Parc d'Activités Schweitzer
26 rue du bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEIL

SAUVEGARDE DECONNECTEE REPONSE ULTIME AUX RANSOMWARES

POURQUOI RAJOUTER UNE SAUVEGARDE DECONECTEE SANS RESIDENT ?

Plusieurs dizaines d'entreprises locales de toutes tailles (de 1 à plusieurs centaines de collaborateurs) et d'activités diverses se sont vues chiffrer les données des serveurs, des postes de travail, les sauvegardes et même les sauvegardes externalisées.

Une partie des victimes hébergeaient leurs serveurs dans le Cloud et d'autres en local.

A notre connaissance le seul lien entre les victimes est la situation géographique régionale.

Aucun de nos clients dont nous gérons l'infrastructure n'a été impacté, il convient cependant de rester très prudent.

Les rançons demandées dépassent les 100.000 €, après paiement les pirates demandent un complément et ainsi de suite, jusqu'à doubler le montant initial.

Sans aucune garantie sur la restitution des données.

Fait nouveau, même les sauvegardes externalisées sont désormais en zone de risque.

Cette nouvelle donne nous pousse à proposer une solution complémentaire de sauvegarde en mode déconnectée.

Seule façon (à notre avis) de garantir la protection des données.

Ce que nous pouvons observer :

- Les pirates pénètrent les systèmes d'information via des failles (que ce soit en mode local ou hébergé (cloud))
- Ils restent en écoute du réseau plusieurs semaines jusqu'à récupération des identifiants Administrateur du SI, des sauvegardes locales et externalisées.
- Ils lancent des chiffrements sur le SI et les sauvegardes.
- Demandent des rançons
- Vont jusqu'à publier sur le web des informations confidentielles des victimes (Brevets, informations clients, fournisseurs et salariés)
- Certains signes laissent à penser qu'il s'agit d'une organisation structurée comptant de nombreux individus communiquant H24.
- Nous avons même constaté que des pirates n'arrivant pas à obtenir la rançon de la victime, publient sur le web les informations confidentielles (clients, fournisseurs, collaborateurs, brevets, documents juridiques et comptables).

La rentabilité des rançons perçues permet aux pirates de lancer des attaques manuelles (et non par des robots). Ils prennent leur temps et lancent le chiffrement lorsqu'ils sont certains que la victime n'aura pas de parade. Ils sont nombreux et fonctionnent en organisation structurée. Ils attaquent à partir de pays permissifs et n'ont aucun scrupule. Ils utilisent des logiciels sophistiqués issus de l'intelligence artificielle et profitent des moindres failles (Mises à jours non effectuées, ports ouverts, logiciels incluant des failles, Mots de passe courts ou logiques, télétravailleurs non sécurisés, périphériques non sécurisés, sécurités réseau mal configurées, usurpation d'identités par mail ou par téléphone, complices, prestataires malveillants etc…).

LA SOLUTION SAUVEGARDE DECONNECTEE SELON ESPACE TECHNOLOGIE

Le principe :

Proposer une solution sous forme de service pilotée par les services Expert d'Espace Technologie :

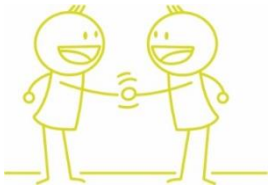
- Mise en place d'un boitier dont les disques sont dimensionnés au volume de données à sauvegarder
- Le boitier sera paramétré pour être hors du domaine réseau
  - Le boitier se situe sur votre site si vous n'avez pas de sauevagrde externalisée et dans notre Data Center dans le cas contraire.
- Aucun résidant présent sur le serveur, afin de ne donner aucune piste aux cyber criminels
- Un logiciel installé sur le boitier pilote la mise sous tension automatique du boitier
- Le boitier sauvegarde les données présente sur la sauvegarde 1er niveau
- Le boitier se déconnecte après le labs de temps nécessaire à la sauvegarde
- Le boitier est supervisée par sonde et communique avec Espace Technologie
- Cette sauvegarde se lance une fois par semaine ou une fois par mois suivant le choix du client *
- Les services d'Espace Technologie contrôle humainement que la sauvegarde soit bien réalisée
- Les services d'Espace Technologie réalisent les tests de restauration une fois par mois ou par trimestre*

Cette couche supplémentaire de sauvegarde est destinée à isoler les données du système d'information, elle ne peut pas se substituer aux autres solutions de sauvegarde car elle ne protège pas contre les risques classiques (Vol, incendie, dégat des eaux, dégat électrique, vandalisme ….)

**Compte tenu du temps de sauvegarde il est difficile de réaliser cette sauvegarde complémentaire quotidiennement lorsque le volume de données est important. Le coût engendré de la supervision serait aussi très élevé. Cependant nous pouvons étudier au cas par cas.*

NOUS VOUS CONSEILLONS VIVEMENT DE REALISER EN AMONT UN AUDIT CYBER SECURITE AFIN D'EVALUER LE NIVEAU DE SECURITE DE VOTRE SYSTEME D'INFORMATION.

NOTRE EXPERT EN CYBER SECURITE EST A VOTRE DISPOSITION POUR EVALUER, CONSEILLER, FORMER ET TESTER VOS VULNERABILITES TECHNIQUES ET HUMAINES.



Partenaire de confiance

ESPACE TECHNOLOGIE
Parc d'Activités Schweitzer
26 rue du Bois Fossé - BP 147
85301 CHALLANS cedex
Tél. 02 51 49 31 31
www.espace-technologie.com
contact@espace-technologie.com