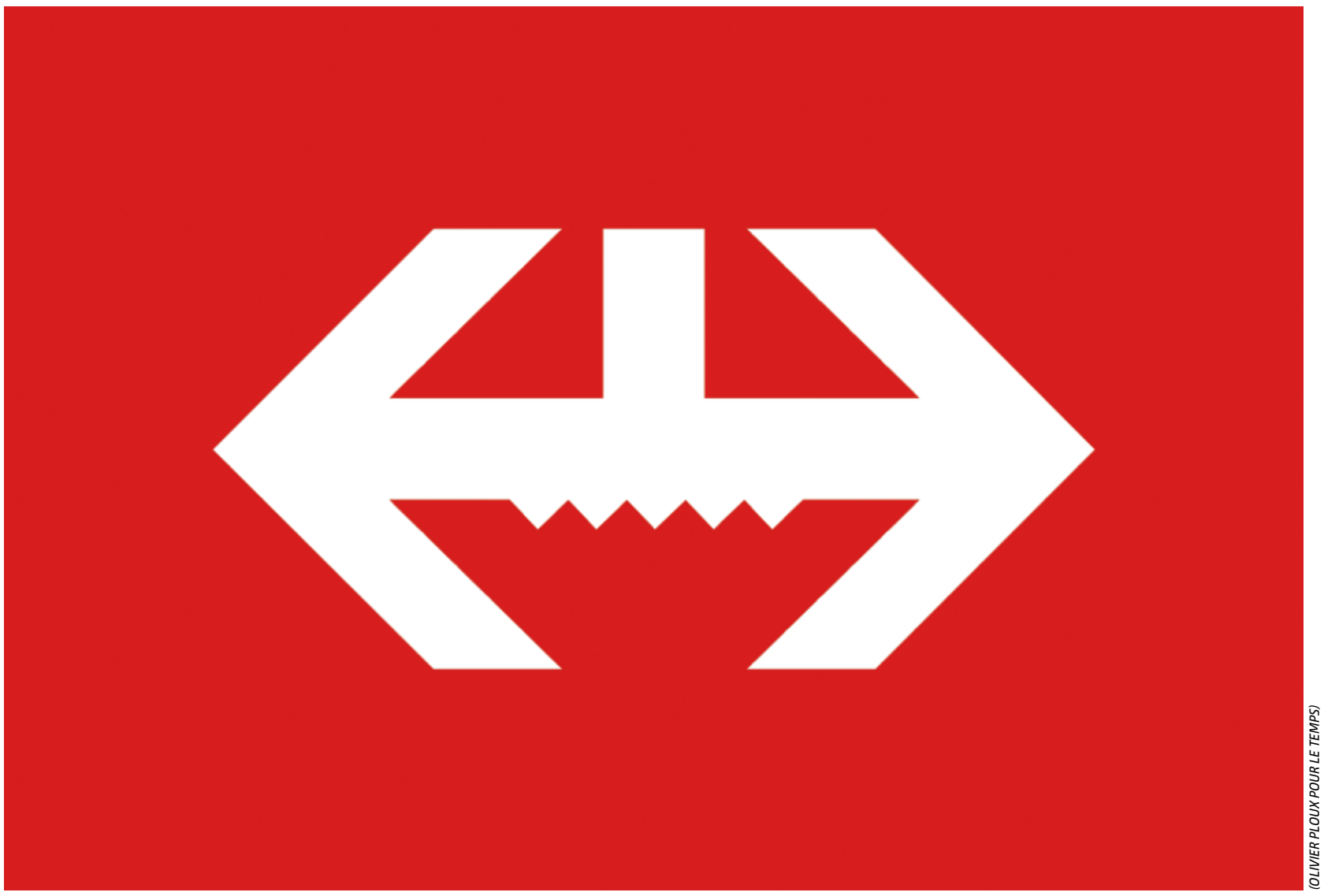
Aux CFF, la faille qui sème le doute

TECHNOLOGIE Un million de blocs de données, comprenant des noms et des informations de déplacements, étaient accessibles en ligne. L'ex-régie fédérale affirme que ses clients ne subiront aucun préjudice. Mais des experts ne sont pas aussi affirmatifs

ANOUCH SEYDTAGHIA
@Anouch



(OLIVIER PLOUX POUR LE TEMPS)

Des prénoms, des noms, des itinéraires... Au total, un million d'informations détenues par les CFF sur leurs clients se sont retrouvées, durant plusieurs jours, en quasi libre accès. Lundi, l'ex-régie fédérale a reconnu un gros souci de sécurité dans sa base de données. Alertée par un spécialiste en sécurité, l'entreprise affirme avoir immédiatement colmaté les brèches. «La clientèle n'a subi aucun préjudice», selon les CFF. Mais cette interprétation des faits est disputée par des experts, qui estiment que les CFF sont sans doute trop optimistes, trop tôt.

