LA CYBERSÉCURITÉ est l'affaire de tous

Rencontre avec Nicolas Aubé (93), fondateur et CEO de CELESTE et Simon Fabre, responsable commercial de NBS System. Ils partagent avec nous leur vision des principales tendances qui se dessinent sur le marché de la cybersécurité ces dernières années et nous en disent davantage sur leur offre orientée vers la sécurité offensive.

Nicolas Aubé (93)

Simon Fabre

Quelles sont les tendances qui ont marqué votre secteur au cours des dernières décennies ?

Nicolas Aubé : Nous vivons une révolution numérique. Les entreprises sont de plus en plus connectées notamment en termes de flux télécoms et d'informations. Nous constatons une augmentation des flux de 50 % par an chez nos clients. Les Français (et le monde entier d'ailleurs), sont tous en train de s'équiper en fibre optique. Et 100 % des entreprises le seront bientôt.

D'ailleurs, nous entendons de plus en plus parler de cloud computing, une infrastructure dans laquelle la puissance de calcul et le stockage sont gérés par des serveurs distants auxquels les usagers se connectent via une liaison internet. De ce fait, les risques liés au numérique augmentent considérablement. Nous notons sur le marché depuis quelques années une multiplication des menaces et des attaques sur des entreprises. De manière générale, si nous ne sommes pas en mesure de protéger ce nouveau monde du numérique, nous ne pourrons pas le développer. L'économie de demain est donc en jeu.

Simon Fabre : Le numérique nous a ouvert les portes pour accéder à un nouveau monde mais nous ne sommes pas les seuls à avoir les clés. Elles sont aussi à disposition des attaquants et de personnes malveillantes. D'ailleurs, nous notons depuis peu, une réelle professionnalisation des attaquants qui évoluent désormais en bandes organisées. Une réelle filière métiers se développe avec des acteurs pour créer des ransomwares, d'autres, chargés de les distribuer avec des RaaS (Ransomwares as a Service) qui peuvent être achetés aisément sur internet. Il y a également ceux qui s'occupent de négocier avec leurs victimes ou encore de blanchir les fonds récoltés.

Par ailleurs, le nombre de ransomwares a explosé ces dernières années. Il y a eu une cinquantaine de signalements en 2019 contre 192 en 2020. Il s'agit d'attaques de plus en plus développées et précises malgré le fait qu'avec peu de compétences, il est possible de devenir un attaquant. Enfin, nous assistons même à l'apparition d'attaques étatiques. Néanmoins, il existe un cadre légal et réglementaire qui évolue aussi.

Nous avons deux instances, que sont la CNIL et l'ANSSI, qui viennent accompagner et sécuriser le numérique. Par exemple, en mai 2018, l'Union européenne a adopté le RGPD pour encadrer le traitement des données personnelles.

En définitive, nous sommes sur un marché en forte exposition, ce qui génère de nouveaux acteurs français en charge de garantir la sécurité de leur client.

Comment appréhendez-vous la question de la cybersécurité ?

S.F : Je représente notre filiale NBS System, qui est prestataire de services en cybersécurité depuis 1999. Nous avons toujours eu une forte expertise en matière de tests d'intrusion. Contrairement à un audit, dont l'objectif est de valider la conformité par rapport à une politique ou un référentiel, le test d'intrusion informatique mesure le risque associé à un système d'information. L'idée étant de simuler le comportement d'un attaquant allant chercher les vulnérabilités d'une entreprise. Initialement, NBS

System était donc positionné sur un métier de pirate éthique, qui accompagne les sociétés à la découverte de leur vulnérabilité. Après 10 ans de R&D, nous avons évolué et lancé une offre d'hébergement sécurisé CerberHost. En 2016, nous nous sommes rapprochés d'Oceanet Technology, un spécialiste du cloud, qui a repris l'activité d'hébergement de NBS System. Ainsi nous avons pu nous concentrer sur notre cœur de métier avec les prestations de cybersécurité. En juillet dernier, grâce à notre rapprochement avec CELESTE, nous maîtrisons désormais toute la chaîne de valeur : télécoms, cloud et hébergement et cybersécurité.

N.A : Nous avons l'avantage d'avoir une très forte synergie entre les différentes entités et filiales du groupe. Cela nous permet finalement d'avoir une forme de triple casquette et la maîtrise de toutes les problématiques liées au numérique. Nous accompagnons nos clients par la dispense de prestation de services qui peuvent être de différentes natures.

Vous êtes donc un peu orienté vers la sécurité offensive. Qu'en est-il ?

S.F : Nous allons en effet accompagner nos clients à évaluer et à optimiser leurs niveaux de sécurité au sein de leur organisation. Pour cela, nous mettons l'accent sur deux principales missions :

- les tests d'intrusions : nous simulons le comportement de l'attaquant pour identifier des vulnérabilités, ce qui va nous permettre de fournir un rapport avec des recommandations personnalisées ;
- les forensics : ils ont aussi pour but d'identifier les vecteurs d'attaque qui pourraient être employés pour réaliser une compromission et d'en saisir la portée. Nos experts sécurité vont ainsi déterminer les risques encourus par un vol d'équipement en agissant de la même manière qu'un attaquant potentiel.

Aujourd'hui, sur quels axes et enjeux vous concentrez-vous ?

S.F : Nous mettons fortement l'accent sur notre cœur de métier, qui est la partie tests d'intrusion. Nous souhaitons faire perdurer ce savoir-faire et continuer à adapter notre offre aux marchés et aux besoins de nos clients. Nous suivons de près les tendances cyber et les dernières tentatives d'attaques pour pouvoir accompagner aux mieux nos clients vis-à-vis de ces problématiques. Par exemple, nous nous sommes rendu compte dernièrement que presque la moitié des attaques de type ransomware étaient réalisées par le biais de phishing. Il s'agit d'une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données.

N.A : Nous voulons aussi renforcer le DevSecOps, qui est la combinaison du développement, de la sécurité et des opérationnels. L'idée est d'accompagner à l'intégration de la sécurité dès l'initiation des projets et ce au fil de l'eau.

Quelles sont vos perspectives sur ce segment ?

N.A : Nous avons pour ambition de devenir un acteur de référence en matière de sécurité offensive. Pour y parvenir, nous faisons de nombreux investissements, tant sur le plan matériel qu'humain. Cette année, nous allons renforcer nos équipes techniques et commerciales.

L'année dernière, nous avons doublé nos effectifs et nous connaissons une croissance à deux chiffres depuis 2019. Nos projections pour les deux prochaines années sont d'autant plus élevées. Notre objectif est de démocratiser la cybersécurité. Aujourd'hui, les PME contrairement aux grandes entreprises, ne sont pas habituées à ce type de prestations. Pourtant, elles sont aussi concernées par ces attaques. Notre enjeu est de pouvoir étendre nos prestations à toute cette gamme de clients.

EN BREF

CELESTE a été fondée en 2001 par Nicolas Aubé (93). Convaincu d'assister à une nouvelle révolution industrielle avec l'émergence du très haut débit, il décide de proposer des offres haut de gamme et innovantes et de positionner CELESTE comme l'opérateur de référence des entreprises. Dès sa création, CELESTE s'est positionné sur deux valeurs : la qualité de service et l'innovation. Les équipes de CELESTE ont pour mission de répondre de façon réactive et sur mesure aux besoins spécifiques et évolutifs des entreprises.