Faut-il avoir peur des ransomwares ?

	Faut-il avoir peur des ransomwares ?

Depuis le premier virus détecté en 1986, le nombre d'attaque n'a cessé d'augmenter, devenant la menace la plus importante pour les entreprises.

En effet, cette forme d'attaque profite aux cybercriminels qui ont trouvé le bon filon pour gagner de l'argent. En constante mouvance, les formes d'attaques sont de plus en plus redoutables et ont généré un trafic de données important : les informations détenues par les entreprises sont désormais toutes disponibles en environnement virtuel et constituent l'élément essentiel pour l'économie de la société (données sensibles, fichiers clients, etc). Leur perte est inconcevable et cela, les cybercriminels l'ont bien compris. Au fil des ans, leurs techniques ont changé jusqu'à l'arrivée des ransomwares. Ce type d'attaque se révèle être la plus rentable pour les attaquants qui multiplient les variantes. La tendance est d'ailleurs à l'augmentation sur tous types de support connecté.
Parce que la perte de données en entreprise peut avoir des conséquences irrémédiables sur son activité si l'on prend en compte les paramètres suivants : perte de productivité, perte de données et la réputation liée à ces deux pertes, le non-paiement de factures émises, perte de confiance des salariés dans leur entreprise ; l'impact d'un ransomware peut être catastrophique. Le succès et les méthodes pour obtenir un paiement rapide de la rançon ont permis aux cybercriminels d'attirer l'attention des médias et d'entretenir ce climat de tension.
Il y a quelques mois, ESET a averti les utilisateurs qu'un nombre impressionnant d'e-mails infectés propageaient des ransomwares, submergeant ainsi les boîtes de réception dans le monde entier. Feignant de ne contenir que des fichiers inoffensifs, JS/TrojanDownloader.Nemucod essayait en réalité de forcer les victimes à télécharger et à installer des ransomwares tels que TeslaCrypt ou Locky. Cette stratégie fut efficace puisque les cybercriminels l'ont répété plusieurs fois, multipliant également les variantes utilisées tels que CTBLocker ou Filecoder.DG.
Heureusement les ransomwares ne sont pas toujours aussi dangereux que ceux cités ci-dessus. Beaucoup de cybercriminels amateurs surfent sur cette tendance et développent leur propre ransomware dont l'exécutable, de faible qualité, est facile à contrer. Ceci fut le cas de Petya et Jigsaw qu'ESET a analysé : tous deux contenaient des défauts de mise en œuvre qui ont permis aux victimes touchées de récupérer leurs fichiers sans payer un centime.

Comment vaincre cette peur du ransomware ?
Avoir peur du ransomware ne vous en protègera pas pour autant et payer la rançon ne résoudra pas forcément vos problèmes. Si vous en arrivez à ce stade, c'est que vous n'avez pas appliqué toutes les précautions nécessaires.
La meilleure façon de ne plus avoir peur des ransomwares est de se protéger avec une solution efficace et reconnue, et de s'assurer de couvrir 3 domaines complémentaires : technologique, politique de sécurité et éducation des employés. Sous l'impulsion de l'Etat et des agences de sécurité, les entreprises sont encouragées à adopter des mesures de protection. Les textes, dont le RGPD, étant là pour cadrer l'utilisation et la sécurité des données détenues par les entreprises. En particulier, les investissements dans la recherche et le développement de nouvelles technologies nécessitent un plan de sécurité permettant d'évaluer et de décrire leur sécurité.
Par conséquent, avec des attaques de plus grande envergure et l'émergence de nouvelles vulnérabilités, le plus grand défi de 2016 est de mettre l'accent sur la protection des réseaux et l'accès aux données. Les meilleures pratiques de sécurité doivent donc être appliquées pour protéger les données, les informations et la vie privée. Il s'agit là d'un travail transversal qui exige une participation active des plus hautes fonctions de l'entreprise.
Faut-il avoir peur des ransomwares ? La réponse est non pour tout dirigeant préparé à cette éventualité.
Source : Benoît Grunemwald – Directeur des Opérations ESET France

---

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Charts | ESET Virusradar