

LE FIGARO·fr

FIGARO ECONOMIE Entreprises

Orange veut investir davantage dans la cybersécurité

Ingrid Vergara; ivergara@lefigaro.fr

787 mots

30 novembre 2022

Le Figaro

FIGARO

A

27

24346

Français

(c) Copyright 2022 Le Figaro.

Le groupe multiplie les acquisitions et vise les marchés de l'industrie et des PME.

SÉCURITÉ Le message est très clair. Développer ses activités dans la cybersécurité restera une des priorités stratégiques d'Orange. « Nous avons pris la décision d'investir des centaines de millions d'euros dans la cyber depuis plusieurs années. Je veux amplifier et poursuivre ces investissements », annonce Christel Heydemann, la nouvelle directrice générale de l'opérateur télécoms.

L'objectif : atteindre la taille critique pour s'imposer sur le marché en Europe. Avec son rythme actuel de croissance (entre 10 % et 15 % par an), Orange Cyberdefense (OCD), dont les activités sont filialisées depuis le mois de mai au sein d'une société holding, dépassera l'an prochain le milliard d'euros de chiffre d'affaires (après plus de 970 millions en 2022). Si elle se revendique leader en France et en Belgique, la société reste challenger sur les deux plus gros marchés cyber du Vieux Continent, le Royaume-Uni et l'Allemagne. Elle souhaite s'implanter en Espagne et en Italie.

Pour y parvenir, OCD va poursuivre sa politique d'acquisitions, au gré des opportunités. « Le marché de la cybersécurité reste un marché très fragmenté, avec plus de 3 500 acteurs dans le monde », rappelle la dirigeante. Orange a récemment acheté deux sociétés en Suisse, SCRT et Telsys, pour un montant qu'elle ne souhaite pas communiquer. Si la correction du secteur technologique n'a pas épargné les sociétés de cybersécurité, leurs valorisations restent à un niveau élevé, rendant la tâche plus ardue.

Pour accélérer sa croissance, Orange Cyberdefense mise aussi sur deux typologies de clients, particulièrement vulnérables aux attaques ces dernières années : les industriels et les PME. « La première cible parmi les victimes est de loin l'industrie manufacturière, car c'est aujourd'hui beaucoup plus simple d'attaquer un industriel » explique Hugues Foulon, le PDG d'Orange Cyberdefense. Jusqu'à une période récente, les systèmes informatiques industriels étaient des environnements fermés et donc protégés des attaques.

La digitalisation des chaînes de production a totalement changé la donne en matière de sécurité. Avec l'hyperconnectivité des usines 4.0, il est possible pour un pirate informatique d'atteindre le « cerveau central » des infrastructures industrielles via, par exemple, un système de climatisation et de bloquer ou de désorganiser l'ensemble d'un processus. Les cas d'attaques avec de très graves conséquences sont encore peu connus, mais en 2021, aux États-Unis, un pirate informatique a pu s'introduire dans la station de traitement des eaux d'une ville de Floride et modifier à distance les concentrations de soude caustique utilisées pour réguler l'acidité de l'eau.

« La plupart des projets pour l'industrie 4.0 n'intègrent pas de compétences cyber. Le sujet n'est pas encore pris à la bonne hauteur par les entreprises », regrette Fabrice Mourron, le directeur du Centre national technique dédié à la cybersécurité industrielle d'OCD. Outre des solutions « sur mesure » pour ses grands clients, Orange Cyberdefense espère séduire un maximum de PME avec une solution plus standard et abordable, sorte de « bouclier digital » répondant à leurs principaux besoins, à commencer par un audit de leur sécurité. « 60 % des PME subissant une cyberattaque déposent le bilan sous dix-huit mois » indique Hugues Foulon. La société s'appuie sur les synergies avec sa branche services aux entreprises (OBS) et le réseau de distribution de l'opérateur télécoms, qui lui permet aussi d'être bien positionné pour adresser le marché grand public.

Des enjeux de souveraineté

« Nous sommes un opérateur de confiance et nous maîtrisons toute la chaîne de sécurité, des câbles sous-marins aux centres de données » insiste Christel Heydemann. Sur un marché mondial dominé à 90 % par des logiciels de sécurité américains et israéliens, les enjeux de souveraineté ont aussi leur importance.

La nouvelle direction d'Orange, qui détaillera son plan stratégique le 26 février prochain, reste très ouverte sur la façon dont elle va donner les moyens de son ambition industrielle à sa pépite cyber. Tous les scénarios restent sur la table. Introduction en Bourse d'Orange Cyberdefense si les conditions de marché le permettent, ouverture du capital à des partenaires... « La vraie question est surtout : que veut-on faire ? Insiste Christel Heydemann. Ce type d'opération doit être un moyen d'appuyer la croissance d'Orange Cyberdefense. Ce n'est pas le besoin d'aujourd'hui. » À court terme, ses besoins sont de recruter des ressources humaines pour accompagner son développement. Dans un marché de compétences disponibles très tendu, OCD prévoit d'embaucher 600 personnes en 2023, pour renforcer son effectif actuel de 2 700 experts.

1012.0.480415128

Document FIGARO0020221130eibu0002s