Retour d'expérience

CHIFFREMENT COMPLET D'UN SYSTÈME D'INFORMATION

D'UNE ENTREPRISE SEMI-PRIVEE DE 50 SALARIÉS

SPÉCIALISÉE DANS LA GESTION DE PARKINGS

Contexte

Le Système d'information a fait l'objet d'une cyber-attaque par la diffusion et l'exécution du ransomware « BabyK ». Le dimanche matin, l'attaquant a pris la main sur un des serveurs en ayant usurpé l'identité du compte Administrateur et a lancé l'exécution du ransomware puis s'est chargé de supprimer tous les clichés Windows serveur et toutes les sauvegardes qui étaient centralisées sur un NAS Synology. La télésauvegarde ayant aussi été identifiée par l'attaquant, il s'est assuré d'avoir également supprimé les jeux distants chez OVH. Le lundi matin, plus aucun serveur n'est accessible, le responsable informatique constate les dégâts et demande à son prestataire d'intervenir pour remédier au plus vite.

Les 3 serveurs physiques étant partiellement ou totalement cryptés avec l'ensemble des jeux de sauvegarde corrompus, le prestataire propose au client de tout réinstaller car, selon lui, plus rien n'est récupérable.

Le responsable informatique déclenche alors une demande d'assistance sur cybermalveillance.gouv.fr afin de faire appel à un expert en récupération de données.

La réponse apportée par Mederi Consulting

Au regard des 1ère actions qui ont été menées par le prestataire historique, les serveurs sont tous déconnectés du réseau, l'ensemble des disques durs (Raid 5) des 3 serveurs sont clonés et séquestrés. Des récupérations de données par les logiciel Ontrack et Recoveo sont effectuées sur les disques clonés et sur les disques durs des NAS (certains en Raid1 et d'autres en Raid5).

Sans aucune documentation, Mederi Consulting assiste le responsable informatique en l'identification des procédures de sauvegarde des bases de données Cegid et des fichiers bureautiques (Word et Excel).

Des preuves devant être conservées, il a fallu envisager de reconstruire un Système d'Information à l'identique, raison pour laquelle de nouveaux disques ont été approvisionnés pour une réinstallation « from scratch ».

Une méthodologie de remédiation a été proposée, ainsi qu'un planning de tâches à exécuter pour envisager une reprise en mode dégradé dans les meilleurs délais et une équipe a été constituée pour ressaisir les éléments de comptabilité dans l'application Cegid redémarrée en urgence sur le Cloud.

Les résultats obtenus

Aucune donnée des jeux de sauvegarde n'a pu être récupérée car le NAS principal de sauvegarde a été totalement réinstallé par le prestataire historique (nous n'avons pas eu connaissance des raisons de cette action effectuée en priorité, sachant qu'elle a définitivement privé le client d'une possibilité de récupération de données, ce qui l'aurait sauvé). Par ailleurs:

- Les données d'un des NAS ont été récupérées, permettant de disposer de nouveau de l'ensemble des fichiers bureautiques (datant de 4 mois)
- Les fichiers de base de données SqlServer pour CEGID ont été récupérés par le logiciel Recoveo et la comptabilité a pu être redémarrée
- Le Système d'Information a été reconstruit dans un environnement virtuel
- Une sauvegarde professionnelle a été déployée, intégrant son isolation complète pour éviter d'être attaquée à l'avenir

Le client a pu reprendre sa production 2 semaines 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