# Informer les entreprises du risque cybercriminel

***Lors de portes ouvertes à Est Multicopie à Maxéville, un consultant en sécurité numérique a effectué des conférences sur le risque cybercriminel. Décryptage.***

Des banderoles noires et jaunes à l'entrée, le corps d'une victime matérialisé par un marquage au sol, pas de doute, le visiteur tombe de plein pied dans une scène de crime. « On voulait informer nos clients sur la cybercriminalité et la question des flux documentaires », expose Lucile Fourrier, chargée de l'accompagnement des commerciaux à Est Multicopie basé à Maxéville.

Sur la scène de crime, au beau milieu des photocopieurs, un consultant en sécurité numérique employé par un éditeur liste trois objectifs à sa présence lors de ces portes ouvertes du 5 au 7 décembre : informer, conseiller, s'équiper.


## Vers un "Far West numérique" ?

«Aujourd'hui, une PME sur deux en Europe est victime de cyber-attaque. Il y a dix ans, il y avait 1833 attaques informatiques par mois. Aujourd'hui, il y en a 9300 par semaine», affirme Brieuc Lavie, consultant en sécurité informatique. Selon ce dernier, les entreprises évoluent dans un « Far West numérique » dans-lequel les Daltons ont troqué leur tenues de prisonniers pour des masques de hackers (pirates).

« Entre 2015 et 2017, les attaques informatiques ont augmenté de 68% à travers une stratégie de valeur et de volume. D'ici trois ans, ce chiffre-là pourrait doubler », alerte Brieuc Lavie. Cette augmentation importante du nombre de cyber-attaques illustre pour le consultant un « Far West numérique » dans-lequel évoluent toutes les entreprises.

Sur le darknet (marché noir du web, partie immergée de l'iceberg), coordonnées bancaires, numéros de sécurité sociale, faux papiers (carte d'identité, passeport, permis de conduire, etc.) s'échangent en bitcoin (crypto-monnaie utilisée pour les transactions sur le darknet).

Comment les hackers parviennent-ils à dérober toutes ces données ? Pour pénétrer dans le parc informatique des entreprises et des particuliers, ils utilisent la technique du «phishing». Par l'intermédiaire d'un mail accompagné d'une pièce-jointe, ils sont capables d'entrer dans le système et d'inoculer le virus. Ils dupent les internautes via des faux sites qui ressemblent comme deux gouttes d'eau à un vrai site. Ainsi, ils récupèrent les identifiants des utilisateurs via des logiciels espions qui enregistrent les frappes effectuées sur le clavier.

L'arme d'intimidation massive des hackers pour voler les entreprises reste le rançongiciel (logiciel de rançon). Dans ce cas de figure, les pirates s'emparent de l'ensemble des données informatiques de l'entreprise, les cryptent, puis demandent une rançon. Comme les pionniers recherchaient les pépites d'or dans le Far West, les hackers traquent « les données informatiques à forte valeur ajoutée des TPE et PME ».

## Quelles solutions pour se prémunir du risque cybercriminel ?

Parce qu'ils naviguent sous couvert d'anonymat via une connexion internet qui renvoie à des adresses IP dans une multitude de pays, les hackers jouissent d'un écran de fumée face à la Justice. « L'activité est peu risquée car en cas d'attaque, l'avocat va devoir remonter à l'origine de l'attaque et s'adresse à chaque pays avec sa propre législation », explique le consultant en sécurité informatique.

La diffusion de l'information auprès des entreprises, surtout auprès des TPE et PME est indispensable. Sans pour autant surestimer cette menace, le risque (technologique) 0 n'existe pas. Cependant, il existe en amont plusieurs moyens pour se protéger d'une cyber-attaque. En préventif, il est possible d'installer un firewall (pare-feu), proxy (logiciel qui facilite et surveille entre deux hôtes), un antivirus et un anti-spam (logiciel pour protéger les messageries). En curatif, il est fortement recommandé d'effectuer des sauvegardes de l'ensemble de ses données et d'effectuer des expérimentations de PRA-PCA (Plan de Reprise d'Activité-Plan de Continuité d'Activité).

Lorsqu'une entreprise est victime d'une attaque et qu'une rançon lui est demandée, « mieux vaut ne pas payer », affirme Brieuc Lavie. Rien ne garantit en effet que le versement de celle-ci permettra à la société, ni de récupérer l'intégralité de ses données, ni que celles-ci ne soient pas corrompues. Dans ce cas, la seule parade est d'avoir effectué des sauvegardes pour pouvoir poursuivre son activité.

**Kévin Lamblé**

MEURTHE-ET-MOSELLE
Informer les entreprises du risque cybercriminel
page 32


l'abeille 54
jeudi 14 décembre 2017
9 "770181" 559109
9006 °N -
l'abeille
GRAND EST