

Un employé pirate sa société pour gonfler ses heures de travail

L'histoire se déroule aux Etats-Unis et plus exactement en Californie. [Un juge vient de condamner un ex-employé à verser plus de 300 000 dollars](#) de dommages à son ancien employeur. Le motif ? Le piratage du réseau et du logiciel RH de cette entreprise afin de gonfler les heures de travail et être rémunéré en conséquence.

Les faits se déroulent en 2014 et concernent la société Security Specialists, proposant des services de patrouilles de surveillance dans le sud de la Californie. Son patron, Nick Tsotsikyan, a créé une base de données sur FileMaker Pro pour gérer son personnel et les différentes missions. Cet outil est mis à disposition des patrouilleurs sur un PC, afin qu'ils y rapportent leur action quotidienne. Ces rapports sont ensuite transmis aux clients et une copie est conservée dans la base de données. Cette dernière n'est accessible qu'à Nick Tsotsikyan et Steve Leon, directeur des opérations.

Une falsification des heures pour déjeuner

Or le responsable opérationnel a remarqué en juillet 2014 des détails anormaux sur la feuille de paie d'un salarié, Yovan Garcia. Sur une période de 2 semaines de travail, le nombre d'heures effectuées, qui était normalement de 8 heures par jour, était passé à 12 heures, soit 40 heures supplémentaires sur la période. Steve Leon a cru d'abord à un bug du programme avant de s'apercevoir que le champ « déjeuner » du rapport de Yovan Garcia avait été falsifié avec un ajout de 4 heures chaque jour, correspondant aux 40 heures indues. Dans son enquête, il a constaté un accès non autorisé, mais avec des identifiants et mots de passe légitimes à la base de données de la paie. In fine, Steve Leon a découvert que ce gonflement des heures existait depuis janvier 2014.

Le salarié a tenté de se dédouaner en expliquant avoir un jour été appelé par un ami travaillant pour une société concurrente. Cet ami détenait un portable en panne. Ayant quelques bases informatiques, Mr Garcia est tombé sur un fichier nommé Security Specialists. Il en a fait une copie sur son PC. Son ami au courant lui a demandé de ne rien dire et c'est à ce moment-là que les salaires de Yovan Garcia ont grimpé artificiellement.

L'affaire aurait pu en rester là, mais à l'occasion d'un conflit sur une réaffectation non souhaitée par le salarié, il a été licencié, à la fin septembre. Il s'en est ému auprès d'un collègue en lui envoyant des images de fichiers confidentiels de personnes de la société, dont ceux de Steve Leon. Celui-ci a indiqué à la cours que personne ne pouvait avoir accès à ces informations à moins d'avoir un identifiant et un mot de passe réservés aux administrateurs.

Un piratage des données et un défaçage du site web

En parallèle de cet évènement, en octobre 2014, le site et les serveurs de Security Specialists ont été piratés. Dans le viseur, les pirates souhaitaient obtenir les archives mails, des fichiers serveurs, l'accès au logiciel de comptabilité, les bases de données, les factures, les données RH, etc. A noter

que les cybercriminels avaient commencé à effacer les sauvegardes de la société et formater les différents lecteurs de l'entreprise. Heureusement, cette intrusion a été découverte et les serveurs déconnectés d'Internet. Toujours au début octobre, le site de Security Specialists a été défacé avec un message « êtes-vous prêts ? » avec la date du 1^{er} décembre 2014 ainsi que 5 chiffres correspondant au début du numéro de sécurité sociale de Steve Leon.

Le responsable informatique de Security Specialists a remonté la trace du pirate signant theAnonygroup@gmail.com. Une requête a été faite à Google qui a répondu en donnant une adresse IP liée à ce mail. Après une recherche, cette adresse correspond au quartier où habite Yovan Garcia. Le suspect a eu beau contesté, le tribunal n'a pas jugé crédible sa défense. En conséquence, il le considère comme le pirate du site web et celui qui s'est introduit dans le réseau pour gonfler ses heures de travail et donc sa paye. Et la facture est particulièrement salée, 318 661 dollars.

A lire aussi :

[Par crainte d'être licencié, un devops pirate son employeur](#)

[Quand un DSI laisse des backdoors pour pirater son ancien employeur](#)

Crédit Photo : Security Specialists