Comment se protéger des ransomwares avec Nuabee

Cyber-Résilience by Nuabee · https://preview.nuabee.fr/documents/comment-se-proteger-ransomwares-avec-solutions-nuabee/

Qu’est-ce qu’une Attaque par Ransomware ?

Une **attaque par ransomware** est un type spécifique de cyberattaque où les attaquants utilisent un logiciel malveillant pour chiffrer les données de la victime, rendant ces données inaccessibles. Les attaquants exigent ensuite une rançon pour fournir la clé de déchiffrement. Voici les principales caractéristiques d’une attaque par ransomware :

- **Chiffrement des Données :** Le ransomware chiffre les fichiers de l’utilisateur (sur le poste de travail ou les serveurs), les rendant inaccessibles sans la clé de déchiffrement.
- **Demande de Rançon :** Les attaquants demandent une rançon, souvent en cryptomonnaie, pour déchiffrer les données.
- **Propagation Rapide :** Certains ransomwares se propagent rapidement à travers les réseaux, infectant de nombreux systèmes en peu de temps.
- **Impact Direct :** Les victimes perdent immédiatement l’accès à leurs données, perturbant les opérations jusqu’à ce que le problème soit résolu.

Les mécanismes de protection contre les Ransomware

Evidemment il existe beaucoup de mesures de sécurité pour réduire **la probabilité** pour une entreprise d’être touchée par une **attaque par ransomware,** on peut citer :

1. **Formation et Sensibilisation :** Former les employés à reconnaître les tentatives de phishing et autres menaces.
2. **Sécurité Réseau :** Utiliser des pare-feu, des systèmes de détection d’intrusion (IDS), et des réseaux privés virtuels (VPN).
3. **Outils de Détection de Malware :** Déployer des solutions de détection et de prévention de malware (EDR/XDR)

4. **Segmentation du Réseau :** Segmenter le réseau pour limiter la propagation du ransomware en cas d'infection.

Mais toutes ces **mesures de protection** ne garantissent pas à 100% d'une attaque réussie, il faut dont avoir des **mesures de récupération**, la plus importante étant la sauvegarde de vos données externalisée.

Comment Nuabee permet de récupérer d'une attaque via Ransomware

Au travers de ses solutions de sauvegardes Cloud externalisées, les principales protection apportées par Nuabee sont :

1. Un premier niveau de protection est évidemment la **profondeur des sauvegardes de recours** dans le Cloud.
   - Même si certaines données ont été chiffrées et sont envoyées dans le Cloud, la profondeur des sauvegardes permettra de repartir d'une sauvegarde antérieur saine, c'est à dire non chiffrée par le ransomware.

2. Ensuite, il s'agit également d'**immutabilité des sauvegardes** et d'être sûr que le ransomware n'a pas pu avoir accès à l'espace de stockage Cloud et n'a pas pu corrompre les données de sauvegarde.
   - L'isolation entre le cloud et l'environnement de production du Client (avec des AK/SK complètement distinct et des mécanismes de sécurités dédiés) permettent de sanctuariser les sauvegardes.
   - Le changement de technologie entre l'infrastructure du Client et les espaces de secours (stockage S3) assurent une rupture technologique

3. Il ne faut pas oublier que dans le contexte d'un chiffrement par Ransomware, il y a **100% d'entropie des sauvegarde**, ce qui veut dire que 100% des données chiffrées vont être réuploadés (comme dans un chargement initial).
   - Les outils de monitoring de Nuabee permettent de détecter ce comportement et d'alerter rapidement en cas de chiffrement des données à la source.