LastPass •••|

Étude de cas : Crunchr

crunchr

**« Pour nous, LastPass offre une hygiène de base.
C'est comme prendre sa douche quotidienne.
Il s'assure que quoi que l'on fasse, on est propre et sécurisé. »**

Jan Joris *Vereijken*, Directeur technique

Le défi

Basé à Amsterdam, Crunchr aide des organisations du monde entier à recueillir des renseignements utiles sur le fonctionnement du personnel. La société aide les entreprises à créer un environnement de travail sain en fournissant des données qui permettent aux conseillers en personnel, aux ressources humaines et à la direction d'anticiper les tendances et de limiter la rotation des collaborateurs. Jan Joris *Vereijken*, le directeur technique de Crunchr, a rejoint l'organisation il y a cinq ans, mais son impact sur l'infrastructure de la société l'a précédé. Lorsque Dirk Jonker, un ami de *M. Vereijken* et fondateur de Crunchr, envisageait de monter sa propre entreprise, *M. Vereijken* lui a conseillé d'investir immédiatement dans un gestionnaire de mots de passe. *M. Vereijken* a mesuré l'importance d'un gestionnaire de mots de passe lorsque son compte Twitter personnel a été piraté en 2012 en raison d'un mot de passe réutilisé. Il a alors pris conscience à la fois des risques liés à la réutilisation des identifiants de connexion, et de la difficulté de créer des mots de passe sûrs.

M. Vereijken ajoute : *« J'ai compris qu'il me fallait des mots de passe différents pour chaque site, puisqu'il s'agissait de la raison principale du piratage de mes comptes Twitter. »* Lorsqu'il était à la recherche d'un outil adapté pour ses besoins personnels, un ami lui a conseillé LastPass.

Conscient des risques associés à une mauvaise hygiène des mots de passe, *M. Vereijken* a conseillé à M. Jonker d'investir dans LastPass afin de minimiser les risques de piratage de données chez Crunchr, ou que des informations essentielles soient exposées ou dérobées dès le lancement de son activité.

La solution

En 2014, Crunchr a investi dans LastPass. Lorsque son équipe s'est étoffée, la société a continué à ajouter des licences pour conserver une infrastructure sécurisée.

Le générateur de mots de passe de LastPass est particulièrement prisé par l'équipe, puisqu'il permet aux employés de Crunchr de créer des mots de passe aléatoires robustes. Les administrateurs peuvent imposer l'utilisation de mots de passe comportant au moins 12 caractères et contenant des chiffres, des lettres et des caractères spéciaux. *M. Vereijken* remarque : *« J'ai appris qu'il est vital d'avoir un mot de passe unique pour chaque compte, et c'est devenu la règle pour tous les employés de l'entreprise. »* En créant des mots de passe uniques pour chaque application, les employés peuvent rester vigilants face aux tentatives d'hameçonnage et limiter les dégâts potentiels.

La capacité de LastPass à être utilisé sur plusieurs appareils a été un autre facteur clé pour *Vereijken*. L'équipe de Crunchr fonctionne dans un format hybride, 60 % de l'organisation travaillant à distance. De plus, l'organisation utilise une gamme variée de technologies au sein de l'entreprise et souhaitait une solution accessible aussi bien sur Apple iOS que sur Microsoft Windows. *M. Vereijken* ajoute : *« La possibilité d'y accéder sur différents systèmes d'exploitation était importante pour moi. Je voulais que le déploiement soit simple pour l'équipe, et que les coffres-forts de mots de passe soient*
accessibles à tout moment et de partout. LastPass est accessible sur différentes plates-formes sans sacrifier l'expérience utilisateur, ce qui en fait le choix idéal pour nous. »

« Ce n'est pas un sujet de débat chez nous. Observer une bonne hygiène des mots de passe avec LastPass est tout simplement une obligation pour tous. »

Le résultat

Depuis l'investissement de Crunchr, LastPass est devenu incontournable pour ses employés. En exploitant une trentaine de règles, pour imposer une longueur minimale du mot de passe maître, empêcher la réutilisation des mots de passe ou encore imposer l'authentification multifacteur, Crunchr a pu s'assurer que l'équipe prenait des mesures conséquentes pour améliorer son hygiène des mots de passe. Avec actuellement un seul mot de passe maître faible dans toute l'organisation, il est clair que LastPass a eu un impact positif sur le comportement des membres de l'équipe. Leur score de sécurité moyen atteint 86 %, avec une fiabilité moyenne des mots de passe de 85 %. *M. Vereijken* ajoute : *« Mon score de sécurité personnel atteint 94 %, mais certains membres de mon équipe m'ont dépassé ! »*

Crunchr utilise plus de 60 solutions différentes basées dans le cloud, dont HubSpot, Bitbucket et Google Workspace. Dans le cadre de la rationalisation de ses processus, la société espère intégrer l'authentification unique pour simplifier les accès. Les employés utilisent le partage de mots de passe via LastPass au quotidien pour collaborer en toute sécurité. Grâce aux dossiers partagés de LastPass, les administrateurs peuvent gérer les comptes et s'assurer que les employés qui quittent l'entreprise ne conservent pas leurs accès. *M. Vereijken* remarque : *« Le service financier a récemment connu un départ, et la première chose que j'ai faite a été de changer les identifiants. Si l'équipe suit nos consignes et accède aux mots de passe via les dossiers partagés, elle n'aura même pas réalisé qu'une modification a eu lieu. »*

« J'ai accumulé plus de mille comptes dans mon coffre-fort LastPass, et je peux affirmer fièrement qu'ils ont chacun leurs propres identifiants. »

Découvrez comment Crunchr a renforcé sa sécurité des mots de passe avec LastPass.

Nous contacter