Document d'information, Boîte à outils de cybersécurité de la GCA : Sauvegarder et récupérer

D'un point de vue commercial et personnel, la sauvegarde des données est essentielle car de plus en plus d'informations sont conservées en ligne. Elle joue un rôle crucial dans la continuité des activités de votre entreprise.

La perte de l'accès à vos données peut avoir de nombreuses causes. Dans notre cas, nous allons examiner la perte ou la corruption de données suite à une cyberattaque, mais la sauvegarde permet également de récupérer des données suite à la défaillance d'un disque dur, au vol de matériel, à une erreur humaine, à des dommages accidentels, à une inondation, etc.

Au vu de la forte dépendance à l'égard des ordinateurs et du monde virtuel, l'impact de la perte de données ou d'une interruption des activités peut avoir de graves répercussions sur la productivité et la rentabilité d'une organisation. La perte de photos de grande valeur sentimentale sur un ordinateur personnel est tout aussi catastrophique.

Réfléchissez à l'impact sur les finances et la réputation de votre entreprise si :

- Vos systèmes informatiques n'ont pas pu être utilisés pendant une journée.
- Vous avez manqué une proposition importante qui aurait pu vous faire remporter un gros contrat.
- Les fichiers des clients n'étaient plus accessibles ou ont été corrompus.
- Vous avez été informé que vous ne pourriez accéder à vos informations qu'à la condition de payer une rançon.

Les sauvegardes sont indispensables pour pouvoir récupérer vos données rapidement et reprendre vos activités !

Ransomware :

Un ransomware ou rançongiciel est un type de programme malveillant qui bloque l'accès à un système, un appareil ou un fichier tant qu'une rançon n'est pas payée. La rançon est généralement exigée en crypto-monnaie (c.-à-d., en bitcoin) car elle est moins facile à retracer que les transferts traditionnels.

Les ransomwares ont gagné en popularité et sont à l'origine d'un grand nombre d'attaques de haut niveau. Voici quelques exemples d'attaques de ransomware :

- WannaCry : ce ransomware a profité d'une vulnérabilité dans le système d'exploitation Windows en 2017. NHS, Renault et FedEx ont été touchés.

- Petya (2016) et NotPetya (2017) : Petya s'est répandu, caché dans un PDF joint à un e-mail (sous la forme d'un CV malveillant envoyé au service des RH), puis a évolué en NotPetya qui a profité, en partie, de la même faille que WannaCry.
- Début 2020, TravelEx, une société de change britannique, a été victime d'une attaque de ransomware qui l'a coupée d'Internet pendant plus de deux semaines, provoquant le chaos pour des millions de voyageurs.

Bien qu'il puisse être tentant de payer la rançon, il est recommandé de NE PAS le faire.

Protégez-vous contre les ransomwares :

- **Assurez-vous que tous vos systèmes sont à jour.** L'adoption d'une bonne cyber-hygiène, l'application de mises à jour correctives, la configuration de mises à jour automatiques et l'installation d'un logiciel antivirus en temps réel vous aideront à bloquer les attaques de ransomware.
- **Bloquez les messages d'hameçonnage/indésirables** en activant les filtres appropriés et en apprenant aux utilisateurs à ne pas cliquer sur les liens ou à ne pas ouvrir les pièces jointes provenant de sources non fiables.
- **Effectuez des sauvegardes régulières et externes** pour faciliter la récupération de vos données si vous êtes victime d'une attaque de ransomware (mais également d'un programme malveillant ou de toute autre cause de perte/corruption de vos données).

Les méthodes de sauvegarde sont variées :

- Les **sauvegardes hors ligne** désignent le stockage de données en local et hors connexion, tel que le stockage sur un disque dur externe, une clé USB, une carte mémoire ou tout autre appareil. Ces appareils doivent être déconnectés et stockés séparément de l'appareil lui-même.
- Les **sauvegardes en ligne** ou sauvegardes sur le cloud réalisent des copies de vos données importantes et les stockent hors site sur des serveurs sécurisés « dans le cloud ».

Les sauvegardes en ligne peuvent être configurées pour effectuer des sauvegardes automatiques à intervalles réguliers et constituent une bonne solution de récupération dans de nombreuses situations (le vol et les inondations par exemple). Lorsque vous tentez de récupérer vos données suite à une cyberattaque ou une attaque de ransomware, assurez-vous également que la sauvegarde n'a pas été impactée. Il est recommandé d'adopter une politique qui utilise les sauvegardes en ligne et hors ligne.

Réfléchissez à l'impact que pourrait avoir la perte de vos données et élaborez une politique de sauvegarde en conséquence. Il est recommandé d'utiliser le chiffrement pour protéger vos informations sensibles.

- Mettez en œuvre une approche (politique) sensée pour sauvegarder vos données en classifiant les différents types de données que vous détenez.
- Concernant vos données importantes et sensibles, réfléchissez à la fréquence à laquelle vous devriez les sauvegarder et à la méthode ainsi qu'à l'emplacement de stockage.

Utilisez les outils de la boîte à outils « Sauvegarder et récupérer » pour configurer des sauvegardes sur tous vos systèmes. Utilisez une unité ou un appareil externe pour effectuer des sauvegardes hors ligne.

https://gcatoolkit.org/fr/petites-entreprises/sauvegarder-et-recuperer/