TRIBUNE BULLETIN CÔTE D'AZUR
n° 1125 du vendredi 3 décembre 2021

FOCUS. HUGUES FOULON PDG d'Orange Cyberdefense, membre du comité exécutif du groupe Orange, responsable de la stratégie

"La cybersécurité est devenue une priorité absolue pour le groupe Orange"

Il est intervenu sur cette thématique ultra-sensible aux dernières Entreprenariales. Son message est clair : aucune structure, aujourd'hui, n'est à l'abri d'une cyber-attaque. Pourtant, des solutions existent.

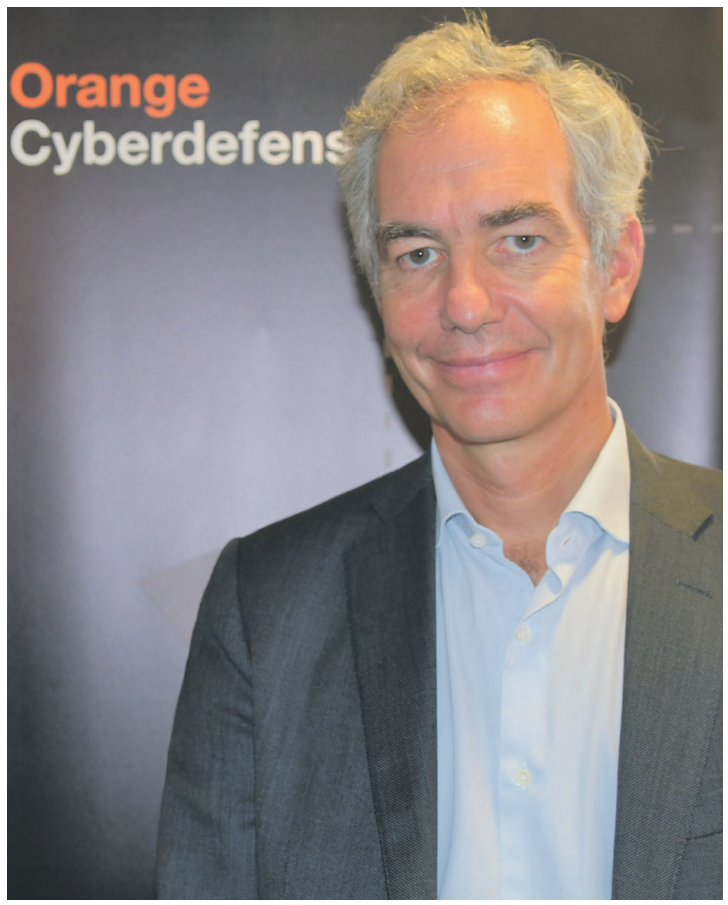
Orange Cyberdefense ?
Une filiale du groupe Orange, créée en 2014, chargée de proposer des solutions aux entreprises. En transportant et en stockant les données de nos clients -et de nos salariés-, nous avons bien sûr été nous-mêmes attaqués, très tôt. Il fallait se protéger de cette menace. Aujourd'hui 2.500 collaborateurs s'y emploient, dont 1.200 en France et 55 en région Sud, à Marseille. Avec deux centres principaux, en Ile-de-France et dans la région de Rennes.

Leur rôle ?
Tout dépend des besoins du client, chaque situation est particulière. Mais notre spécificité, c'est que, de l'amont à l'aval, Orange Cyberdefense veut répondre à l'ensemble de ses besoins en termes de cybersécurité. En amont, nous sommes capables d'anticiper les éventuelles failles, de rendre un avis éclairé sur la menace potentielle d'attaque en détectant les faiblesses des systèmes informatiques de nos clients, tout en assurant une veille pointue pour caractériser les nouvelles pratiques criminelles et ainsi adapter nos solutions de protection. On peut donc protéger, en sécurisant, on peut aussi détecter les intrusions éventuelles, même si elles ne sont pas repérées, et puis surtout, en aval, on intervient en situation de crise, en réparant les systèmes victimes d'attaques. De l'anticipation à la réaction, nous avons des solutions. On ne le répètera jamais assez, mais aucun système n'est infaillible, et la cybercriminalité est malheureusement une activité lucrative. Même les grands groupes n'hésitent pas à co-construire leur solution avec nous, nous nous adaptons dans ce cas à leurs process.

