Retour d'expérience

ARNAQUE AU PRÉSIDENT

D'UNE ENTREPRISE MULTI-SITE DE 65 SALARIÉS

SPÉCIALISÉE DANS LE FINANCEMENT

Contexte

Le prestataire informatique du client lui a adressé sa facture mensuelle de prestation de maintenance et 4 jours plus tard, malgré la confirmation de paiement par le client, le prestataire n'avait toujours pas les fonds disponibles.

Après avoir contrôlé les échanges d'emails, ils se son rendu-compte d'une modification de pièce jointe (la fameuse facture d'origine) et notamment des informations de Rib dans le document. L'email avait été envoyé de la part du Directeur Financier, ordonnant à son assistante de procéder au virement, ce qui a été fait (avec création d'un nouveau Rib, justifié par le hackeur par le fait qu'il avait changé de banque.

La réponse apportée par Mederi Consulting

La double authentification a été activée sur l'ensemble des emails.

Un audit de la plateforme AzureAD a été mené afin d'extraire toutes les données nécessaires et l'ensemble des journaux pour analyse et opérations de Forensic, qui ont démontré l'intervention d'une tierce personne en la mise en place de règles de transfert, par l'usurpation de l'identité de l'administrateur.

La mise à jour des comptes Office a eu lieu, la procédure de paiement a été revue.

Le pare-feu a été audité et de nouvelles règles ont été mises en place pour limiter les actions sortantes possibles par les utilisateurs.

Les équipes techniques de Microsoft ont été mobilisées afin de mettre en évidence la méthode employée pour permettre l'envoie d'email depuis la plateforme Office365 (sachant que le Directeur financier utilisait déjà le MFA) et les actions correctrices ont été appliquées (notamment le DKIM et D-MARC)

Les résultats obtenus

L'ensemble des comptes email a été sécurisé par la double authentification, l'environnement Office365 a été assainie (moins de comptes déclarés et tous les droits ont été révisés).
La solution Never Be Hacked (solution de formation continue tout au long de l'année, disponible en mode SaaS) est en cours d'étude pour sensibiliser les utilisateurs notamment aux méthodes de fishing employées par les hackeurs.

Le client a pu réutiliser pleinement Office365 4 heures après la cyber-attaque.

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