

# Depuis Montpellier, Ziwit lance une bouée de sauvetage aux CHU

## CYBERSÉCURITÉ

Il y a peu, les hôpitaux de Dax et Villefranche-sur-Saône ont subi des cyberattaques. Le groupe Ziwit (Montpellier) a offert aux CHU de France une protection gratuite.

**L**erisque pour les hôpitaux est grand. On est conscient qu'il y a un danger de mort à cause de ces cyberattaques, parce que refuser des admissions, ne pas pouvoir suivre les gens qui sont hospitalisés, c'est quelque chose de très critique», réagit Mohammed Boumediane. Ingénieur en sécurité de l'information et cryptologie, né à Meknès au Maroc en 1987, il a fondé sa société en 2011, après qu'elle ait été incubée à Montpellier. Aujourd'hui groupe spécialisé en cybersécurité, le siège social de Ziwit est situé dans cette ville. Ziwit compte 4 filiales à l'étranger, en Israël et aux États-Unis. « Nous sommes en contact régulier avec les services de sécurité informatique des hôpitaux. Il y a eu un cri d'alarme, une vraie détresse de leur part, car ils savent qu'ils sont vulnérables, et malheureusement ils manquent de moyens financiers. » Le 18 février, Mohammed Boumediane a proposé aux CHU de France de mettre à leur disposition, pour se protéger des cyberattaques, « nos moyens techniques



Mohammed Boumediane, PDG du groupe Ziwit, expert en cybersécurité, dont le siège social se trouve à Montpellier. PHOTO DR

sans aucune condition. On y consacre 15 millions d'euros. On leur lance une bouée de sauvetage». À ce jour, « on a reçu une centaine de demandes ».

### Hausse des cyberattaques

Cibles privilégiées des hackers\*, les hôpitaux français, depuis début 2021, subissent chaque semaine des cyberattaques. Celles-ci ont pour objectif de bloquer tout le système informatique, avec à la clé une demande de rançon. Les attaques informatiques ont été multipliées par 4 en France l'an dernier.

plique leur augmentation par « l'intensification du télétravail du fait de la pandémie. Ces systèmes pour se connecter depuis son domicile, conçus dans la précipitation, sont vulnérables. Les salariés en télétravail, d'après pas mal d'études, sont également moins vigilants. Du coup ils ouvrent des mails, cliquent sur des pièces jointes qui peuvent être des virus ».

Il observe : « On pense toujours que l'appât du gain guide les cyberattaques. Pas toujours. Parfois, des grandes entreprises sont infectées, cela fait des

milliers d'euros de factures de téléphonie, mais en réalité elles ne devraient pas. C'est dû au fait qu'un ou des pirates appellent des numéros surtaxés le soir sans qu'elles s'en doutent... »

Conscient des vulnérabilités françaises, le président Macron a présenté, le 18 février, un plan à 1 milliard d'euros d'ici à 2025 pour renforcer la cybersécurité du pays. « C'est un bon début, mais c'est très peu », assure le PDG de Ziwit.

Catherine Vingtrinier

## Cyber'Occ, un outil régional

La fuite de 500 000 données de patients clients de labos médicaux du Nord Ouest de la France à cause d'une cyberattaque, révélée le 24 février, fait une fois encore froid dans le dos. En Occitanie, la Région a confié à son agence de développement économique Ad'Occ, la mission de créer le Centre régional de cybersécurité, Cyber'Occ, « qui va aboutir courant 2021 », renseigne Caroline de Rubiana, chargée de mission. « Il s'agit d'accompagner les entreprises pour qu'elles sécurisent leur système informatique et les produits qu'elles développent. Comme en Occitanie, 98% du tissu d'entreprises emploie moins de 10 salariés, et se trouve démunie face aux cyberattaques, l'objectif est de les mettre en relation avec les bons interlocuteurs. Le portail Cyber'Occ apporte déjà des réponses. » Les autres missions seront « d'animer l'écosystème Cybersécurité, riche mais peu visible, en Occitanie. Et répondre aux besoins de la filière en matière d'innovation, de recherche de talents ». C.V.