Les entreprises, notamment les TPE-PME, ont-elles conscience des dangers encourus ?
Le problème de la cybercriminalité, c'est que par définition, c'est abstrait, immatériel... Deux chiffres cependant me semblent intéressants du côté des petites entreprises : les ransomwares (*les pirates demandent une rançon en échange de la restitution de l'accès ou du déchiffrement des fichiers, ndlr*) ont été multipliés par quatre entre 2019 et 2020. Et la tendance est toujours à l'accélération. Si on cumule tous les coûts des cyber-attaques à l'échelle internationale, on atteint presque le PIB de la Chine, deuxième puissance économique du monde... On voit mieux l'ampleur des montants en jeu.

Cette cyber-menace permanente ne constitue-t-elle pas un frein à la digitalisation des petites structures ?
Je pense plutôt que nous terminons une phase que l'on pourrait qualifier de... naïveté envers internet et le digital. Mais des risques, on en prend tous les jours, en voiture, en société, en matière sanitaire, c'est quelque part un juste retour des choses que le monde digital ne soit pas exempt de menaces. Et comme dans la vie, il y a des règles d'hygiène à respecter. On ne part pas de chez soi en laissant la porte ouverte... Malheureusement, dans le monde digital, ce genre de comportements existe. La plupart du temps, l'attaque est le fruit d'une négligence individuelle, laisser son téléphone non verrouillé, choisir des mots de passe trop simples, ne jamais changer ses codes d'accès ou les reproduire sur l'ensemble du matériel utilisé.

Un avant et un après-Covid en matière de cybercriminalité ?
Pas tant que ça... La menace était déjà en croissance forte avant que les habitudes de travail ne soient perturbées par les confinements notamment. Et elle est toujours très forte. En revanche, le Covid a introduit, c'est vrai, un désordre dans le mode de fonctionnement général des entreprises. Les nouvelles habitudes ont créé de nouvelles opportunités pour les cybercriminels, je pense notamment au phishing. Deuxième phénomène, le Covid a momentanément -mais sans doute durablement- accéléré la digitalisation de nos façons de faire, dans la vie personnelle comme dans la vie professionnelle. Là-encore, cela crée de nouvelles opportunités pour les hackers, plus nombreuses. Qui n'a jamais utilisé sa tablette, son ordinateur, son téléphone professionnel pour un usage personnel, même éphémère, une commande,



une réservation ? Les frontières ne sont plus aussi rigides qu'auparavant.

Y a-t-il des tendances en matière de cybercriminalité?
Les modes opératoires sont extrêmement nombreux. Le ransomware est le plus courant, mais il peut aussi y avoir le vol de données. Ça n'est pas forcément public, mais des entreprises françaises se sont fait voler des brevets, exploités quelques mois plus tard par des unités chinoises beaucoup plus compétitives... Sans compter les tentatives de déstabilisation. En matière de cyber, tous les coups sont permis.

PROPOS RECUEILLIS PAR ISABELLE AUZIAS

Ransomwares : faut-il payer ?

● "*On ne vend pas un forfait cyber tout compris, tout dépend de la typologie de l'entreprise, de ses besoins en termes de sécurité informatique.*" De l'audit de conformité avec identification des risques et test des systèmes de protection déjà en vigueur à des accès hyper-sécurisés, cloud compris, la palette de solutions est immense."*Pendant la crise Covid, nous avons eu beaucoup de demandes émanant de centres hospitaliers, pour réagir en urgence à divers incidents. Notre mission, c'est alors de contenir l'attaque au maximum, avec des systèmes d'isolement notamment*." Parmi ces incidents, les fameux ransomwares, que Hugues Foulon recommande de ne pas payer. "*Il y a des solutions de reconstruction, de récupération pour que l'entreprise retrouve un régime de fonctionnement normal rapidement*."
Derrière l'attaque ? Difficile de remonter le fil. "*Le hacker n'est plus le jeune geek dans son garage, il officie aujourd'hui en bande organisée, en mode challenge, en cherchant l'exploit. Ou il fonctionne en véritable mafia, avec pour seul objectif un retour sur investissement le plus important possible, via le racket. Troisième typologie, que nous avons déjà détectée, les organismes étatiques ou para-étatiques, hébergés par certains Etats. Là, le but, c'est la déstabilisation*." D'où le besoin constant d'améliorer les différents moyens de protection, en se calquant sur les pratiques criminelles. Et d'où l'importance de l'ANSSI (Agence nationale de la sécurité des systèmes d'information), chargée de favoriser la transmission des informations liées aux cyber-attaques et d'organiser la sensibilisation, la veille, pour tout le réseau de "résistants". "*Dans ce réseau, Orange, acteur historique des communications, dans le Top 5 européen, est par nature bien implanté. Et informé.*"
Sur un marché de la cyberdéfense en croissance de 9 à 10% par an.