RÉG

Votre supplément économie s'intéresse cette semaine aux entreprises sp

RHÔNE. C-Cure Systems parie sur le chiffrement

C'est dans les sous-sols d'une ancienne banque localisée dans la métropole lyonnaise, précisément dans la salle des coffres, que Stéphane Deguillaume et Jean-Frédéric Brun, les deux cofondateurs de C-Cure Systems (entreprise villeurbannaise de 6 salariés), une société experte en sécurité informatique et réseaux, opèrent, aujourd'hui, en toute discrétion pour des professionnels libéraux, des industriels, etc. Des clients qui veulent intégrer la cybersécurité dans leur stratégie pour qu'aucune information confidentielle, stratégique, ne puisse filtrer, et pour ne pas être des proies faciles pour les fameux pirates informatiques « qui usent d'une multiplicité de moulinettes devenues industrielles qui compilent chaque seconde, 24 heures sur 24, des millions de données », souligne Stéphane Deguillaume.

Stéphane Deguillaume et Jean-Frédéric Brun, les deux cofondateurs de C-Cure Systems, société experte en cybersécurité.
Photo Progrès/Stéphane GUIOCHON

« Le piratage est infini »

En quelques secondes, à peine, ce dernier parvient, pour faire une démonstration, avec une technicité digne d'un hacker, à craquer avec un simple email, les mots de passe de vos réseaux sociaux, les codes confidentiels de vos smartphones, etc. « Sans une extrême vigilance, de bonnes préconisations pour éviter les cyberattaques de tous types, le piratage est infini », souligne ce Centralien, diplômé des Mines, déjà à la tête d'une société informatique qu'il a créée il y a 20 ans, qui a décidé en 2018 avec Jean-Marc Brun, spécialisé dans le contrôle d'accès, de mettre ses compétences en commun pour s'orienter sur l'effervescent marché de la cybersécurité.

Des smartphones et des visio ultra-sécurisés

Un marché que les deux hommes ont abordé en s'appuyant sur une combinaison de systèmes de chiffrement qu'ils ont décliné sur la téléphonie et la visioconférence : « nous proposons des C-Cure phone, des téléphones inédits qui s'initialisent grâce à une suite de 24 mots que chaque client séquestre dans nos coffres. Ces 24 mots permettent de créer une phrase unique qui vous permet de vous identifier et de communiquer en toute sécurité, d'éviter par exemple l'espionnage industriel. Nos terminaux protègent l'ensemble de vos conversations téléphoniques, e-mail, sms, vidéoconférences. Le principe de nos C-Cure phone est de dégoogliser des téléphones Android. Nous réalisons ainsi un assemblage d'open source, avec la suppression de l'Android, puis le téléphone est chiffré via une combinaison de 24 mots issus de la blockchain. L'utilisateur peut communiquer en toute confidentialité sans être identifié. Les communications ne peuvent pas être interceptées, elles sont intraçables, ni géolocalisables. En effet, elles transitent par quatre serveurs disséminés géographiquement. Les échanges de données deviennent donc indétectables, de telle manière à ce qu'il n'y ait aucune faille », avance Stéphane Deguillaume. Une recette que les deux dirigeants ont dupliquée sur la visioconférence chiffrée ultra-sécurisée qu'ils proposent à façon « un serveur par entreprise ». Des dispositifs qui ont déjà convaincu disent-ils une centaine de clients disséminés dans toute l'Europe pour lesquels ils réalisent aujourd'hui des audits en mesurant l'exposition au risque Cyber, en identifiant les points faibles, en définissant les axes d'amélioration, un plan d'action Cyber, et en mettant en place de bonnes pratiques ainsi que les outils pour les suivre. Une offre de solutions qui leur aurait permis de faire bondir leur chiffre d'affaires -qu'ils se refusent à communiquer- avec une croissance à trois chiffres qui laisse augurer de belles perspectives pour l'avenir.

Franck BENSAID

LOIRE. La jeune boîte Serenicity veut apporter de la sérénité à ses clients

Serenicity est spécialisée dans la protection des TPE et des PME contre les attaques informatiques malveillantes et tous les risques liés au piratage de données.

Serenicity avait été créée il y a 3 ans sur l'idée des capteurs urbains de bruits anormaux. L'expérimentation devait être lancée à Saint-Etienne en 2019, mais devant la levée de boucliers et le recadrage de la CNIL, le sujet a finalement été mis de côté. La start-up - qui compte à son actionnariat un pool d'entrepreneurs locaux - a donc recentré ses efforts sur la cybersécurité. « Pour nos capteurs, nous avions mis au point une solution de sécurisation des serveurs innovante qui nous a permis de déposer cinq brevets », explique son directeur général, Fabrice Koszyk.

Un boîtier qui filtre les flux toxiques

L'un des outils développé s'appelle Detoxio : un boîtier « aussi facile à brancher qu'une box Internet » qui filtre les flux toxiques entrants et sortants dans l'ordinateur de l'utilisateur. « C'est du plug and play, très facile à installer. Nous visons principalement les TPE et les PME ». Le boîtier est associé à un logiciel traduisant par des symboles météorologiques la situation du jour du réseau de l'entreprise en matière de cybersécurité. Les boîtiers sont entièrement programmés à Saint-Etienne, mais pour l'instant fabriqués en Asie, une situation à laquelle Serenicity espère remédier sous deux à trois ans, en relocalisant cette production dans la région.

La start-up, qui compte cinq salariés, peut déjà se targuer de protéger une centaine d'entreprises, représentant 50 000 équipements informatiques. Serenicity a réalisé en 2020 un chiffre d'affaires de 100 000 euros et table sur 1 million sous trois ans.

Catherine RUSSIER

Pour Fabrice Koszyk, « aucune entreprise n'est à l'abri d'une cyber-attaque ». Photo Progrès/Stéphanie GALLO-TRIOULEYRE