Gendarmerie nationale

Groupement de gendarmerie départementale du Var

Fiche réflexe en cas d'attaque de type ransomware

Un ransomware, ou rançongiciel en français, est un logiciel informatique malveillant, prenant en otage les données. Le ransomware chiffre et bloque les fichiers contenus sur votre ordinateur (ou votre serveur informatique) et vous demande une rançon (sous forme de monnaie virtuelle généralement de type Bitcoin) en échange d'une clé permettant de les déchiffrer.

Le ransomware s'infiltre sous la forme d'un ver informatique, à travers un fichier téléchargé ou reçu par email. Les données numériques chiffrées ne sont alors plus accessibles et parfois définitivement perdues, ce qui occasionne souvent de lourds préjudices pour les entreprises et les collectivités.

1/ Quelles mesures préventives ?

1. Instaurer une politique de sauvegarde et de restauration

Il faut mettre en place une stratégie de sauvegarde et de restauration à échéance très régulière (journalière ou hebdomadaire). Si les données sont sauvegardées et stockées sur un disque dur ou serveur en dehors du réseau internet, il sera alors possible de mettre en place rapidement un Plan de Reprise d'Activité (PRA) et ainsi de court-circuiter le ransomware.

2. Utiliser des outils de sécurité adaptés

Les outils de sécurité email et web permettent d'analyser les pièces jointes de courriel et les sites web visités qui sont deux vecteurs d'attaque privilégiés par les auteurs de ransomware. Ces applications doivent intégrer les fonctionnalités d'une sandbox[1].

3. Corriger et mettre à jour régulièrement tous ses outils informatiques

Les systèmes d'exploitation et les logiciels doivent être régulièrement corrigés et mis à jour car les malwares exploitent les failles de sécurité. Le travail de mise à jour ne doit pas se limiter à ces outils. Les outils de sécurité eux même comme les antivirus, pare-feu et autres anti-malware doivent aussi être actualisés régulièrement.

[1] mécanisme de sécurité informatique qui permet l'exécution de logiciel(s) avec moins de risques pour le système d'exploitation. Ces derniers sont souvent utilisés pour exécuter du code non testé ou de provenance douteuse de manière à ce qu'un fichier, nouvellement identifié ou non reconnu, puisse être exécuté et analysé dans un environnement sécurisé et cloisonné.

4. Mettre une "liste d'application" en place

Ce dispositif restrictif pour les collaborateurs les empêchera de télécharger et d'exécuter des applications qui ne sont pas validées par les responsables de la sécurité informatique. Il peut nécessiter un accompagnement en interne pour déminer la frustration des utilisateurs.

5. Segmenter le réseau

Côté réseau, il est également possible de segmenter virtuellement le réseau de la collectivité en différentes zones de sécurité. L'intérêt ? Empêcher une infection du ransomware présente dans une zone de se propager à d'autres.

6. Définir une politique de BYOD

Côté processus, la mise en place d'une politique de sécurité concernant le BYOD (Bring Your Own Device) doit aussi encadrer les pratiques et limiter l'accès aux ransomware. Il s'agit de fixer en interne les règles de fonctionnement des appareils mobiles des collaborateurs qui mettent en danger le SI comme absence d'anti-malware ou de systèmes d'exploitation non corrigés.

7. (In)former ses collaborateurs

Le facteur humain est le maillon faible de la chaîne de sécurité, c'est pourquoi il est primordial de sensibiliser ses collaborateurs à la sécurité aux travers de formations afin qu'ils apprennent à ne pas télécharger de fichiers douteux, cliquer sur des pièces jointes à des emails ou sur des liens suspects.

2/ Que faire en cas d'attaque ?

1 - Isoler au plus vite de l'internet votre réseau informatique local.

2 - Ne pas payer la rançon ou entrer dans des tractations avec le hacker, même si vous pensez obtenir la clef de déchiffrement après son paiement.

3 - Prévenir votre responsable informatique local la société qui assure la maintenance pour faire "geler" immédiatement les éléments numériques de preuve (créneaux dates/heure, adresses IP sur les logs de connexion de votre serveur attaqué, mails douteux ou pièces jointes suspectes).

4 - Aviser votre brigade de Gendarmerie locale de l'attaque dont vous êtes victimes. Une assistance de techniciens en technologies numériques pourra vous être proposée pour mettre en place les premières mesures d'urgence.

5 - Déposer plainte de manière exhaustive auprès de votre brigade de Gendarmerie locale, une fois les éléments numériques factuels isolés.

6 - Par la suite, dans le cas d'un plan de continuation d'activité, faire réinstaller les sauvegardes par votre technicien informatique.

Votre plainte sera systématiquement prise en compte au niveau départemental par les enquêteurs de la cellule en investigation numérique (recherche du point de compromission, identifications des adresses IP, examen du rançongiciel...).

Contacts :

- Major Jean-Pierre PASSEMARD - 04.94.46.72.18
- Adjudant Frédéric HALTER - 04.94.46.73.10

Cellule Investigation Numérique
GENDARMERIE DU VAR
307 Avenue Eole
83160 LA VALETTE DU VAR