SAUVEGARDER LA SOUVERAINETÉ ET L'INTÉGRITÉ du patrimoine numérique des entreprises

Explosion de la menace cyber, sophistication des attaques, actions d'intelligence économique, souveraineté des solutions, sauvegarde du patrimoine numérique… sont autant d'enjeux au cœur du positionnement d'*Atempo. Luc d'Urso, PDG de l'entreprise,* nous en dit plus.

Luc d'Urso

Quel est votre cœur de métier et votre positionnement ?
Atempo est un éditeur de logiciels français. Nous avons notamment fait partie de la première promotion de la French Tech 120, le programme gouvernemental réservé aux entreprises françaises avec un potentiel d'hyper croissance.
Notre métier est la cybersécurité. De manière générale, dans ce secteur, on retrouve deux volets : les solutions préventives, qui visent à éviter la survenance d'un sinistre, et les solutions curatives qui sont déployées à la suite d'un incident cyber. Atempo est positionné sur cette seconde activité et propose des solutions de protection et de management des données. Concrètement, nous protégeons les postes de travail, les serveurs informatiques physiques ou virtuels, ainsi que le stockage, l'archivage des grands volumes de données. Notre mission est de protéger les entreprises publiques et privées contre la perte de leurs données et l'interruption de leur activité quel que soit le type de sinistre : catastrophes naturelles, erreurs de manipulation des utilisateurs, cybercriminalité…
Atempo est un acteur avec une couverture mondiale. Nous sommes implantés en Europe, aux États-Unis et en Asie au travers de neuf bureaux. Nous accompagnons près de 12 500 clients dans plus de 47 pays dans le monde. Nous sommes engagés depuis déjà plusieurs années dans la lutte contre la cybercriminalité. Nous sommes membres d'HEXATRUST, dont j'assure la vice-présidence, et nous contribuons activement au dispositif gouvernemental cybermalveillance.gouv.fr.

Au cours des dernières années, le sujet de la cybersécurité a fortement gagné en visibilité. Quelles sont les tendances que vous avez vu émerger et celles qui se dessinent actuellement ?
L'activité cybercriminelle s'est intensifiée au cours des dernières années et connaît une forte hausse continue. C'est devenu un véritable fléau économique qui peut représenter près de 1 % du PIB de chaque pays. En parallèle, les cyberattaques se sont sophistiquées et prennent aujourd'hui diverses formes. Nous avons aussi assisté à la reconversion de la criminalité traditionnelle dans la cybercriminalité, où il y a une impunité plus forte que dans le monde physique. Alors qu'il est plus complexe de démanteler un réseau de cybercriminels dans l'espace numérique, les actions de cybercriminalité sont aussi plus rentables que les activités criminelles traditionnelles. En outre, les cybercriminels se sont fortement professionnalisés. Le temps des hackers isolés est révolu. Aujourd'hui, nous sommes face à des plateaux entiers de cybercriminels semblables à ceux que l'on peut retrouver dans le monde de la relation client. Au-delà, on assiste aussi à une forme de « merchandisation » des cyberattaques avec des cybercriminels en col blanc qui montent des réseaux de distribution de produits et de solutions prêts à l'emploi pour mener des cyberattaques (fichiers de clients attaqués, malwares…).
Enfin, on note aussi un renforcement de la cybercriminalité géopolitique nourrie par les tensions entre différents pays et zones du globe. Elle peut prendre la forme de campagnes de désinformation, de déstabilisation des États, mais aussi de moyens de pression dans le cadre de négociation. La guerre qui oppose l'Ukraine à la Russie ou encore les tensions entre la Chine et les États-Unis en sont les illustrations les plus récentes.

Atempo se positionne donc comme le dernier rempart contre la cybercriminalité. Qu'est-ce que ce positionnement implique ?

