7 étapes pour prévenir les ransomwares pendant les fêtes de fin d'année.

Tout le monde apprécie les fêtes de fin d'année, mais personne ne les attend autant que les réseaux de ransomware. Heureusement, il suffit parfois d'un peu de préparation pour éviter les désagréments. C'est pourquoi nous avons préparé une liste de contrôle en sept étapes, destinée aux entreprises, pour leur permettre de profiter des vacances en toute sérénité.

- ☐ **Mettez vos projets en attente.** La période précédant les fêtes n'est pas idéale pour effectuer des changements majeurs dans votre environnement informatique. En cas de ransomware, vous aurez besoin d'un environnement stable et familier. Si vous ne pouvez pas finaliser vos projets avant les fêtes, il est préférable de les différer.
- ☐ **Établissez une liste de contacts.**.En cas d'attaque par ransomware, il est crucial de mobiliser toutes les ressources disponibles. Maintenez une liste à jour des noms et coordonnées, et veillez à la partager de manière sécurisée pour qu'elle reste accessible même si votre réseau est compromis.
- ☐ **Attribuez des rôles et des accès.** Pendant les vacances, il arrive souvent que certains collaborateurs soient indisponibles. Assurez-vous que les postes critiques, notamment en informatique ou en sécurité, soient assurés par au moins une autre personne. Veillez également à ce que ces collaborateurs partent en vacances avec les connaissances, la documentation, les accès et l'équipement nécessaires.
- ☐ **Éteignez ce que vous pouvez**. La configuration la plus sûre pour un ordinateur est de l'éteindre. Moins il y a d'ordinateurs allumés et de logiciels en cours d'exécution, plus il est difficile pour les groupes de ransomware de pénétrer dans votre organisation, de s'y déplacer ou d'accéder à vos données critiques.
- ☐ **Installer les mises à jour de sécurité.** Effectuer les mises à jour est sans doute l'une des tâches les plus importantes que vous puissiez accomplir en matière de sécurité. Avant de partir en vacances, assurez-vous que tous les logiciels de votre environnement ont reçu les dernières mises à jour de sécurité. Si une mise à jour complète n'est pas possible, donnez la priorité aux logiciels connectés à Internet et aux vulnérabilités activement exploitées.
- ☐ **Testez vos sauvegardes.** Elles représentent votre dernière ligne de défense contre les ransomwares, mais elles ne sont utiles que si elles fonctionnent correctement. Les réseaux de ransomware tenteront de les supprimer. Assurez-vous donc de disposer d'une sauvegarde hors ligne de vos données, inaccessible depuis votre réseau, et vérifiez son bon fonctionnement en restaurant des données critiques à partir de cette sauvegarde.
- ☐ **Surveillez vos alertes**. De nombreux cybercriminels génèrent des alertes de sécurité pendant qu'ils préparent leur attaque. Cependant il arrive qu'ils parviennent à passer inaperçus, car ces alertes ne retiennent pas l'attention du personnel, souvent occupé par d'autres priorités. Pour une meilleure protection, optez pour un service géré de détection et de réponse, tel que ThreatDown MDR, offrant une surveillance des menaces en continu, 24h/24, 7j/7 et 365 jours par an.

www.shi.fr
threatdown.com
shi.information@shi.com