Mathias | Avocats

Cybersécurité : quelles obligations et bonnes pratiques pour les entreprises et les prestataires informatiques ?

Focus sur l'arrêt du 19 novembre 2024 - Cour d'appel de Rennes (RG n°23/04627)

Quel est le contexte ?

Une entreprise industrielle spécialisée dans la fabrication de portails ("l'Entreprise Cliente") a confié à un prestataire de services informatiques ("le Prestataire") la modernisation de son infrastructure informatique. Ce projet incluait notamment le remplacement des serveurs et la mise en place d'un système de sauvegarde. **En juin 2020, l'Entreprise Cliente a été victime d'une cyberattaque par rançongiciel, ayant entraîné la perte et le chiffrement de ses données**. Estimant que ces pertes résultaient d'un manquement contractuel du Prestataire, l'Entreprise Cliente l'a assigné en justice pour manquement à son obligation d'information, de conseil et de bonne exécution.
En première instance, le Tribunal de commerce de Nantes a rejeté les demandes de l'Entreprise Cliente, estimant qu'elle ne démontrait pas la faute du Prestataire. L'Entreprise Cliente a interjeté appel de cette décision.

Quelle est la décision de la Cour d'appel ?

La Cour d'appel de Rennes dans son arrêt en date du 19 novembre 2024 infirme le jugement de première instance et retient la responsabilité du Prestataire pour manquement à son obligation d'information, de conseil, de délivrance ainsi que de mise en garde. Elle considère que le Prestataire, en tant que professionnel de l'informatique, aurait dû notamment :

- Analyser les besoins de l'Entreprise Cliente pour proposer une architecture sécurisée et répondant aux besoins du client ;
- Conseiller, informer et mettre en garde son client sur les conséquences des choix opérationnels effectués par ce dernier et lui proposer différentes solutions avec les coûts afférents.

En ne remplissant pas ces obligations, le Prestataire a fait perdre à l'Entreprise Cliente une chance d'éviter ou de limiter les conséquences de la cyberattaque.

Cette jurisprudence rappelle l'importance de formaliser et d'expliciter, dans tous les documents échangés avec le client (CG, offres commerciales, comité de pilotage, etc.) le devoir de conseil, d'information et de mise en garde à l'égard du client.

19 RUE VERNIER 75017 PARIS
+33 (0)1 43 80 02 01
CONTACT@AVOCATS-MATHIAS.COM

BONNES PRATIQUES

👉POUR LES ENTREPRISES CLIENTES :

- **Formalisation du devoir de conseil, d'information et de mise en garde :**
  - Inclure des clauses détaillant explicitement l'obligation de conseil, d'information et de mise en garde du prestataire.
  - Inscrire dans les contrats des engagements précis sur la sécurisation des infrastructures et les responsabilités partagées.

- **Encadrement des niveaux de service :** clarifier dans les contrats les responsabilités du prestataire, les obligations de sécurité et les recours en cas de défaillance (par exemple par la mise en place d'un cahier des charges).

- **Mise en place d'un suivi régulier :** effectuer des audits de sécurité réguliers du prestataire pour s'assurer du respect des engagements contractuels ainsi que du respect de l'état de l'art.Cette obligation doit perdurer pendant toute la durée de la relation contractuelle notamment eu regard de l'évolution de l'état de la menace

- **Formation et sensibilisation** : les entreprises doivent mettre en place des sessions de formation internes régulières sur la cybersécurité afin de limiter les risques d'attaques.

👉POUR LES PRESTATAIRES DE SERVICES INFORMATIQUES :

- **Obligation d'analyse et de conseil** : Un prestataire doit évaluer les risques en matière de cybersécurité spécifiques aux métiers, usages du client et proposer des solutions adaptées en tenant compte de l'état de l'art.
- Dans le cadre de la mise en œuvre, les comités doivent être rédigés de façon factuelle, explicite et objective incluant un relevé de décisions.

- **Une responsabilité limitée et plafonnée :** s'assurer que les contours de son intervention sont clairement définis, tant dans le contrat que dans la proposition commerciale, afin d'éviter toute ambiguïté en cas de litige. Définir précisément les prestations incluses dans les contrats ainsi que dans la proposition commerciale et celles qui relèvent d'une assistance complémentaire. Pour ce faire, l'établissement d'un RACI est vivement recommandé.

- **En cas d'absence de mise en œuvre des préconisations : l**e prestataire doit formaliser ses préconisations par écrit (email, courrier officiel, rapport de réunion, etc...) en expliquant les risques encourus, en proposant des alternatives et en mentionnant le coût. En effet, le prestataire doit fournir l'ensemble des éléments d'appréciation à son client. Cette démarche protège juridiquement le prestataire en cas d'absence de mise en œuvre.

- **Formation et sensibilisation :** Les prestataires doivent encourager leurs clients à mettre en place des sessions de formation interne sur la cybersécurité afin de limiter les risques d'attaques notamment par phishing ou erreurs humaines.

19 RUE VERNIER 75017 PARIS
+33 (0)1 43 80 02 01
CONTACT@AVOCATS-MATHIAS.COM