Le Journal des Entreprises

Interview · BORDEAUX · # CYBERSÉCURITÉ · # TRANSITION NUMÉRIQUE

Nicolas Leroy-Fleuriot

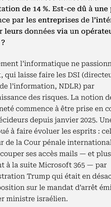
PDG de Cheops Technology

"Nous aurons des affaires d'espionnage retentissantes dans les années qui viennent"

Par Caroline Ansart

Publié le 12 novembre 2025 à 15h58

L'acteur girondin du cloud et de la cybersécurité Cheops Technology est de plus en plus sollicité par des entreprises en quête de souveraineté de leurs données. Mais trop de dirigeants méconnaissent encore les risques qu'ils encourent, estime le PDG de Cheops, Nicolas Leroy-Fleuriot. Il a lancé un tour de France pour "évangéliser" ses homologues.



"La demande s'accélère, à la fois pour réinternaliser le cloud chez le client ou chez un opérateur français, mais aussi pour identifier les tentatives d'intrusion", note Nicolas Leroy-Fleuriot, PDG de Cheops Technology. — Photo : Caroline Ansart

Vous venez de publier les derniers chiffres de Cheops Technology, qui emploie 750 salariés sur 12 sites dans le domaine du cloud et de la cybersécurité, annonçant une croissance de plus de 5 % pour l'exercice 2024-2025. Avec plus de 200 millions d'euros de chiffre d'affaires consolidé et une hausse du résultat d'exploitation de 14 %. Est-ce dû à une prise de conscience par les entreprises de l'intérêt de sécuriser leurs données via un opérateur français ?

Généralement l'informatique ne passionne pas le dirigeant, qui laisse faire les DSI (directeur des services de l'information, NDLR) par méconnaissance des risques. La notion de souveraineté commence à être prise en compte par les décideurs depuis janvier 2025. Une affaire a contribué à faire évoluer les esprits : celle du procureur de la Cour pénale internationale qui s'est fait couper ses accès mails — et plus largement à la suite Microsoft 365 — par l'Administration Trump qui était en désaccord avec sa position sur le mandat d'arrêt émis contre le Premier ministre israélien.

La politique de Donald Trump change-t-elle la donne ?

Trump nous rend un service fou ! C'est lors de son premier mandat en 2018 que le Cloud Act a été mis en place. Renforcé encore dans le second mandat, il intime l'ordre aux opérateurs de cloud américains (Amazon AWS, Google, Microsoft) de révéler les données hébergées chez eux de n'importe quelle entreprise (y compris dans un de leurs data centers en Europe) si un juge ou une agence de renseignement américaine — il en existe 17 — estime qu'il y a un risque pour la sécurité des États-Unis. La concurrence économique étant considérée comme telle. Désormais les entreprises concernées n'ont même plus à être prévenues. Les risques d'espionnage industriels sont majeurs. Le Cloud Act est fait pour ça ! Nous aurons des affaires retentissantes dans les années qui viennent.

Pourtant vous avez entamé un "tour de France" pour prêcher la bonne parole auprès des dirigeants, en organisant sur les mois de novembre et décembre 11 journées dans les principales villes de France pour expliquer les enjeux de l'IA, de la cybersécurité et de la souveraineté. Le message n'est donc pas encore bien passé. Qu'est-ce qui freine les entreprises

Je me retrouve effectivement pour la première fois de ma vie à devoir évangéliser mes homologues dirigeants. J'aborde parce qu'il reste un méconnaissance des risques, la prise de conscience s'amorce tout juste. La cybersécurité, l'IA et la souveraineté ne sont pas l'apanage des grands groupes. Ensuite, la souveraineté n'apporte pas de valeur, elle a même coût, comme une assurance. Si vous n'avez pas de préjudice, l'assurance ne fait que vous coûter de l'argent. Mais le risque est majeur. Concrètement, basculer pour un service souverain (cloud, messageries, etc., NDLR) a un coût de migration et un coût d'abonnement. Pour l'abonnement on est aligné sur les grands acteurs, et on apporte des services supplémentaires notamment le maintient des applications en conditions opérationnelles.

