La responsabilité d'un prestataire informatique retenue pour une cyberattaque chez son client.

Par un arrêt du 19 novembre 2024, la Cour d'appel de Rennes a retenu la responsabilité d'un prestataire informatique à la suite d'une cyberattaque par rançongiciel chez son client en invoquant un manquement à l'obligation de conseil, d'information et de mise en garde.

- **Les faits**

La société [L] INDUSTRIE, le client, spécialisée dans la fabrication de portails, a fait appel à la société MISMO, le prestataire, pour la modernisation de son infrastructure informatique. Le projet comportait plusieurs phases, dont la configuration et l'installation du matériel, ainsi que la mise en place d'un dispositif de sécurisation des données.

Cependant, le 17 juin 2020, le client a été victime d'une cyberattaque par rançongiciel. Les pirates ont chiffré l'ensemble des données du système d'information, y compris ses sauvegardes. Le client met en cause le prestataire au motif que l'attaque était due à des failles dans le matériel informatique, accentuées par une mauvaise configuration du contrôleur de domaine installé par le prestataire. Estimant que ces défaillances ont facilité l'intrusion des cybercriminels et aggravé l'impact de l'attaque, le client a dénoncé ces manquements auprès du prestataire le 30 juillet 2020. Le prestataire contestait cette analyse.

Par un jugement du Tribunal de commerce de Nantes du 17 juillet 2023, le client avait été débouté de ses demandes. Il a interjeté appel le 27 juillet 2023.

- **Les motivations des parties**

Le client considère que le prestataire a manqué à son devoir de conseil et fournit des diagnostics réalisés par des tiers afin d'apporter la preuve d'une mauvaise configuration du contrôleur de domaine, et notamment l'absence d'un mécanisme de sauvegardes déconnectées.

Le prestataire fait valoir que (i) son contrat avec le client se limitait uniquement à la fourniture de matériels et logiciels en remplacement d'équipements obsolètes, prestation qu'il indique avoir réalisée selon le cahier des charges, (ii) la gestion des sauvegardes ne relevait pas de ses missions et était de la responsabilité du client, et (iii) la société étant composée d'un service informatique, ce qui l'exonérait de toute obligation d'information et de conseil en matière de sécurité.

- **Décision de la Cour d'appel de Rennes**

La Cour d'appel de Rennes a infirmé le jugement de première instance et a estimé que le prestataire avait manqué à ses obligations d'information, de conseil et de mise en garde envers le client.

Elle souligne que l'installation d'une nouvelle infrastructure devait être considérée comme un produit complexe et indique ainsi que le prestataire devait s'assurer que les services répondaient aux besoins du client. Elle précise que le service informatique du client, composé de trois personnes, ne pouvait être assimilé en compétence à celui du prestataire, spécialisé en cybersécurité et que le client n'était donc pas un professionnel du domaine.

Ainsi, le prestataire devait informer le client sur la nécessité d'adapter ou de modifier son système de sauvegarde afin de garantir la conservation et la restauration des données en cas de sinistre. À aucun moment, le prestataire ne démontre avoir informé son client de ce risque, manquant ainsi à son devoir de mise en garde.

Concernant l'indemnisation, la Cour juge que les manquements du prestataire sont à l'origine des préjudices subis par le client. Le défaut d'information et de conseil a privé le client de la possibilité d'éviter le sinistre. Toutefois, l'indemnisation doit être évaluée en fonction de cette perte de chance et ne pourra être équivalente au dommage total causé par l'incident. Elle condamne ainsi le prestataire à payer une fraction des préjudices supportés par la victime. Le prestataire est condamné à payer 50 000 euros afin de prendre en charge une fraction des coûts externes (notamment les factures des différents prestataires étant intervenus à la suite de la cyberattaque) ainsi que l'atteinte

à l’image. Cependant, les juges refusent d’indemniser les coûts de mobilisation des salariés en interne.

Lien utile :

Décision - Cour d'appel de Rennes : RG n°23/04627 | Cour de cassation