Ransomwares - Mesures préventives

↳ **SENSIBILISER** la formation et la sensibilisation restent la meilleure des défenses. Se tenir régulièrement informer des menaces de sécurité. Apprendre à détecter et gérer les anomalies rencontrées (ingénierie sociale, phishing, etc…) ;

↳ **NE PAS OUVRIR** les mails, leurs pièces jointes et ne pas cliquer sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide. Qui ne vous semble pas adressé et qui comporte des anomalies, ou incohérences.

↳ **REALISER** régulièrement des sauvegardes des données et du système afin de pouvoir le cas échéant les réinstaller à une date antérieure, si ces derniers n'ont pas été corrompus. Diversifier les sources et niveau de sauvegarde.

↳ **TOUJOURS** maintenir son système à jour les mises à jour logicielles apportent les correctifs nécessaires sur les failles de vulnérabilités connues. Il est donc nécessaire de les faire systématiquement dès qu'elles sont disponibles chez l'éditeur.

↳ **TENIR A JOUR** l'antivirus et configurer votre pare-feu, vérifier et mettre en place un protocole ne laissant passer que les applications, services, accès et machines autorisés. **S'assurer que ces softwares soient à jour** afin d'avoir toujours les dernières définitions de virus connues à ce jour.

↳ **UTILISER** des mots de passe suffisamment complexes et les changer régulièrement, l'utilisation d'un gestionnaire de mots de passe est privilégié. A minima il faut un mot de passe de 12 caractère avec des caractères spéciaux.

↳ **NE PAS INSTALLER** d'applications ou de programmes dont l'origine ou la réputation sont douteuses.

↳ **CLOISONNER** l'accès administrateur du système, il convient de définir très précisément l'accès au compte administrateur du système tout comme les personnes pouvant bénéficier de ces privilèges. En agissant de la sorte et en différenciant les comptes utilisateurs des comptes administrateurs, on limite l'accès aux points critiques du systèmes.

↳ **EVITER** les sites non sûrs ou illicites tels que ceux permettant le téléchargement de contenus numériques (musique, films, logiciels…) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.

↳ **DESACTIVER LES MACROS** présentes dans de nombreux fichiers, notamment ceux des suites bureautiques, elles peuvent exécuter un malware. Les désactiver d'office réduit les conséquences que cela peut avoir si utilisateur sélectionne un fichier infecté.

↳ **ETRE VIGILANT** avec les supports externes ils peuvent contenir des malwares qui s'éxecuteront sur le système, ou à l'inverse le malware pourra s'intaller dessus et s'installer sur d'autres systèmes.

↳ **COMPARTIMENTER LE RESEAU** les ransomwares chercheront à se propager, d'abord latéralement dans le système pour obtenir le maximum de données nécessaires puis « verticalement » en élevant consécutivement leurs privilèges jusqu'à atteindre administrateur. Ainsi un cloisement permet de limiter cette propagation du malware dans le système.

↳ **NE JAMAIS TRANSMETTRE** ses données personnels avant d'avoir vérifier les garanties d'un site. Dans tous les cas il est vivement conseillé de ne pas fournir ses coordonnées bancaires en ligne, pour une mise à jour de son dossier.

↳ **CHIFFRER** dès que possibles données sensibles présentes sur votre PC.

↳ **ÉTEINDRE** votre machine dès lors que vous ne vous en servez pas.