Sécurité : la CNIL vote un carton jaune au Parti Socialiste

Informée en mai dernier par le blogueur Damien Bancal d'une faille permettant d'accéder aux données personnelles de plusieurs dizaines de milliers d'adhérents au Parti Socialiste, la CNIL adresse un avertissement public au parti politique. « *Cette faille avait été rendue possible par l'utilisation d'une technique non sécurisée d'authentification à la plateforme* », explique la Commission dans son avertissement. Selon Damien Bancal, qui anime le blog Zataz, ce sont les liens personnalisés envoyés aux candidats à l'adhésion qui donnaient accès aux données confidentielles stockées par le site Web. La CNIL précise que les noms, prénoms, e-mails, numéros de téléphone fixe et mobile, dates de naissance, adresses IP, moyens de paiement ainsi que les montants des cotisations ont ainsi été exposés. Plus amusant encore, toujours via la même faille, les enquêteurs de la CNIL ont eu accès aux login et mots de passe des utilisateurs légitimes de la plate-forme de gestion des adhésions. Et même à la fonction permettant d'ajouter un nouvel utilisateur.

Si cette vulnérabilité a été corrigée dès que la CNIL a fait les gros yeux au parti politique, rappelons que Damien Bancal s'était échiné pendant plusieurs semaines à tenter d'alerter l'organisation. En vain. De guerre lasse, il avait soumis le dossier à la CNIL qui a su rapidement se faire entendre, après vérification de la réalité de la faille.

Une modification mal maîtrisée

Et la Commission ne s'est pas arrêtée là, puisqu'elle a mené le 15 juin dernier un second contrôle, dans les locaux du PS cette fois, afin de comprendre l'origine de cette boulette et d'évaluer le niveau de sécurité de l'organisation. Le DSI de cette dernière a informé la CNIL que les données librement accessibles provenaient d'une plate-forme de suivi des paiements des primo-adhérents arrivant via le site du Parti Socialiste. Une application qui vient ensuite injecter les inscriptions validées dans la base de données nationale des adhérents, Rosam.

Premier problème relevé par la CNIL : les données de la plate-forme gérant les adhésions en ligne ne sont associées à aucune durée de conservation. Des informations remontant à 2010 y figurent encore. Un sujet de fâcherie récurrent pour la Commission nationale de l'informatique et des libertés. Plus troublant, selon le DSI du PS, l'URL litigieuse « *a été obtenue par l'injection d'un script Javascript dans un formulaire d'adhésion* », écrit la CNIL dans sa délibération. Le PS assure que ce défaut résulte en fait d'une modification mal maîtrisée de l'application du suivi des paiements des primo-adhérents, le 12 mai 2016.

Une authentification époque SFIO

Selon le DSI, ce type d'injection de code – permettant tout de même de modifier les listes d'adhérents ! – n'est aujourd'hui plus possible. Le PS a également renouvelé son système d'authentification : un token à durée de vie limitée remplaçant le secret passé en paramètre de l'URL.

Ce qui n'empêche pas la CNIL de critiquer vertement la façon dont le PS protégeait auparavant, la confidentialité de ses nouveaux adhérents. La Commission relève que la méthode dite « GET », intégrant le secret d'authentification de l'utilisateur dans l'URL, est dépassée. Surtout quand ledit secret intégré à l'URL est transformé avec l'algorithme de hachage MD5 sans sel (ce dernier amenant un facteur aléatoire supplémentaire). « *Pour empêcher toute attaque dite par 'force brute', une fonction de hachage doit non seulement être réputée forte mais également faire intervenir un aléa dans son calcul* », rappelle la CNIL, qui critique aussi l'absence de traçabilité des connexions à la plate-forme. Or, remarquons que, sans cette *« précaution d'usage essentielle* », le PS a beau jeu d'affirmer aujourd'hui que la faille n'a jamais été exploitée de façon malveillante…

Début juin, après la correction de la vulnérabilité et de premiers éléments dévoilés par Zataz, *Silicon.f*r avait demandé des explications au PS sur l'origine du dysfonctionnement. La rue de Solférino nous promettait alors une mise en relation avec un interlocuteur au fait des questions de sécurité. La rédaction attend toujours…

A lire aussi :

La Cnil tance Cdiscount pour manquements « graves » à la sécurité des données

La Cnil épingle Windows 10 sur la collecte des données

Crédit photo : Maksim Kabakou / Shutterstock