En notre qualité d'acteur curatif, nous intervenons quand toutes les défenses de l'entreprise ont été percées. Dans un contexte où les attaques sont de plus en plus sophistiquées, nous sommes devenus une brique essentielle de la cybersécurité. Nos solutions sont installées en amont et en anticipation de la survenance d'un sinistre afin de garantir à nos clients zéro perte de données et zéro interruption d'activité. Notre capacité à tenir cette promesse est toutefois dépendante de l'infrastructure de nos clients. En effet, aujourd'hui, on voit encore dans de nombreuses entreprises des collaborateurs qui utilisent des applications ou des versions de solutions ou de logiciels obsolètes ou bannies par les éditeurs, et qui sont truffées de failles de sécurité. Nous avons donc un important travail de sensibilisation à réaliser afin d'alerter nos clients sur ces risques et de les aider à mettre en place des plans de reprise d'activité (PRA). Ces plans, régulièrement mis à jour en fonction de l'évolution de l'infrastructure et des systèmes des entreprises, s'appuient sur une procédure prédéfinie et testée, détaillant précisément les process à dérouler en cas d'incident.

En parallèle, nous avons aussi une activité de remédiation. Nos solutions installées permettent de restaurer les données. Pour ce faire, nous nous concentrons sur deux enjeux stratégiques pour la continuité de l'activité de nos clients : la sauvegarde des données et la préservation de leur intégrité. En effet, de plus en plus, nous remarquons que les cyberattaques visent d'abord les sauvegardes avant le système de l'entreprise. Les cybercriminels essaient, en effet, de corrompre ou d'effacer les données pour empêcher l'entreprise visée de restaurer ses données suite à l'attaque. Notre défi est donc de garantir la sécurité des données, de la sauvegarde et d'assurer leur intégrité pour permettre à une entreprise touchée par une cyberattaque de redémarrer le plus rapidement.

Se pose aussi, en matière de cybersécurité, la question de l'intelligence économique. Alors que la Chine et les États-Unis ont interdit leurs solutions respectives, l'Europe est, quant à elle, restée ouverte aussi bien aux solutions chinoises qu'américaines avec, toutefois, une protection des logiciels et du matériel qui reste relativement faible. Dans notre cœur de métier de protection des données, à la différence des applications qui vont sauvegarder des données qui leur sont propres, nous avons la capacité à sauvegarder de manière transverse l'ensemble des données d'une entreprise (messagerie, chat, sharepoint, TEAMS, CRM, applications RH, paie…). Cela nous permet de sécuriser en quelque sorte tout le patrimoine numérique de l'entreprise contre des cyberattaques, mais aussi des actions d'intelligence économique. Prenons l'exemple du Cloud Act. Cette loi extraterritoriale donne à l'état américain un droit de lecture de toutes les données qui sont traitées par les entreprises de la Tech américaine dans le monde entier. Cela concerne de nombreux équipements, logiciels, solutions américaines qui sont utilisés au quotidien par les entreprises européennes et françaises. Atempo propose des solutions qui ne sont pas soumises au Cloud Act, qui garantissent la confidentialité des données de nos clients et qui sont bien évidemment conformes au RGPD.

Sur ce segment, comment résumeriez-vous vos forces et votre valeur ajoutée ?

Nous proposons avant tout une solution souveraine qui garantit la confidentialité des données et qui est donc immune aux actions d'intelligence économique. Nous garantissons aussi à nos clients que nos actions de sauvegarde sont conformes au RGPD. Dans le contexte géopolitique actuel, nous contrôlons et ne sous-traitons aucun de nos codes à l'étranger. Ils sont à 100 % édités en France ce qui garantit, dans le cadre d'une mise à jour, qu'aucun logiciel malicieux ne sera embarqué. En parallèle, à la différence des acteurs américains, nous sommes soumis à une juridiction territoriale ce qui facilite aussi bien les procédures judiciaires qu'assurantielles. Enfin, notre dernier point de différenciation a trait à la RSE.

En mettant à disposition des entreprises des solutions souveraines, nous contribuons à renforcer la politique sociétale des entreprises, la création de valeur et l'employabilité.

Quelles pistes de réflexion pourriez-vous partager avec nos lecteurs ?

Dans un monde numérique en pleine transformation et à la croisée de forts enjeux économiques, géopolitiques, mais aussi de souveraineté et de cybersécurité, notre pays doit se doter d'une politique ambitieuse en matière de propriété intellectuelle.

En effet, c'est aussi ce qui nous permettra de conserver nos talents et nos compétences, de créer des emplois et de la valeur. Ces filières souveraines peuvent offrir de très belles perspectives de carrière aux jeunes diplômés et pour les rendre encore plus impactantes, nous devons veiller à y promouvoir la mixité et la diversité, qui sont une véritable richesse pour nos métiers.