Une entreprise protège gratuitement les hôpitaux contre les hackeurs

Ziwit, un des leaders français de la cybersécurité, a débloqué 15 millions d'euros pour aider les CHU.

DE NOTRE CORRESPONDANT
ALEXANDRE SEBA
À MONTPELLIER (HÉRAULT)

DES ARTICLES de presse du monde entier tapissent l'accueil du local montpelliérain. Et d'autres pourraient bientôt venir s'y ajouter : Ziwit, leader européen de la cybersécurité, a débloqué 15 millions d'euros (M€) pour protéger gratuitement les CHU victimes de cyberattaques. « Nous ne demandons rien en échange », répète Mohammed Boumediane, PDG de l'entreprise qu'il a fondée en 2011, à seulement 23 ans, et qui compte aujourd'hui parmi ses clients Google, Adobe, Sanofi... Et désormais plusieurs centres hospitaliers.

« Un système informatique qui est attaqué, c'est tout le système de soins qui s'arrête, explique-t-il. Et, indirectement, des gens en danger de mort à cause d'opérations annulées ou du manque de suivi. C'est presque une obligation pour nous d'essayer d'apporter des solutions. »

LP/ALEXANDRE SEBA

« Un système informatique qui est attaqué, c'est tout le système de soins qui s'arrête », explique Mohammed Boumediane, PDG de Ziwit.

En quelques jours seulement, l'entreprise a déjà reçu et traité une centaine de demandes d'intervention. Un besoin alarmant qui confirme « le désarroi et la détresse » des responsables de la sécurité informatique dans les CHU face à une menace croissante, constate Mohammed Boumediane. « Ils subissent bien plus qu'une attaque par semaine, affirme le spécialiste. Et sont démunis pour les stopper car ils manquent de moyens. » Face à l'urgence, le gouvernement a annoncé lundi le déblocage de 350 M€ pour renforcer la cybersécurité des hôpitaux.

« Donner du sens à notre action »

Profitant de leur vulnérabilité, les assaillants multiplient les assauts numériques : vols de données pour les revendre ou les échanger contre de la cryptomonnaie, redirection du système informatique vers un numéro surtaxé, demande de rançon... Le développement du télétravail, avec la mise en place de réseaux souvent mal sécurisés, facilite l'accès aux hackeurs.

Les actions malveillantes peuvent provenir de la France ou de l'étranger. Et être aussi bien menées en équipe que par un individu isolé. « Il n'y a pas de profil type du hackeur, souligne le patron de Ziwit. Il suffit d'une porte d'entrée mal verrouillée pour pénétrer un système et ouvrir ensuite d'autres portes. »

Quand un centre hospitalier est pris pour cible, les experts de Ziwit – dont l'effectif est tenu secret, comme tous les chiffres de l'entreprise, « pour éviter de donner des informations aux hackeurs » – analysent le parc informatique « afin d'éliminer rapidement les brèches et les failles de sécurité les plus critiques ». Si l'intervention nécessite un déplacement, celui-ci est aussi pris en charge par l'entreprise. Ces missions résultent d'une volonté personnelle de l'équipe. « Beaucoup d'entre nous ont été touchés depuis le début de la pandémie, confie M. Boumediane. J'ai moi-même perdu mon papa en novembre. »

Les 15 M€ engagés par Ziwit proviennent, en partie, du budget 2020 dédié aux déplacements et salons. « Nous aurions pu les reverser en dividendes mais nous préférons donner du sens à notre action, affirme le PDG. Nous estimons que c'est notre rôle plutôt que de rester les bras croisés face à cette crise. »