Rançongiciel : prévenir plutôt que guérir

Les attaques au rançongiciel ont plus que doublé en 2019 selon une étude de McAfee. Elles ciblent principalement les petites structures qui sont en général moins bien protégées. Pour prévenir les risques, il faut sensibiliser les membres de l'association.

Un rançongiciel (ransomware en anglais) est un virus qui accède aux ordinateurs par les moyens classiques de diffusion des virus : mails « malicieux », images ou vidéos infectées, action spécifique dans un site internet ou de téléchargement… Dans le cas le plus classique, le rançongiciel va crypter les données ou la totalité du disque dur. Le virus affiche alors sur votre écran les coordonnées du pirate auquel vous devez verser une certaine somme pour qu'il vous transmette la clé secrète qui permettra le décryptage. La redevance moyenne est de l'ordre de 700 euros par poste. D'autres ransomwares sont moins intrusifs, mais font du chantage à l'utilisateur : par exemple une fausse amende d'un faux site gouvernemental pour consultation de site illicite avec blocage des accès internet.

Ne jamais payer

En cas d'attaque, il faut isoler la machine infectée de la connexion internet et du réseau de l'association tout en avertissant les utilisateurs. Ensuite, il faut identifier la source de l'infection : virus concerné, vecteur d'entrée (mail, fichier, mise à jour…). Un deuxième principe est de ne jamais payer : les moyens de décryptage promis par le pirate ne sont fournis en retour que dans un petit pourcentage de cas. Pour certains ransomwares, il existe des solutions de décryptage publiques (disponibles auprès des éditeurs d'antivirus), mais cela ne concerne que les virus les plus classiques. Dans tous les cas, il faut porter plainte auprès des services spécialisés de police ou de gendarmerie et se faire assister par des organismes publics (www.cybersurveillance.gouv.fr, www.anssi.fr).

Mises à jour et sauvegardes

Toutes ces actions curatives ne peuvent être que des mesures d'exception. La protection passe d'abord par des options préventives à la fois dans le domaine technique et comportemental. Côté technique, il faut appliquer toutes les mises à jour de sécurité de votre système dès qu'elles sont publiées et obliger les utilisateurs à le faire indépendamment de leur volonté (mise à jour automatique non invalidable). Il faut également avoir un antivirus à jour (mise à jour quotidienne si possible) avec les mêmes implications pour l'utilisateur que pour les mises à jour système. Il faut surtout faire des sauvegardes régulières et sur des supports successifs : un par jour par exemple gardé pendant 7 jours : on dispose alors des 7 dernières sauvegardes permettant de remettre le poste infecté en état avec la dernière sauvegarde qui n'a pas stocké le virus.

PRENDRE EN COMPTE LES SPÉCIFICITÉS ASSOCIATIVES

Les associations ont parfois du matériel informatique ancien. En outre il est fréquent que les bénévoles partagent un même mot de passe informatique ou un même ordinateur. Il est donc difficile d'identifier la connexion en cas de problème. Il faut prendre en compte ces spécificités pour sensibiliser les utilisateurs de votre association aux risques de cybercriminalité.

Précautions d'utilisation

Côté comportemental, les actions sont plus difficiles à mettre en œuvre car elles impliquent la participation active des utilisateurs. Il faut convaincre ces derniers par des séances de sensibilisation que ce sont eux le maillon faible de la chaîne de sécurité et qu'ils peuvent, par leur comportement, invalider les options techniques mises en place. Ne pas ouvrir de mails, des pièces jointes ou de liens issus d'expéditeurs inconnus et de faire attention à ceux provenant d'expéditeurs connus, mais dont la structure semble bizarre (cas de « l'hameçonnage » pour provoquer une action de la part de l'utilisateur qui va installer le virus). Ne pas installer de logiciels contrefaits et éviter les sites de téléchargement non légaux. Enfin, ultime protection : éteindre son ordinateur pour éviter les risques d'utilisation d'un ordinateur à l'insu de l'utilisateur. ■

Jean-Luc Austin et Thierry Legrand, associés Exponens