Retour d'expérience

CHIFFREMENT COMPLET D'UN SYSTÈME D'INFORMATION
D'UNE ENTREPRISE MULTI-SITE DE 650 SALARIÉS
SPÉCIALISÉE DANS LE CONSEIL JURIDIQUE

Contexte

Le Système d'information a fait l'objet d'une cyber-attaque de grande ampleur par la diffusion et l'exécution des scripts par le malware CONTI. Le vendredi soir, l'équipe informatique constate des dysfonctionnements ci et là sur leurs outils de supervision et certains serveurs ne répondent plus aux connexions distantes. Le samedi matin, plus aucun serveur n'est accessible, le responsable informatique se rend sur place pour constater les dégâts : les serveurs virtuels sont partiellement ou totalement cryptés et les hyperviseurs VmWare Esx sont eux aussi corrompus. La baie de stockage DELL contenant des espaces SAN et NAS séparés est cryptée, la sauvegarde semble corrompue car exposée elle aussi en direct au serveur de sauvegarde, lui-même attaqué par le virus CONTI.

Le responsable informatique déclenche une demande d'assistance sur cybermalveillance.gouv.fr vers 14h00 et une cellule de crise est immédiatement montée avec les équipes du client et celles de Mederi Consulting.

La réponse apportée par Mederi Consulting

Le Système d'information est totalement déconnecté du réseau, les serveurs sont isolés et les quelques périphériques (PC et copieurs) sont déconnectés.

Sans aucune documentation, Mederi Consulting assiste le client d'une part à tenter d'annuler le cryptage par des snapshots de baie, et d'autre par à identifier les possibilités d'accéder à des jeux de sauvegarde (disque dur USB et solution de stockage vers 2nde baie + lecteur de bande.

Des preuves devant être conservées, il s'agissait d'envisager de reconstruire à l'identique un Système d'Information, sans réutiliser les baies de stockage, un challenge de plus !

Une méthodologie de remédiation a été proposée, ainsi qu'un planning de tâches à exécuter le Dimanche pour envisager une reprise en mode dégradé le lundi.

Mederi s'est donc positionné en tant que pilote de la cellule de crise et des différents intervenants, évitant ainsi de corrompre les sauvegardes.

Les résultats obtenus

Les données du disque dur USB n'ont pu être exploitées mais celles stockées sur la baie de sauvegarde ont pu être restaurées. La quasi-totalité des serveurs ont été restaurés au jeudi soir (certains ont du être recréés car non sauvegardés) et les snapshots de la baie ont permis une restauration sur la partie NAS.
Un partenaire a été missionné pour effectuer des opérations de Forensic (recherche des « root cause ») et de pentesting (identification des failles de Systèmes et du réseau).
Une lite de sujets de renforcement de la sécurité informatique a été dressée, afin de lancer des chantiers après la remédiation.

Le client a pu reprendre sa production 1 semaine 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