Retour d'expérience

SYSTÈME D'INFORMATION PRIS EN OTAGE PAR LE PRESTATAIRE INFORMATIQUE

D'UNE ENTREPRISE DE 35 SALARIÉS

SPÉCIALISÉE DANS LE NETTOYAGE INDUSTRIEL

Contexte

Suite au décès brutal du dirigeant, le Système d'information a fait l'objet d'une immobilisation complète par le prestataire en place. Prétextant qu'il avait des « engagements » de l'ancien dirigeant en matière de primes exceptionnelles (ce que pas mal d'anciens fournisseurs réclamaient eux-aussi), il menaçait de bloquer le serveur et la messagerie tant qu'il n'aura pas été payé de ces primes (montants très élevés pour la société et hors cadre standard).

Ayant mis ses menaces à exécution, la société perd le contact avec ses clients (relations très étroites par email, dont tous les mots de passe ont été changé et une double authentification activée, avec une adresse de messagerie principale changée) et n'a plus aucune visibilité sur son activité commerciale (le serveur a été arrêté).

La réponse apportée par Mederi Consulting

A notre arrivée, nous constatons que le serveur ne démarre plus (clef de cryptage activée et ordre de démarrage modifié) et que les comptes d'accès aux messageries (chez OVH) ont été usurpés. Le prestataire ayant déployé des solutions de prise en main à distance et ayant verrouillé également les accès aux routeurs, bornes wifi, caméras de surveillance, etc..

Une fois la clef de décryptage trouvée (pas assez malin pour ne pas la laisser affichée sur le dessous du serveur), nous avons décidé d'externaliser la totalité du SI en notre Datacenter, mettant en place un routeur (connexion IPSec oblige) et remasterisant les 8 postes de travail.

Nous avons également accompagné le client en la récupération des droits administrateur sur ses domaines (déclarés chez OVH) et in-fine sur ses comptes de messagerie.

Les résultats obtenus

Le serveur a été intégré au sein de notre Datacenter, autorisant uniquement, dans un 1er temps, les accès en provenance de la société par des connexions « bureau à distance ».

Les opérations de Forensic, ainsi que les révisions des droits, ont permis de reprendre complètement la main sur le Système d'Information, écartant toute intervention possible du prestataire informatique.

Un dépôt de plainte du client, adossée à une déclaration de notre part, lui a permis de demander des dommages et intérêts.

Cette virtualisation menée dans l'urgence a permis au client de reprendre sa production le lendemain (en tous cas pour les accès serveur) après notre intervention. L'accès à la messagerie a été beaucoup plus complexe, face à des interlocuteurs OVH qui ne voulaient rien savoir, il a fallu user d'astuce pour contourner leurs procédures et migrer les comptes email dans un nouveau NicHandle ;-)

Plus d'informations…

Site Internet : http://www.reseau-legio.fr

Contact : Christophe Moisan – cmoisan@reseau-legio.fr

LEGIO, un puissant réseau de 10 professionnels piloté par Christophe Moisan, chef de projets confirmé, tous spécialisés dans leur propre corps de métier et en interaction directe avec le système d'information des entreprises.

RASSEMBLER DES FORCES AUTOUR DES S.I. POUR VOUS ACCOMPAGNER DANS VOTRE TRANSFORMATION DIGITALE ET VOUS PROCURER UN AVANTAGE CONCURRENTIEL