Un sysadmin plastique la base Oracle de son ex-employeur

Il y a quelques semaines, nous relations une affaire impliquant un responsable IT qui avait placé une backdoor dans le réseau de son ancien employeur pour pirater des données commerciales importantes. Aujourd'hui, c'est une autre affaire impliquant un administrateur qui fait la une. Ce dernier est accusé d'avoir placé une « bombe à retardement » dans la base de données de son ancienne entreprise.

Des PC portables de l'entreprise non rendus

La personne incriminée se nomme Nimesh Patel, de Shrewsbury, dans le Massachusetts. Il a travaillé de 2002 au 8 janvier 2016 chez Allegro MicroSystems. Au sein du fabricant de semi-conducteurs hautes performances, il était en charge de la base de données et plus précisément d'un module financier Oracle. Au cours de sa vie de salarié, Nimesh Patel a reçu 3 ordinateurs de son employeur, 2 pour le travail et un troisième plus ancien pour un usage personnel.

Quand il a démissionné d'Allegro, l'administrateur aurait renvoyé un seul des deux portables professionnels. Allegro a, en conséquence, convoqué son ex-employé pour lui demander de retourner le second portable, capable d'accéder au réseau de la firme. Mais, au lieu de se conformer à la demande, Patel aurait renvoyé l'ancien ordinateur portable à usage personnel, après en avoir nettoyé le disque dur.

Intrusion et bombe à retardement

Avec le PC portable restant, Nimesh Patel se serait rendu le 31 janvier 2016 au siège d'Allegro, à Worcester dans le Massachusetts, pour être à portée du réseau WiFi de l'entreprise. Il aurait alors réussi à s'y connecter avec les droits d'un autre salarié. Droits obtenus en tant qu'administrateur système, fonction grâce à laquelle il avait conservé une copie des identifiants. Une fois entré dans le réseau de l'entreprise, il aurait téléchargé une « *bombe à retardement* » dans le module financier de la base de données Oracle. Ce code était conçu pour être activé le 1er avril 2016, soit la 1ère semaine du nouvel exercice fiscal de la société.

Après l'explosion de cette bombe logique, les équipes IT d'Allegro affirment avoir découvert le pot aux roses le 14 avril 2016. Après enquête, ces équipes ont pu identifier le code malveillant après avoir comparé la base de données à une copie. Elles auraient alors remonté la trace de l'accès non autorisé au réseau et déniché l'empreinte du PC portable gardé par Nimesh Patel. Allegro a déposé plainte contre son ancien employé. La firme considère qu'il s'agit d'un sabotage intentionnel : « *il savait que le sabotage du module financier lors de 1ère semaine du nouvel exercice fiscal allait faire un maximum de dégâts, car cela nous empêchait de consolider l'exercice précédent et les reports sur le nouvel exercice* ».

Allegro réclame des dommages et intérêts, ainsi qu'une condamnation pour l'intrusion illégale sur

son réseau. La firme explique, dans sa requête, qu'elle a déboursé 100 000 dollars pour réparer sa base de données après l'exaction présumée de son ex-employé.

A lire aussi :

Quand un DSI laisse des backdoors pour pirater son ancien employeur

Fournir les données de son smartphone pour entrer aux Etats-Unis : sérieusement ?