Ransomware : ne payez jamais la rançon

Ransomware : ne payez jamais la rançon

Lors d'une conférence sur la cybersécurité organisée la semaine dernière à Boston par SecureWorld, un consultant a recommandé de ne pas régler la rançon réclamée par les cybercriminels pour obtenir la clef de décryptage des fichiers verrouillés. Il recommande plutôt de veiller à bien sauvegarder ses données.

Dès qu'une demande de rançon apparaît sur l'écran, il faut immédiatement déconnecter le poste de travail du réseau. (Crédit D.R.)

Lors d'une conférence sur la cybersécurité organisée la semaine dernière à Boston par SecureWorld, un consultant a recommandé de ne pas régler la rançon réclamée par les cybercriminels pour obtenir la clef de décryptage des fichiers verrouillés. Il recommande plutôt de veiller à bien sauvegarder ses données. « Cela semble facile à dire, surtout quand le risque de perdre des données critiques est assez faible. Cela nécessite aussi une certaine préparation », a ainsi déclaré Michael Corby, consultant exécutif pour CGI. Selon lui, « le plus important est de stocker ses données sous une forme qui ne pourra pas être affectée par le ransomware, en les chiffrant et en les stockant hors du réseau de production ». Ajoutant que l'entreprise « a besoin d'une copie propre des données qui sera facile à restaurer ». Celui-ci recommande également de vérifier « que les sauvegardes fonctionnent ». Restauration et récupération sont donc les maîtres mots, et « il faut bien penser à supprimer le malware avant de procéder à ces opérations ».
Si le consultant préconise de ne pas payer de rançon, il sait aussi que les autorités judiciaires estiment généralement que le paiement de la rançon est parfois inévitable et que c'est aussi le seul moyen pour l'entreprise de récupérer des données essentielles. Elles vont même jusqu'à les encourager à se doter d'un porte-monnaie bitcoin avant d'être affectées par un ransomware. Elles pourront ainsi effectuer un paiement rapide si nécessaire, les ultimatums posés par les pirates étant souvent assez courts.

Déconnecter immédiatement le terminal

La première règle que tous les employés doivent connaître quand l'entreprise est confrontée à un ransomware c'est de ne pas essayer de comprendre ce qui se passe. Dès que la demande de rançon apparaît sur l'écran, le ou les utilisateurs doivent déconnecter immédiatement le poste de travail du réseau et en informer le responsable de la sécurité. À son tour, ce dernier doit mettre en branle son équipe d'intervention, c'est à dire lui-même, mais aussi le département juridique, les relations publiques, les relations humaines, les cadres et l'IT.
En France, l'entreprise doit immédiatement informer la cybergendarmerie ou la police judiciaire. La procédure est contraignante, car en s'adressant aux forces de l'ordre, l'entreprise renonce au contrôle de l'enquête et parfois aux dispositifs et aux données qu'ils contiennent, puisqu'ils peuvent seraient saisis pour la recherche de preuves.

Comment bloquer les ransomwares

Voici quelques-unes des meilleures pratiques que les entreprises doivent adopter pour lutter contre les ransomwares. Ces mesures seront également très bénéfiques pour le réseau en général :
– Sensibiliser les utilisateurs finaux sur les logiciels malveillants en proposant des programmes d'information réguliers.
– Corriger et mettre à jour ses systèmes, y compris les solutions de sécurité et le logiciel antivirus.
– Déculpabiliser l'utilisateur final, afin qu'il n'ait pas peur de signaler l'attaque immédiatement.
– Bien gérer les privilèges des comptes d'administration.
– Désactiver les macros.
– Limiter le Byod à quelques périphériques et leur appliquer des politiques de sécurité strictes.
Article rédigé par Tim Greene / Network World (adaptation Jean Elyan)

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Ransomware : ne payez jamais la rançon – Le Monde Informatique*