FACE À LA COMPLEXITÉ DES ENJEUX DE SÉCURITÉ, un accompagnement nécessaire

Dotée d'une solide expérience en matière de cybersécurité, la société *ADVENS* considère que l'élargissement de la surface d'attaque rebat les cartes pour les organisations qui doivent se protéger : les solutions techniques existent, à condition de prendre la mesure des enjeux. Entretien avec *Benjamin Leroux, directeur marketing et responsable sécurité.*

Benjamin Leroux

Bio express
Après avoir obtenu un diplôme d'ingénieur chez Télécom SudParis, Benjamin Leroux a toujours travaillé dans la cybersécurité, notamment comme consultant. Il est aujourd'hui directeur marketing et responsable sécurité chez ADVENS.

Pouvez-vous présenter votre cœur de métier, votre activité ?
Advens est un pure player de la cybersécurité : c'est notre seul métier. En tant que société de service, nous accompagnons des clients de tout secteur d'activité pour les aider à définir une politique de sécurité, et surtout à l'animer au quotidien. Nous proposons toute une gamme de solutions qui vont de l'accompagnement des responsables sécurité dans leur politique de sécurité jusqu'au management de leur cybersécurité au quotidien en mode as a service : détecter un incident de sécurité, trouver une réponse en cas d'incident, mettre en œuvre des logiciels de protection et de mise en conformité.

"La cybersécurité doit devenir un levier d'accélération du numérique en entreprises en redonnant de la visibilité et de la maîtrise sur les réseaux informatiques."

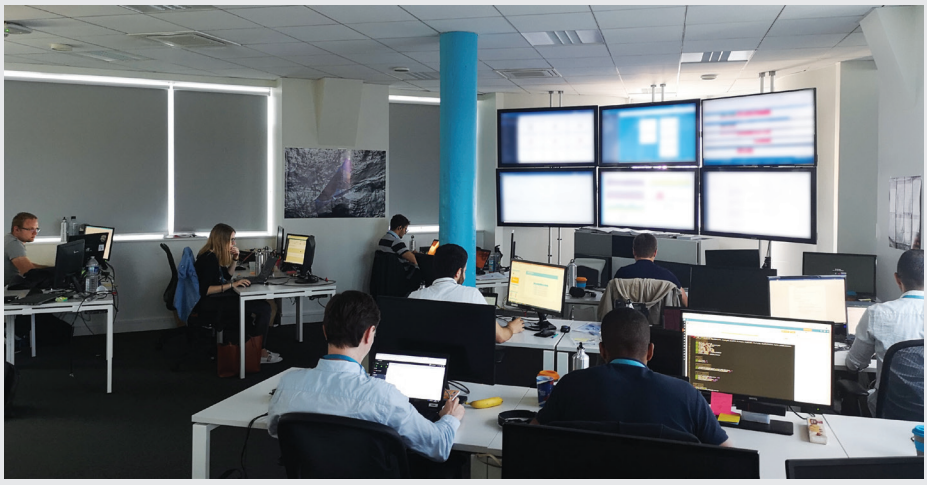
L'objectif est de pouvoir aider l'organisation sur toutes les facettes de sa cybersécurité : il y a donc des sujets extrêmement techniques comme des sujets plus organisationnels autour des métiers, des processus dans l'organisation.
Notre credo, c'est d'avoir un message optimiste vis-à-vis de la cybersécurité. Il y a souvent un marketing de la peur dans ce domaine. Notre approche se veut rassurante : les mesures à prendre et les solutions existent. Le plus difficile, c'est d'orchestrer, de faire un pas après l'autre et d'avancer. Nous sommes justement là pour cela. La cybersécurité doit devenir un levier d'accélération du numérique en entreprises en redonnant de la visibilité et de la maîtrise sur les réseaux informatiques. Car aujourd'hui, la Cyber reste encore trop perçue comme un élément bloquant le lancement de nouveaux services.

La flexibilité et la capacité d'adaptation sont-elles importantes pour vous ?
C'est même le cœur de notre activité. Nous proposons à nos clients de déployer un processus de protection de bout en bout pour leur simplifier le casse-tête de la cybersécurité. Cela s'appuie sur une approche « centre de service » qui englobe tous les savoir-faire en matière de sécurité (RSSI délégué, SOC externalisé, réaction en cas d'incident). Ce centre de service s'appuie sur un catalogue de services riche, que nos experts sont capables de décliner en fonction des risques et du métier de nos clients. Nous enrichissons également cela via la prise en compte des vulnérabilités et de nouvelles méthodes d'attaques propres à un secteur d'activité donnée. La sécurité s'en trouve simplifiée, sans pour autant être réduite à des généralités.

Selon vous, qu'est-ce qui a changé récemment dans l'évolution des menaces proprement dites ?
Les attaquants sont devenus des professionnels. Ce n'est plus le cliché du jeune qui bidouille sur son ordinateur et veut percer un système pour impressionner ses copains. C'est tout un écosystème très organisé avec des groupes d'attaquants extrêmement bien outillés et professionnalisés. Il y a ceux qui volent des données, d'autres qui ouvrent les portes d'entrée des systèmes, etc. Ce qui fait que nous avons une menace intense, professionnelle et très efficace.