Ce ne sont donc pas eux qui ont constaté cette faille, mais une personne externe. En janvier, durant plusieurs jours, cette dernière a pu consulter en ligne les déplacements de centaines de milliers de voyageurs. Selon l'entreprise, un million de blocs de données, soit 0,2% du total, étaient accessibles. Parmi eux se trouvaient des informations sur les billets, sur les abonnements, ainsi que les noms, prénoms et dates de naissance des clients. Les CFF assurent qu'aucune information n'était disponible sur le lieu de résidence de ses clients, les moyens de paiement, les mots de passe ou les adresses e-mails.

«Décision malheureuse»

Comment ces données ont-elles pu être si facilement disponibles? Les CFF invoquent une erreur technique. Ils exploitent la plateforme informatique Nova, sur mandat de l'Alliance SwissPass. Ce sont donc eux qui gèrent cette centrale mettant en relation plus de 250 entreprises de transports suisses. A la fin de 2020, les CFF ont mis à jour Nova, mais comme cela a créé un bug pour des utilisateurs qui ne pouvaient plus renouveler leur abonnement, ils ont rétabli l'accès avec l'ancien mécanisme en décembre 2021. «Cette décision s'est révélée malheureuse: elle a créé une faille de sécurité», reconnaît l'entreprise.

L'affaire suscite de nombreuses questions. D'abord, qui est cette personne externe, lanceuse d'alerte? «Il s'agit d'un expert en informatique suisse indépendant. Il a immédiatement contacté les CFF après avoir constaté pouvoir télécharger ces données», répond un porte-parole, qui affirme que personne d'autre n'a pu accéder à ces données. Cet homme a parlé, sous le couvert de l'anonymat, à la radiotélévision alémanique (SRF). Selon lui, «il n'était même pas nécessaire d'avoir des connaissances particulières. N'importe qui aurait pu le faire. Les données sensibles étaient pratiquement publiques sur le réseau.» L'homme affirme par ailleurs ne pas être un criminel: «Je veux sensibiliser à la protection des données», dit-il.

La version donnée par les CFF ne convainc pas totalement François Charlet, juriste spécialisé dans les nouvelles technologies. «Si une personne externe – dont on ne sait pas si elle a été mandatée par les CFF dans le but d'auditer le système Nova – a pu consulter ces informations, il est probable que d'autres aient pu le faire également. Si la faille a été annoncée et que les CFF ont pris des mesures ensuite, cela peut indiquer qu'ils n'ont pas remarqué un trafic de données inhabituel et donc qu'ils n'auraient probablement pas remarqué un trafic de données effectué par d'autres personnes, malveillantes cette fois-ci.»

Selon le spécialiste, «cette bourde est grave: on a préféré faire un *downgrade* (avec les conséquences qu'on connaît) vers une version moins sécurisée plutôt que de régler le problème sur la version actuelle de la plateforme qui était justement censée améliorer la sécurité, et ce depuis fin 2020». Selon François Charlet, «la faille a donc été exploitable pendant des semaines entre décembre 2021 et janvier 2022, et rien ne nous empêche de penser qu'elle n'était pas présente avant janvier 2022, voire avant la mise à jour de 2020.»

> **«Affirmer que la clientèle n'a subi aucun préjudice est très présomptueux. Comment une entreprise victime d'une fuite de données peut-elle évaluer (à l'avance) si ses clients ont subi un dommage?»**
>
> FRANÇOIS CHARLET, JURISTE SPÉCIALISÉ DANS LES NOUVELLES TECHNOLOGIES

David Billard, professeur associé à la Haute Ecole de gestion de Genève (HES GE) et spécialisé en cybersécurité, est un peu moins sévère. Selon lui, «plus qu'une bourde, c'est plutôt une mauvaise décision de gestion au cours de laquelle la pesée des risques a été mal appréhendée. J'imagine que le service client a remonté les plaintes des clients et quelqu'un, entre l'Alliance SwissPass et les CFF, a décidé de revenir en arrière en remettant l'ancien système de renouvellement d'abonnements en fonction.» Le spécialiste poursuit: «Cependant, comme tout système informatique, il est probable que l'ancien système n'ait pas été mis à jour au niveau de sa sécurité, [puisque désactivé depuis quelques mois]. Revenir en arrière est toujours délicat.»

Se pose aussi la question de l'attitude des CFF, qui assurent qu'il n'arrivera rien à leurs clients. «Affirmer que la clientèle n'a subi aucun préjudice est très présomptueux, réagit François Charlet. Comment une entreprise victime d'une fuite de données peut-elle évaluer (à l'avance) si ses clients ont subi un dommage en raison de celle-ci? On n'en sait rien et on ne le saura pas avant qu'un client affirme avoir subi un tel dommage et parvienne à démontrer la causalité entre son dommage et la fuite de données.»

