

Flash 

IKEA Nice Saint-Isidore : ouverture le 11 mai 2022 (/article/ikea-nice-saint-isidore-ouverture-le-11-mai-2022)  Philip 
(/artic

 (https://twitter.com/webtimemedias)

 (https://facebook.com/webtimemedias)

 (https://instagram.com/webtimemedias)

 (https://www.linkedin.com/company/webtime-medias/)

Cybersécurité : la question n'est plus de savoir quand on sera attaqué

 jeu 09/12/2021 - 09:52  Jean-Pierre Largillet (/user-profile/jean-pierre-largillet)

Invité aux dernières Entrepreneariales à Nice, Hugues Foulon, Pdg d'Orange Cyberdefense, a rappelé que la menace concernait aujourd'hui les entreprises de toutes tailles, du grand groupe à l'artisan. Pour lui, la question n'est plus de savoir "quand on sera attaqué" mais "comment se protéger de ces cyberattaques".



Pourquoi les entreprises se doivent de mettre aujourd'hui l'accent sur la cybersécurité ? **Hugues Foulon**, Pdg d'Orange Cyberdefense, est venu l'expliquer fin novembre aux Entrepreneariales, rendez-vous des entreprises de la Côte d'Azur qui avait pris pour thème cette année la transition numérique. Pour lui, la question n'est plus de savoir "quand sera-t-on attaqué ?" mais "comment se protéger de ces cyberattaques ?". (Photo WTM : Hugues Foulon -à droite- à la tribune en compagnie de Bernard Kleynoff, président de Rising SUD, lors de la conférence donnée aux Entrepreneariales 2021).

Car aujourd'hui, phénomène accéléré par la crise sanitaire et la marche forcée vers la digitalisation, les grands groupes ne sont plus les seuls principalement concernés. Désormais et plus que jamais, toutes les entreprises, PME, TPE, artisans, professions libérales le sont. Selon le Club des Experts de la Sécurité de l'Information et du Numérique, en 2020, plus d'une entreprise sur deux aurait été victime d'une cyberattaque. Et selon une autre étude de l'ONU de 2020, 60% des PME attaquées ont déposé le bilan dans les six mois. Un risque qui est donc bien réel et lourd de conséquences.

"Filiale d'Orange, Orange Cyberdefense (1.200 personnes au niveau national, plus d'une cinquantaine en Région PACA) a aussi pour objectif de faire face à ce risque", explique **Hugues Foulon**. "Nous nous chargeons d'aider les entreprises à identifier la menace, à s'en protéger et éventuellement, s'il y a une attaque, à réagir et à réparer leur système. Nous pouvons intervenir en amont comme en aval. En amont sur un format d'audit pour analyser les systèmes informatiques, repérer leurs fragilités, s'assurer de leurs protections. Nous pouvons

aussi agir en renforçant la protection avec des systèmes comme des fire-walls, ou en détectant les attaques. En aval, quand l'attaque est arrivée, nous pouvons également intervenir pour contenir cette attaque, réduire son impact et restaurer le système afin de revenir dans un régime opérationnel."

"Nos interventions suivent un format "sur-mesure". Notamment, nos techniciens proposent des solutions adaptées à la taille de l'entreprise. Un grand groupe du CAC 40 avec des milliers de postes informatiques, n'a évidemment pas les mêmes besoins qu'une PME azurienne avec une dizaine de postes. Donc nous savons proposer des solutions adaptées à la taille de l'entreprise."

"Quant au nombre d'attaques, il est en forte croissance. Ainsi les ransomwares, les demandes de rançons avec cryptage, ont été multipliées par quatre l'an dernier et elles se sont de nouveau multipliées cette année. Il en a été beaucoup question dans les hôpitaux ces derniers temps parce que nous nous trouvons en pleine crise sanitaire. Mais ce type d'attaques s'est intensifié dans tous les secteurs économiques, transports, énergie, télécoms, banques... Dès qu'il y a un levier possible pour gagner de l'argent facilement, les entreprises se font attaquer..."

(/ #facebook) (/ #twitter) (/ #linkedin)
(/ #email)

AJOUTER UN COMMENTAIRE

Votre nom
Objet
Commentaire *
 À propos des formats de texte (/filter/tips)