# « Credential stuffing » : la CNIL sanctionne un responsable de traitement et son sous-traitant

27 janvier 2021

La formation restreinte de la CNIL a récemment sanctionné de 150 000 euros et 75 000 euros un responsable de traitement et son sous-traitant pour ne pas avoir pris de mesures satisfaisantes pour faire face à des attaques par bourrage d'identifiants (credential stuffing) sur le site web du responsable de traitement.

Entre juin 2018 et janvier 2020, la CNIL a reçu plusieurs dizaines de notifications de violations de données personnelles en lien avec un site internet à partir duquel plusieurs millions de clients effectuent régulièrement des achats. La CNIL a décidé de mener des contrôles auprès du responsable du traitement et de son sous-traitant, a qui était confié la gestion de ce site web.

Au cours de ses investigations, la CNIL a constaté que le site web en cause avait subi de nombreuses vagues d'attaques de type *credential stuffing*. Dans ce type d'attaque, une personne malveillante récupère des listes d'identifiants et de mots de passe « en clair » publiées sur Internet, généralement à la suite d'une violation de données. Partant du principe que les utilisateurs se servent souvent du même mot de passe et du même identifiant (l'adresse courriel) pour différents services, l'attaquant va, grâce à des « robots », tenter un grand nombre de connexions sur des sites. Lorsque l'authentification réussit, cela lui permet de prendre connaissance des informations associées aux comptes en question.

La CNIL a constaté que des attaquants ont ainsi pu prendre connaissance des informations suivantes : nom, prénom, adresse courriel et date de naissance des clients, mais également numéro et solde de leur carte de fidélité et des informations liées à leurs commandes.

# Des mesures de sécurité insuffisantes

La formation restreinte — organe de la CNIL chargé de prononcer les sanctions — a considéré que les deux sociétés avaient manqué à leur obligation de préserver la sécurité des données personnelles des clients, prévue par l'article 32 du RGPD.

En effet, les sociétés ont tardé à mettre en place des mesures permettant de lutter efficacement contre ces attaques répétées. Elles avaient décidé de concentrer leur stratégie de réponse sur le développement d'un outil permettant de détecter et de bloquer les attaques lancées à partir de robots. Toutefois, le développement de cet outil a pris un an à compter des premières attaques.

Or, dans l'intervalle, plusieurs autres mesures produisant des effets plus rapides auraient pu être envisagées afin d'empêcher de nouvelles attaques ou d'en atténuer les conséquences négatives pour les personnes, telles que :

- la limitation du nombre de requêtes autorisées par adresse IP sur le site web, qui aurait pu permettre de freiner le rythme auquel les attaques étaient menées ;
- l'apparition d'un CAPTCHA dès la première tentative d'authentification des utilisateurs à leur compte, très difficile à contourner pour un robot.

Du fait de ce manque de diligence, les données d'environ 40 000 clients du site web ont été rendues accessibles à des tiers non autorisés entre mars 2018 et février 2019.

# Les sanctions prononcées par la formation restreinte

Par conséquent, la formation restreinte a prononcé deux amendes distinctes – 150 000 euros à l'encontre du responsable de traitement et 75 000 euros à l'encontre du sous-traitant – au regard de leur responsabilité respective. En effet, elle a souligné que le responsable de traitement doit décider de la mise en place de mesures et donner des instructions documentées à son sous-traitant. Mais le sous-traitant doit aussi rechercher les solutions techniques et organisationnelles les plus appropriées pour assurer la sécurité des données personnelles, et les proposer au responsable de traitement.

La formation restreinte n'a pas décidé de rendre publiques ces délibérations. Néanmoins, elle souhaite communiquer sur ces décisions pour alerter les professionnels sur la nécessité de renforcer leur vigilance concernant les attaques par *credential stuffing*, et de développer, en lien avec leur sous-traitant, des mesures suffisantes pour garantir la protection des données personnelles.

Texte reference

# Articles en relation

> La violation du trimestre : attaque par credential stuffing sur un site web
> Sécurité des données
> Guide de la sécurité des données personnelles

> Les violations de données personnelles
> Les étapes de la procédure de sanction
Texte reference

# Textes de référence

> Article 32 du RGPD