L’est Républicain – supplément économie du 16 novembre 2019

Digital "La sécurité informatique n’est pas encore dans nos mœurs"

Créateur de la société 2PIE (Sécurisation de l’Information, Gestion de Crise, Intelligence économique) qu’il a créée à Dole (Jura) en 2013, Bruno Migeot a été gendarme à l’antiterrorisme de Paris avant d’arriver à la tête de l’antenne Intelligence économique de Franche-Comté. Interview.

Le 17/11/2019 à 05:00

Bruno Migeot : « Le minimum est d’avoir un antivirus, un pare-feu,des machines et des logiciels mis à jour, des mots de passe solide,des sauvegardes fréquentes… Bref toutes ces préconisations que l’on répètedepuis dix ans mais qui sont loin d’être toujours mises en œuvre ».

Vous donnez des conseils et réalisez des diagnostics en matière de cybercriminalité pour les entreprises, de la PME-PMI aux grandes entreprises type Alstom. Comment la situation a-t-elle évolué ces dernières années ?

Mon premier constat est que la prise de conscience n’avance que très lentement. La sécurité informatique n’est pas encore dans nos mœurs. Il y a toujours du relâchement. Alors qu’en face, les attaques sont de plus en plus nombreuses, sophistiquées, et toujours plus différentes. Sachant

qu'il est très difficile d'avoir des statistiques. Ce sont des chiffres noirs : les entreprises qui se font avoir ne s'en vantent pas…

Quelles sont les principales cibles et quels types d'attaques subissent-elles ?

Les cibles sont le plus souvent les petites entreprises. Quant aux attaques, elles sont de plusieurs types. Vous avez celles, très fréquentes, pour gagner de l'argent immédiat (escroqueries, faux ordre de virement, fraude au président…). On commence aussi à voir de plus en plus de mining : des gens qui injectent des virus dans les ordinateurs pour ralentir les processeurs. Il y a aussi le wiper, ou essuie-grace, qui efface toutes les données pour le pur plaisir de nuire. Et après vous avez les attaques informatiques, la cybercriminalité, les cryptolockers qui fonctionnent au chantage.

Qu'est-ce que ce crypto-blocage ?

Il s'agit de virus qui cryptent les données des entreprises. C'est un fléau. Ces attaques ont souvent lieu le vendredi soir comme cela le virus se propage tout le week-end et quand vous arrivez le lundi, vous avez un message sur votre écran vous demandant une rançon en bitcoins. Et quand on paye, on a une chance sur deux d'avoir la clé. C'est très fréquent chez les professions libérales. Je connais un cabinet immobilier de la région dont toutes les agences ont été totalement bloquées parce qu'elles n'avaient pas de sauvegarde.

Quels bons usages préconisez-vous ?

Le premier, c'est le bon sens. Ne pas avoir la tête dans le guidon. Et commencer par réaliser des sauvegardes fréquentes. Ensuite, si les anti-virus sont la plupart du temps efficaces, l'utilisateur demeure le maillon faible. Il faut connaître les risques afin de savoir éviter des erreurs qui coutent très cher à l'entreprise. C'est un souci quotidien et il faut des piqûres de rappel régulières pour que tout le monde, de la direction générale à la base, soit sensibilisé et participe globalement à la politique de sécurité.

Propos recueillis par Pierre LAURENT