Courir après le wagon étranger du cloud et des logiciels cyber me semble ridicule.

Avertissement *: Souveraine Tech revendique par vocation une approche transpartisane. Seule nous oblige la défense des intérêts supérieurs de notre pays. Nous proposons ainsi un lieu de « disputatio » ouvert aux grandes figures actives de tous horizons. La parole y est naturellement libre et n'engage que ceux qui la prennent ici. Cependant, nous sommes bien conscients des enjeux en présence, et peu dupes des habiles moyens d'influence plus ou moins visibles parfois mis en œuvre, et dont tout un chacun peut faire l'objet, ici comme ailleurs. Nous tenons la capacité de discernement de notre lectorat en une telle estime que nous le laissons seul juge de l'adéquation entre le dire et l'agir de nos invités.*

Vendredi 7 juin 2024

Hugues Foulon est directeur exécutif d'Orange et CEO d'Orange Cyberdéfense

1/ Quelle différence faites-vous entre « cyberdéfense » et « cybersécurité » ?

Dans les acceptions traditionnelles, la cyberdéfense recouvre plutôt ce qui est du ressort de la défense nationale – d'une forme de mission de service public. La défense est dynamique, évolutive en mesure de protéger et de riposter, quand la sécurité est statique.

Adosser le terme Cyberdefense à l'opérateur Orange pour représenter nos couleurs est un choix fort et réfléchi qui témoigne de notre capacité à accompagner de manière exhaustive nos clients. Orange Cyberdéfense est un acteur cyber à 360° capable d'adresser l'ensemble de la *kill chain* et d'évoluer au rythme de la menace.

Chez Orange Cyberdefense nous n'avons que des solutions de défense, sauf sur un domaine d'activités précis : le pentesting. Il s'agit d'attaquer – à la demande du client – la sécurité informatique d'un périmètre donné afin de tester sa résistance et atteindre différentes cibles, différentes missions ; de l'arrêt d'une usine à l'infiltration dans les boites mail de membres du comité exécutif.

2/ A quels facteurs attribuez-vous le déchainement « aveugle » de la cybercriminalité ?

En premier lieu, l'appât du gain et le retour sur investissement. L'argent facile est dans ce domaine intrinsèquement lié au manque d'hygiène numérique des citoyens. Imaginez un instant l'explosion du nombre de cambriolages si 1 habitant sur 2 ne fermait pas à double tour la porte de sa maison en quittant son domicile, laissait trainer son double de clé dans le jardin ou une fenêtre mal fermée à l'étage. Ce même appât du gain rend le cyberattaquant susceptible d'attaquer une cible vulnérable et donc de plus en plus les petites entreprises ou les particuliers.

Ensuite, l'instabilité géopolitique renforce l'accélération et la complexification de la menace en cybersécurité. Nous observons (dans le rapport annuel d'Orange Cyberdefense, Security Navigator 2024) l'émergence d'une tendance autour de l'hacktivisme qui vise particulièrement l'Europe.

Le rapport à l'argent et les conflits internationaux sont à l'origine de bien des maux dans nos sociétés modernes ; la cybercriminalité n'y échappe pas.

3/ Notre arsenal juridique vous paraît-il suffisamment dissuasif en la matière ?

L'arsenal juridique tout comme l'arsenal règlementaire sont renforcés au sein des pays européens et doivent venir en soutien d'acteurs privés forts et en capacité d'innover et se développer. Le propre de nos démocraties est d'avoir la capacité de nous doter d'outils parfois puissants, souvent dissuasifs pour accompagner des bouleversements de société

Mais au-delà des arsenaux juridiques et règlementaires, l'Europe doit aussi être en mesure de stimuler son tissu d'acteurs privés sous peine de rester au ban des économies mondiales, spectateur des entreprises *tech* américaines ou chinoises. La comparaison au monde physique est toujours édifiante : espère-t-on que l'arsenal juridique suffise à réduire cambriolages, vols et autres infractions ou délits ?

Par ailleurs, l'arsenal juridique européen bute sur la virtualisation des attaques et des preuves ainsi que sur la domiciliation des cybercriminels dans des pays inaccessibles par nos tribunaux sans une coopération internationale forte et volontariste.

4/ Comment évaluez-vous le degré de coopération internationale face à ce fléau universel ?

Comme mentionné auparavant, la coopération internationale est nécessaire pour faire face au risque en cybersécurité. Nous notons des lacunes sur notre capacité à interpeller des cybercriminels et l'arsenal juridique gagnerait à être étendu et partagé à l'échelle mondiale.

Au-delà des Etats et institutions internationales cherchant à renforcer leur collaboration stratégique en matière de cybersécurité, l'écosystème bénéficie d'une coopération naturelle entre experts, observateurs avertis, *aficionados* ou héros sans cape : l'alliance du bien contre le mal. La connaissance de la menace est ainsi bénévolement partagée sur

des réseaux de connaisseurs palliant le manque actuel de coopération institutionnalisée.

5/ Nous avons coutume de dire ici que la moitié de l'économie mondiale sera bientôt dévolue à la sécurisation de l'autre ? Qu'est-ce que cela dit des temps que nous vivons et particulièrement du progrès que nous pensons avoir manifesté ?

L'augmentation inexorable et nécessaire des dépenses en matière de sécurité (informatique notamment) traduit un monde qui se conflictualise et se digitalise. Les surfaces d'attaques ne font que grandir, de même que les motifs pour attaquer son adversaire, historique ou de circonstance. Nos sociétés ont longtemps conféré au monde digital une confiance dont il n'est historiquement pas digne. Les investissements vont continuer car le « *Secured by design* » est encore loin d'être la norme.