Sur ce point, David Billard est partagé. Selon lui, l'attitude des CFF est correcte «si le problème est très circonscrit, car on connaît exactement la faille et exactement les données mises en accès «libre») et si les CFF peuvent avoir la certitude qu'aucune autre personne que le spécialiste externe n'y a eu accès.» Par contre, poursuit David Billard, les CFF s'avancent peut-être un peu trop «car des données clients ont bien été accessibles, et lues (au moins par le spécialiste externe) pendant un temps indéterminé, en tout cas entre le moment de la bascule vers l'ancien système et la correction de la faille». De plus, note le professeur, «le fait que des données d'abonnements et des données de distributeurs automatiques soient mêlées (alors qu'il s'agit de deux processus distincts) m'incite à être plus prudent que les CFF».

Lundi, sur Twitter, un client des CFF leur demandait: «Avez-vous prévu de mettre à disposition un outil permettant de vérifier si nos données font partie (ou non) de celles qui ont été dérobées?» Réponse des CFF, toujours sur Twitter: «Actuellement, nous n'avons pas encore d'information. Désolé de ne pas pouvoir vous répondre précisément.» ▬

Toutes ces informations sur les clients sont-elles vraiment nécessaires?

PROTECTION DES DONNÉES **La faille de sécurité interroge la nécessité de recueillir les informations personnelles des usagers au-delà de ce qui est nécessaire**

PROPOS RECUEILLIS PAR MARC GUÉNIAT

La charge est sévère. «Vous pouvez transformer une entreprise de transport en une société de traitement de données. Mais lorsqu'il y a un problème, vous restez une entreprise de transport», note Alexis Roussel, co-auteur de *Notre si précieuse intégrité numérique* (Ed. Slatkine). Selon lui, une telle fuite de données personnelles avait toutes les chances de survenir un jour ou l'autre aux CFF.

«Cela fait des années que les CFF prennent de haut les problèmes de protection des données», tranche Sébastien Fanti, préposé valaisan à la protection des données. Il cite notamment la géolocalisation de l'application mobile, permettant d'acquérir billets et abonnements. Prenant connaissance de la communication de la régie publique, qu'il décrit comme une «pirouette optimiste», il redoute qu'elle instaure, à force, «une culture du désarroi» chez les usagers, spectateurs impuissants d'un schéma qui se répète – Swisscom a vécu une fuite analogue. Dans les deux cas, aucun vilain hacker ne peut être pointé du doigt.

Vulnérabilité numérique

De fait, le communiqué des CFF n'exclut pas que les photos d'individus aient été accessibles sur le web, ni les données relatives aux resquilleurs, des informations hautement sensibles puisqu'elles concernent des procédures pénales. Sollicités, les CFF indiquent que la base de données des resquilleurs est gérée par

ALEXIS ROUSSEL
CO-AUTEUR DU LIVRE «NOTRE SI PRÉCIEUSE INTÉGRITÉ NUMÉRIQUE»

SÉBASTIEN FANTI
PRÉPOSÉ VALAISAN À LA PROTECTION DES DONNÉES

CarPostal, sans que l'on sache si cela doit rassurer.

On peut d'ailleurs se demander pourquoi les CFF compilent toutes ces données que l'usager captif doit concéder, sauf à payer son billet au prix fort au distributeur. Car il est pratiquement impossible de se prémunir contre cette vulnérabilité numérique, ni de s'affranchir de l'offre des CFF.

A l'origine, les CFF avaient opéré ce virage stratégique dans la récolte de données, contenues dans le SwissPass, afin de gérer les abonnements, offrir des services personnalisés et analyser les comportements pour améliorer l'offre de transport. «A cette époque, la technologie disponible justifiait cette collecte massive. Mais aujourd'hui, des solutions permettent de s'en passer, soutient Alexis Roussel. D'après lui, les CFF n'ont pas besoin du nom des personnes transportées pour administrer les flux. L'expert relève ainsi que les transports publics lausannois parviennent très bien à calculer les mouvements de passagers sans recueillir leurs identités. «Les CFF vont devoir suivre cette route rapidement» estime Alexis Roussel.

Par le biais d'un porte-parole, les CFF indiquent qu'il est légitime de conserver les données liées aux abonnements, parce que ceux-ci constituent des titres de transport nominatifs. Il faut donc s'assurer qu'ils ne soient pas transmis à des tierces personnes. C'est la seule réponse que l'on peut obtenir pour l'instant aux questions posées par cette «fuite de données sur la plateforme de vente des transports». Le directeur général des CFF, Vincent Ducrot, n'était pas disponible lundi pour discuter des orientations stratégiques de l'entreprise et notamment de la possibilité de s'affranchir de la récolte des données personnelles des usagers. ▬