Ne pas payer de rançon et porter plainte

En premier lieu, nous recommandons vivement à toute organisation victime d'un ransomware de ne pas payer la rançon car son paiement ne garantit aucunement le recouvrement des fichiers chiffrés : une fois la rançon payée, la clé de déchiffrement sera-t-elle vraiment remise à l'organisation attaquée ? De plus, la clé de déchiffrement ne permet pas toujours de reconstituer les fichiers.

Ensuite, il faut ouvrir une main courante afin de tracer les événements liés à l'incident : heure, date, nom des personnes impliquées, identification des machines à l'origine de l'action, description de l'événement et l'impact. Cela sera notamment utile pour déposer plainte. La démarche peut être initiée en ligne : https://www.pre-plainte-en-ligne.gouv.fr/.

Ouvrir une cellule de crise et communiquer

En parallèle, la constitution d'une cellule de crise, indépendante des groupes de travail opérationnels occupés à stopper la propagation du virus et à remettre le système d'information en marche, vous permettra de gérer les enjeux stratégiques liés à l'attaque de manière coordonnée : communication interne et externe, judiciarisation ou notification règlementaire liée à l'attaque en lien avec le DPO, etc. En effet, il est capital de communiquer en interne, afin d'accompagner les collaborateurs. Le mode opératoire des ransomware génère souvent émoi et anxiété en interne. C'est aussi le moment de demander aux collaborateurs d'appliquer la clause de confidentialité liée à leur contrat (médias, réseaux sociaux, etc.) et de s'assurer qu'ils transmettront bien toute sollicitation extérieure au service communication de l'organisation. Concernant la communication externe, les situations sont variées mais nous vous recommandons en général la transparence sur ce type d'attaques.

Quelques actions permettant de gérer la crise

- Déconnecter au plus vite les supports de sauvegarde
- Bloquer toutes les communications vers et depuis Internet (attention aux pertes d'accès à certaines applications externalisées, aux gels de l'envoi de courriels avec l'extérieur, etc.)
- Une fois les programmes malveillants identifiés, rechercher dans les journaux des caractéristiques propre à ceux-ci :

    - ⇨ URL utilisées pour communiquer avec l'infrastructure de l'attaquant
    - ⇨ Nom de fichier
    - ⇨ Hash
    - ⇨ Objet du courriel...

- Ne pas allumer les équipements non démarrés (retour de congés, démarrage d'une machine en début de journée, …)
- Interdire l'utilisation de supports amovible (clé USB, disque dur externe, etc.)
- Conserver les données chiffrées dans l'attente d'une solution de déchiffrement
- Restaurer les systèmes depuis des sources saines :

    - ⇨ La vulnérabilité exploitée pour l'attaque doit être corrigée (mise à jour logicielle, modification de la politique de filtrage réseau, etc.)
    - ⇨ Si les recherches ont permis d'identifier le logiciel malveillant, vérifier qu'aucune modification n'a été réalisée par ce dernier

- Changer les mots de passe
- Demander une assistance technique. La plateforme cybermalveillance.gouv.fr permet d'entrer en contact avec des prestataires de proximité.