Néanmoins, les progrès technologiques notamment de l'Intelligence Artificielle devraient venir diminuer le poids des dépenses dévolue à la sécurisation et concourir à des gains de productivité, d'efficacité et mise à l'échelle de la sécurisation.

6/ Auriez-vous en tête une métaphore qui nous permette de comprendre votre vision des modalités nécessaires de protection de nos économies, à l'échelle nationale et à l'échelle communautaire ?

Dans le milieu de la cybersécurité, il n'y a ni ami, ni allié. Tout en construisant une coopération internationale, il est important d'avancer en cavalier seul avec une autonomie stratégique aux bornes européennes ou nationales selon la criticité et la nature des sujets.

7/ On entend parfois que la souveraineté, ce serait « le repli sur soi » (sic), mais l'idée alternative de

l'autonomie stratégique selon laquelle nous devrions « choisir nos dépendances » ne vous semble-t-elle pas friser l'oxymore ?

Les mots totem de « souveraineté » ou « autonomie stratégique » recouvrent chacun un vœu pieu à ce stade de l'Histoire technologique.

Il faut sortir de la naïveté et pousser pour une souveraineté pragmatique, une autonomie stratégique à géométrie variable. Les clouds souverains à l'instar du projet Bleu en sont l'incarnation.

Cela ne doit pas nous empêcher d'investir dans les secteurs d'avenir et de monter dans le train des prochaines évolutions technologiques avant qu'il ne soit trop tard. Mais courir après le wagon étranger du cloud et des logiciels cyber me semble ridicule. Utilisons avec raison les technologies aujourd'hui sur le marché (en cybersécurité, à 99% américaines ou israéliennes) et soyons intransigeants sur nos conditions de partenariat.

Comparaison ne vaut pas toujours raison mais le développement du nucléaire civil en France est illustratif d'une politique industrielle efficace et pragmatique. Dans l'après-guerre, Westinghouse devient le fer de lance de la stratégie américaine pour développer l'énergie nucléaire dans le pays et à l'international. Dans un domaine hautement stratégique, la France se dote donc d'équipements américains, les meilleurs du marché alors.

Aujourd'hui, la France s'est hissée en nation leader en la matière et est dotée d'une filière robuste et réputée mondialement. Le même chemin pourrait être pris par la technologie et particulièrement la cybersécurité.

8/ Observez-vous des aspects de service public dans votre entreprise, qui est une des multiples expressions

de l’ « opérateur historique « ?

Nous pouvons les observer à 3 niveaux.

Dans la protection des actifs critiques propres d’Orange, pour les besoins internes du Groupe. Cela nous amène à protéger les activités de l’opérateur historique et leader mondial des télécommunications, notamment lors d’évènements mondiaux comme les Jeux Olympiques.

Dans notre capacité à offrir des services innovants à nos clients et à tous les Français comme très récemment le lancement d’un portail de levée de doutes en France (Orange Cybersecure) accessibles gratuitement afin d’accompagner les citoyens dans la quête d’une meilleure hygiène numérique. L’enjeu est de ne plus se faire piéger par un mail douteux ou un SMS frauduleux et subir les conséquences financières désastreuses d’une opération de phishing.

Enfin dans les solutions de souveraineté et la proximité de nos équipes que nous proposons à nos clients face à une certaine concurrence encline à proposer de plus en plus des modèles opérationnels localisés dans des pays à bas coûts. Les clients les plus critiques nous font confiance partout dans le monde : les Ministères français, la police belge, un aéroport à Amsterdam ou des hôpitaux suèdois.

9/ A côté de la question de la « commande publique », se trouve celle, non moins importante, de la « commande privée ». Dans quelle mesure soutenez-vous par la commande confiante auprès des acteurs de l’écosystème numérique français ?

Orange Cyberdefense travaille depuis toujours avec l’écosystème cyber français : des startups adressant un nouveau domaine comme Stoik avec l’assurance en cybersécurité, le tissu académique avec des nouvelles écoles spécialisées comme Oteria ou des institutions déjà bien installées ainsi que les fournisseurs de logiciel.

Mais le soutien de l'écosystème de la cybersécurité par les géants du privé ne suffit pas. Cela pose la question du passage à l'échelle, de l'acceptation de l'échec et du risque et des modalités de financements aujourd'hui faibles en Europe, relativement à nos pairs américains et chinois.

10/ Vous êtes passé par Polytechnique, dont la devise est « « Pour la Patrie, les Sciences et la Gloire » et aussi par l'IHEDN. Dans quelle mesure ces deux expériences imprègnent-elles vos actuelles fonctions ?

J'ai la chance d'occuper aujourd'hui une position à la confluence d'appétences personnelles et professionnelles. La cybersécurité recouvre de forts enjeux technologiques, une proximité avec le monde de la défense nationale et des enjeux géopolitiques internationaux, au cœur d'une entreprise avec une mission de service public encore puissante, tout en étant un domaine en pleine croissance et crucial pour l'avenir de nos sociétés. Orange Cyberdefense est une tour de contrôle, un observatoire passionnant et riche de l'évolution du paysage de la cybersécurité. Le pari d'Orange, acteur de confiance historique, d'investir massivement dans la cybersécurité était audacieux mais porte aujourd'hui ses fruits. Mes valeurs patriotiques et scientifiques sont comblées dans cette aventure professionnelle. Pour la Gloire, je laisserai le commentaire à d'autres.