Se protéger des rançongiciels

Les rançongiciels (ou ransomwares) sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament une rançon pour pouvoir y accéder à nouveau. C'est la mésaventure qui est arrivée récemment à la ville d'Annecy, victime de ce type de cyberattaque et qui a vu tous ses services informatiques arrêtés, rendant inaccessibles les démarches administratives auprès des services municipaux. Le plus souvent, les victimes voient leurs ordinateurs se faire infecter par des messages électroniques lors de campagnes de « phishing » (ou hameçonnage). Le phishing étant une technique frauduleuse destinée à leurrer un internaute pour l'inciter, en se faisant passer pour une entreprise connue ou une administration, notamment, à cliquer sur une pièce jointe portant un malware.

Ne pas cliquer sur les pièces jointes de mail inconnus

Pour le site www.cybermalveillance.gouv.fr, plusieurs actions peuvent être mises en place pour s'en prémunir, comme il le rappelle dans une fiche pratique. Il est ainsi conseillé, par exemple, de mettre systématiquement à jour les systèmes de sécurité du système et les logiciels installés. Ou encore de ne pas installer d'application ou de programme piraté, ni de cliquer sur les pièces attachées de mails d'inconnus et dont la structure du message est inhabituelle ou vide.

La fiche pratique aborde également les mesures à prendre si

l’entreprise est victime d’un rançongiciel. Il est clairement indiqué, notamment, de débrancher immédiatement la machine contaminée du réseau de l’entreprise afin d’éviter que d’autres soient contaminées, de ne jamais payer la rançon et de porter plainte systématiquement !

Pour consulter la fiche : www.cybermalveillance.gouv.fr