> ***"Toutes les données sensibles ne doivent plus être hébergées chez les Américains."***

Notre métier aujourd'hui c'est exploiter la meilleure technologie sur le marché (même une américaine mais de façon souveraine) et de placer la bonne application dans le bon service au bon prix. On adapte au maximum.

Concrètement est-ce que la démarche de migration est complexe ? Est-ce que c'est long ?

Entre les débuts d'une discussion et l'opérationnel, il faut entre 6 et 12 mois, le temps de récupérer les données chez le tiers, les basculer chez nous, effectuer des tests et passer en production. Avec notre expérience (auprès de plus de 250 clients, NDLR) on essaie d'automatiser au maximum.

Qui sont les entreprises qui vous contactent aujourd'hui et pour quels services ?

La demande s'accélère, à la fois pour réinternaliser le cloud chez le client ou chez un opérateur français, mais aussi pour identifier les tentatives d'intrusion — nous cumulons 78 contrats sur notre plateforme Cyberpatriot depuis son lancement il y a deux ans. Nous enregistrons davantage d'entreprises industrielles qui font de la R & D. Le secteur de la Défense est, c'est sidérant, souvent hébergée aux États-Unis, mais cela va changer. Celui de la santé doit le devenir aussi, puisqu'on ne peut plus localiser de données médicales personnelles sur une plateforme étrangère depuis une circulaire d'il y a deux ans, mais c'est long. C'est un gros marché potentiel pour nous. De manière générale, toutes les données sensibles, cela varie selon les entreprises — savoir-faire, brevet, fichier clients, sourcing, prix d'achat -, ne doivent plus être hébergées chez les Américains. Il faut le triptyque CSS : confidentialité, sécurité, souveraineté.

Est-ce que les petites PME vous contactent ?

Notre cœur de cible ce sont les ETI et PME qui réalisent au moins 100 millions d'euros de chiffre d'affaires, pour le cloud. Pour la partie infrastructures nous avons même des grands groupes (Airbus, de grandes compagnies d'assurances, quelques banques). Nous ne sommes pas organisés pour des petites PME parce que le risque que l'on assure est le même donc ce n'est pas rentable. Pour autant rien n'est gravé, nous gérons par exemple Cacoche (27 Mc de CA attendus en 2025, 56 salariés, NDLR) qui a un outil informatique prépondérant, ou le campus Cyber de Nouvelle-Aquitaine qui est susceptible d'héberger les mails d'un client hacké.

Il y a deux ans vous avez lancé une messagerie sécurisée, Mail in France, comprenant boîte mail, chat, drive et visio. Séduit-elle ?

De plus en plus, mais elle n'a pas le succès escompté. On espérait un raidje marée, il n'est pas arrivé mais l'intérêt pour la solution monte. Un des freins est le changement d'environnement, l'expérience utilisateur. On a donc développé une version 2 qui reprend l'interface Outlook. Une autre crainte est de se couper de nouvelles fonctionnalités qui sortiraient chez les gros acteurs en premier. Mais les choses vont peut-être changer : sentant le vent tourner en faveur de la souveraineté, Microsoft va peut-être lancer une version hébergeable localement, à disposition de quelques opérateurs comme Cheops.

Qui sont vos concurrents aujourd'hui, voyez-vous émerger de nouveaux acteurs ?

Nous sommes cinq acteurs, Orange est un concurrent sérieux. En revanche, la barrière financière et technologique est désormais trop élevée pour un nouvel acteur. Les investissements sont colossaux.

Comment s'annonce le prochain exercice ? Êtes-vous inquiet de la crise économique ?

Le prochain exercice s'annonce très bien puisque le premier semestre fiscal (du 1er mai au 31 octobre, NDLR) s'est clôturé à + 15 %. Mais nous sommes témoins d'entreprises qui deviennent fragiles financièrement et cela nous inquiète.