logiciel de rançongiciels" qui verrouillent les données

rates utilisent une faille connue. » Avec un budget de

(*) Envois de mails avec des pièces jointes malveillantes pour récupérer des informations.

liard d'euros supplémentaires à la cybersécurité à la suite des attaques de Dax et de Villefranche-sur-Saône.

« Encore trop souvent un dossier sur lequel on se penchera demain… »

David Rozier, cofondateur de Cybersecura.
Photo Cybersecura/Mélanie VERNOUX

David Rozier est cofondateur de Cybersecura, un cabinet d'études et accompagnement en cybersécurité, situé à Grenoble.

Avez-vous, depuis le début de la crise il y a presque un an, constaté une hausse des attaques ?

« On a tous constaté, y compris dans notre utilisation privée du numérique, une forte hausse des e-mails frauduleux, des tentatives de phishing (technique utilisée par des fraudeurs pour obtenir des renseignements personnels, NDLR). Si on prend un peu de recul, il faut être conscient que la question n'est plus : "quand sera-t-on la cible d'une attaque ?" mais "l'attaque va-t-elle réussir ?" »

L'an dernier, la plupart des entreprises ont basculé leurs salariés en télétravail. Étaient-elles prêtes ?

« Globalement, d'un point de vue cybersécurité, elles n'étaient pas préparées. Certaines ont demandé de l'aide mais c'était une minorité. Elles étaient en train de sauver les meubles, leurs trésoreries, de se questionner sur leur solvabilité pour les mois à venir. Ce n'est pas le moment qu'elles ont choisi pour investir dans la cybersécurité. La cybersécurité, c'est encore très souvent un travail, un dossier sur lequel on se penchera demain… »

Aucune entreprise n'est pourtant à l'abri…

« Aucune. Les cyberattaques d'espionnage international, pour dérober des secrets industriels, des brevets pourraient être, un peu plus, réservées à des grandes entreprises mais aujourd'hui, même une TPE peut avoir des secrets de fabrication à protéger. Les cyberattaques avec des rançongiciels, dont le nombre explose aujourd'hui et qui ont pour but d'extorquer des fonds, sont lancées de manière quasi-automatique. Toutes les entreprises peuvent donc être touchées. Les pirates ont même tendance à choisir les TPE/PME parce qu'ils savent qu'elles sont peu protégées. Aujourd'hui, le risque est connu par les entreprises mais dans 100 % des cas, il est sous-estimé. Elles sont sensibilisées mais ne comprennent pas, en profondeur, les mécanismes ».

Quel est l'investissement nécessaire pour une TPE/PME pour se protéger ?

« La plupart du temps, les entreprises ont déjà les outils numériques pour se protéger mais ils sont mal configurés, ils ne sont pas à jour, parfois ils ne sont simplement pas installés. C'est pourquoi nous croyons à un accompagnement par un référent dans la durée pour mettre en place les bons processus, réaliser quelques évolutions, accompagner tous les acteurs de l'entreprise, mettre en place une politique de sécurité du système d'information. On est là sur 8 000 à 10 000 euros par an ».

Que pensez-vous du plan cybersécurité dévoilé jeudi par le gouvernement ?

« L'aspect formation me semble intéressant même si ce n'est pas ce qui va régler les problèmes aujourd'hui. Le gouvernement parle de licornes du côté des éditeurs, de solutions pour les collectivités et les hôpitaux mais il n'y a rien pour aider les TPE/PME. Elles sont encore les grandes oubliées. Elles vont devoir se débrouiller par elles-mêmes, comme d'habitude. On les renvoie vers un guide des bonnes pratiques mais il contient des informations qui ne seront pas comprises par les décideurs ou pas appliqués par manque de moyens. Les TPE/PME attendaient un dispositif de financement de type chèque cybersécurité ».

Propos recueillis par Matthieu ESTRANGIN