

# Les courtiers champenois appellent à la prévention

La filière champagne n'échappe pas aux cyberattaques qui touchent désormais toutes les entreprises. Les plates-formes professionnelles, contenant des données financières sensibles et confidentielles, constituent une nouvelle cible pour la cybercriminalité. Le Syndicat professionnel des courtiers en vins de Champagne (SPCVC) a organisé une matinée pour évoquer les risques encourus et les moyens de se protéger.



« **L**'idée de cette rencontre nous est venue à la suite d'une tentative de piratage de notre réseau. Heureusement nous avons su réagir à temps », lance Franck Hagard, co-président du SPCVC avec Jean-Pierre Dargent. Si, pendant longtemps, les cyberattaques ont essentiellement concerné les grands groupes, c'est maintenant au tour des PME et même des TPE, d'être victimes de cybernautes très organisés. Les courtiers n'y échappent pas alors qu'ils occupent une place centrale entre maisons et vignerons, au cœur de 80 % des transactions en Champagne. « Il nous a semblé primordial de prendre la mesure de cette nouvelle criminalité mais aussi de vérifier que nous avions adopté de bonnes pratiques de prévention et que nous disposions des outils adaptés », souligne Franck Hagard.

S'il faut connaître les techniques de protection, la prévention reste la précaution majeure. « Nous allons organiser une formation sur les bonnes pratiques afin de sensibiliser nos adhérents à ce type de fraude, poursuit Jean-Pierre Dargent. Car la plupart du temps la fraude est rendue possible à la suite d'une erreur humaine. Il faut savoir identifier rapidement une tentative d'attaque et renforcer les systèmes d'alerte. » Une réactivité fondamentale lorsqu'on

sait que les courtiers champenois effectuent des centaines de millions d'euros de transactions par an sous la forme de virements. « Les attaques sont de plus en plus sophistiquées, comme la triche au dopage dans le sport, et le temps de réaction très court, de 24 à 48 heures », explique Jérôme Prince, le président de la Fédération nationale des syndicats de courtiers en vins et spiritueux.

Pour évoquer les stratégies à mettre en place, le SPCVC avait invité plusieurs spécialistes de la fraude en entreprises dont un lieutenant et un commandant de police. Le premier de la Brigade de répression de la délinquance astucieuse (BRDA) et le second chef de la division économique et financière de la police judiciaire de Reims. « Les grands groupes sont aujourd'hui sensibilisés à ces attaques. Mais les victimes sont désormais de petites entreprises qui doivent multiplier les précautions, a commenté le lieutenant de police lors de cette réunion. Il est très important que les sociétés sensibilisent leurs collaborateurs à ces risques. » À cet égard Jean-Pierre Dargent estime que la formation proposée par le syndicat pourrait se faire en lien avec la police. « Il est important de déve-

lopper les échanges. Même si les sociétés informatiques réalisent des mises à jour permanentes. »

Philippe Gaud, responsable Prévention de la fraude au Groupe Crédit Agricole SA, a présenté le travail d'accompagnement qui était réalisé par sa société pour ses clients. « Nous assistons à un accroissement des attaques », estime-t-il. La mondialisation, qui a rendu plus complexes les structures des entreprises et le développement des nouvelles technologies, crée une véritable porte ouverte sur les systèmes d'information de entreprises. Deux chiffres sont particulièrement évocateurs : 70 % des mails sont porteurs de spams et 65 % des internautes ont été victimes d'attaques. La France connaît notamment une progression très importante du volume de fraudes et la cybercriminalité a explosé entre 2014 et 2016, de 24 points. Elle est le deuxième pays en nombre d'attaques sur les réseaux sociaux, et les banques sont particulièrement ciblées. « La sécurité de nos clients fait partie de nos missions. Nous devons encore renforcer le cryptage lors du trajet de données et de fichiers de paiement », précise Jean-Pierre Dargent. ■

**L'importance de l'échange et de l'accompagnement**

Jean Batilliet