Face à ces menaces, quel est l'élément clé pour une organisation selon vous ?
Un des premiers éléments est la prise de conscience. Il y encore trop d'organisations qui considèrent que la cybersécurité est un sujet d'informaticiens exclusivement, très technique, et croient régler le problème avec un logiciel. C'est une erreur. La cybersécurité est une problématique qui doit être à l'agenda des

décideurs, pas simplement du directeur informatique, mais du top management.
L'autre élément, c'est de comprendre ce qu'on est capable de faire soi-même et ce que l'on doit externaliser, là où il faut s'appuyer sur des professionnels. Par exemple, une de nos activités consiste à créer un système de surveillance, à placer des capteurs dans les systèmes d'informations des clients pour analyser et détecter les problèmes. Il y a trop de sujets, d'expertises, de processus, de technologies à maîtriser. Ainsi la seule approche qui permette à une organisation de mettre sa défense au niveau de professionnalisation des attaquants, c'est de s'appuyer sur l'intelligence collective en apprenant des autres et sur l'intelligence artificielle (IA) pour détecter plus rapidement des comportements menaçants. C'est l'approche même que nous suivons au quotidien. Cela nous permet de proposer une approche pré-packagée, clé en main, qui adresse toutes les facettes de la Cyber. Plusieurs technologies récentes sont venues enrichir les dispositifs de sécurité des entreprises. Opérées dans le cloud et mutualisées sur plusieurs clients, elles favorisent le développement et l'entretien de cette intelligence collective (EDR, XDR, NDR). Advens s'est spécialisé sur les 5 dernières années dans l'implémentation et la gestion de ces solutions avec une approche pré-packagées. Le résultat étant une optimisation des budgets Cyber avec une couverture des risques propres à chaque organisation.



Un des challenges que vous voyez dans votre secteur est de faire en sorte que de plus en plus d'entreprises - y compris de petite taille - comprennent l'importance du sujet et qu'elles ne peuvent pas le gérer seules. Voyez-vous d'autres éléments dans vos perspectives de développement ?
Un autre élément que nous voyons est le fait que la surface d'attaque, c'est-à-dire l'ensemble des périmètres à protéger, est de plus en plus important. Prenons le cas d'un industriel, une société avec des usines, des hangars ou des entrepôts. Historiquement, on avait tendance à ne s'intéresser qu'à la sécurité des ordinateurs de bureaux. Or, de plus en plus, les machines dans les usines sont aussi la cible d'attaques, notamment parce que ce sont des systèmes qui sont interconnectés à internet. De la même manière, les objets connectés, les appareils biomédicaux dans la santé, les capteurs, bien d'autre éléments encore sont exposés à la menace. Nous avons donc des périmètres de plus en plus variés à protéger. Il est important que l'organisation prenne la juste mesure de ce périmètre pour ne rien oublier. Dans le cas d'une usine, la panne d'un ordinateur d'un poste de gestion peut avoir moins d'impact que l'arrêt d'une machine qui peut bloquer toute une chaîne de production. Il faut donc avoir une vision globale du problème. Et sur un groupe qui a des filiales, l'approche doit évidemment être internationale.

Je suppose que ces évolutions se répercutent aussi sur votre recrutement et que vous recherchez des compétences un peu différentes qu'auparavant ?
Tout à fait. De manière générale, il y a un énorme déficit de compétences en matière de cyber. Il n'y a pas assez de profils sur le marché, en France et même dans le monde. En milieu d'année, nous aurions dû avoir 60 personnes, nous en avons 80 à cause de notre activité croissante : il y a donc une forte demande.
Et, d'autre part, il faut varier les profils. Pour faire suite à ce que j'ai dit précédemment, nous avons par exemple recruté des personnels qui viennent du monde des automatismes, de l'industrie, et non du monde de la cyber. Nous avons également recruté des juristes pour faire face à toute la dimension réglementaire des métiers - la conformité vis-à-vis de textes de loi qui ont des exigences cyber. Il faut vraiment avoir une vision large du problème et donc trouver des ressources. Sur ce sujet, Advens a d'ailleurs pris une initiative forte. Nous avons créé cet été un fonds de dotation pour permettre des projets à impact. Advens a offert le nom et la visibilité de son voilier de hautetechnologie à LinkedOut, une association qui favorise le retour à l'emploi. Nous pensons que la réponse à cette pénurie, pas nécessairement pour trouver les expertises les plus poussées, mais pour avoir des forces de frappe, c'est d'utiliser les mécanismes en place pour favoriser le retour à l'emploi des jeunes qui se sont un peu éloignés du cadre, pour leur donner une deuxième chance, et en faire de futurs spécialistes de la cyber. Nous souhaitons qu'ils soient demain du côté des défenseurs plutôt que des attaquants. Nous avons donc lancé plusieurs actions grâce au fonds de dotation pour réfléchir à ces actions de sensibilisation et aller jusqu'à l'intégration et l'inclusion.

EN BREF

Fondée en l'an 2000, employant 300 salariés, ADVENS est le premier pure player français de la cybersécurité.