Midi Libre
30 juin 2017

« La sécurité numérique devrait être enseignée à l'école »

Virus. Adel Jomni, expert en cybercriminalité, revient sur les cyberattaques récentes.

Le virus Petya paralyse entreprises et administrations depuis deux jours. Parti d'Ukraine, ce *ransomware* (virus envoyé dans le but d'extorquer de l'argent) s'introduit dans les systèmes informatiques et se propage à travers le monde. En France, le groupe Saint-Gobain, la SNCF ou BNP Paribas ont été touchés. Pour Adel Jomni, enseignant-chercheur et maître de conférence en cybercriminalité à l'université de Montpellier, l'ampleur de ces attaques est due à nos mauvaises pratiques numériques.

Comment fonctionnent ces attaques ?

Il s'agit d'un *ransomware* classique : à la suite d'une vulnérabilité, humaine ou technologique, un virus s'installe sur votre machine, la force à redémarrer, chiffre tous vos fichiers puis on vous demande une rançon contre la clé de décryptage. C'est une méthode très classique, de plus en plus utilisée par les cybercriminels.

Qui peut être touché ?

Tout le monde ! Individus comme entreprises. Bien sûr, les hackers privilégient les entreprises parce qu'il y a souvent plus de données et que les entreprises payent plus rapidement, par peur et pour leur réputation. Même s'il est fortement déconseillé de le faire, car elles encouragent la cybercriminalité en faisant cela, sans avoir l'assurance d'obtenir ce qu'elles veulent.

■ Adel Jomni lors d'une conférence à l'université de Montpellier.

Comment se prémunir ?

Il s'agit de gestes très simples, sur deux niveaux. Premier niveau : mettre à jour vos logiciels. Sur le marché, 80 à 90 % des logiciels vendus sont vulnérables. Et hackers comme entreprises cherchent les failles. Quand elles les trouvent, les entreprises lancent des mises à jour de leurs logiciels. Si vous ne les installez pas, vos logiciels restent vulnérables. Exemple : de très nombreuses entreprises et individus utilisent encore Windows XP pour travailler. Mais Microsoft ne fait plus de mise à jour sur XP depuis longtemps. Les gens qui l'utilisent sont donc exposés.
Par ailleurs, il faut faire de la sensibilisation en entreprise et éduquer tout le monde à l'hygiène numérique : faire des sauvegardes régulières, sur des supports déconnectés du réseau, toujours vérifier les objets et expéditeurs de mails, ne pas ouvrir de pièce jointe douteuse, ne pas cliquer n'importe où, etc.
Le second niveau concerne les usages : mettre un mot de passe, de huit caractères minimum, le changer tous les mois, faire du chiffrement en entreprise, configurer les pare-feu, etc.

Cela semble pourtant assez simple...

Bien sûr. Tout le monde le sait. Mais le nombre de personnes attaquées par ces *ransomware* montre que, malgré tout, on ne le fait pas. Faites le test : depuis quand n'avez-vous pas changé votre mot de passe ? Combien de sauvegardes avez-vous effectuées ce dernier mois ?

Ces attaques vont-elles se multiplier à l'avenir ?

C'est certain. Et je me fais beaucoup de soucis pour les PME. Les grosses structures, elles, sont sensibilisées à ça. Mais pas les petites, malgré un travail formidable de l'Anssi (Agence nationale de la sécurité des systèmes d'information) ou de la Cnil (Commission nationale de l'informatique et des libertés). Aujourd'hui, il n'y a aucune entreprise non connectée. Aucune. Donc se faire avoir par un *ransomware*, c'est une faute professionnelle.

Quelle est la solution ?

Il faut éduquer tout le monde au numérique. Former aux bons usages. À commencer par les jeunes. Personnellement, je pense que le numérique, et donc la sécurité, devrait être une matière à part entière à enseigner à l'école, au collège, au lycée, à l'université, etc. Nous aurons alors une vraie culture numérique. Et elle inclura notre propre protection.

Recueilli par PIERRE BELMONT
redac.montpellier@midilibre.com