LOT CYBER :

Bonjour,

Merci de bien vouloir nous apporter les informations suivantes nécessaires à l'appréciation de la réalité de votre risque Cyber :

SUR UN PLAN TECHNIQUE

1/ Est-ce que des sauvegardes des données et des éléments critiques du système informatique :

- sont réalisées a minima toutes les semaines avec une rétention minimale de 2 semaines ?
  Oui. Sauvegardes automatisées quotidiennes (différentielles) et hebdomadaires (complètes), avec une rétention supérieure à 3 mois.
- sont des sauvegardes déconnectées, des sauvegardes immuables, ou des sauvegardes sécurisées ?
  Oui. Sauvegardes immuables (dépôt durci : points de restauration non modifiables ni supprimables, y compris par un administrateur) et sauvegardes sécurisées (isolées de l'Active Directory, accès filtré par pare-feu, administration protégée par MFA).
- sont des sauvegardes documentées et testées au moins annuellement ?
  Oui. Les sauvegardes et le PRA sont documentés et testés régulièrement ; le PRA est testé et validé au moins une fois par an. Il est disponible en version numérique et papier.

A SAVOIR :

Sauvegardes déconnectées
Une copie des données et éléments critiques du système informatique, réalisée sur un élément physique vous appartenant et maintenu déconnecté du reste de votre système informatique. Cela inclut les bandes, disques durs externes, et ordinateurs jamais connectés à internet ou à un autre élément de votre système informatique.

Sauvegardes immuables
Une copie des données et éléments critiques du système informatique, réalisée sur un élément appartenant à votre système informatique et dont les données ne pourraient pas être modifiées ni supprimées compte tenu du caractère immuable de la sauvegarde. Une sauvegarde immuable ne peut être modifiée ou supprimée, même par un administrateur. Quelques exemples de services permettant la mise en place de sauvegardes immuables : Amazon S3 Glacier, Microsoft Azure Immutable vaults, Veeam Hardened Repository. À noter : l'utilisation du terme « immuable » dans le contexte de certaines solutions NAS, comme QNAP, est incorrecte car elles peuvent être contournées par un administrateur – ces solutions ne sont pas considérées comme immuables au titre de ce contrat.

Sauvegardes sécurisées
Une copie des données et éléments critiques du système informatique, réalisée sur un élément physique vous appartenant et isolé de l'Active Directory, dont l'accès est restreint au travers d'un pare-feu n'autorisant que :
a. un flux d'envoi de sauvegardes depuis une liste limitée de serveurs ; et
b. un accès aux sauvegardes par une interface web protégée par une authentification multi-facteur (MFA).

2/ Un logiciel antivirus est-il installé sur tous les postes de travail et serveurs Windows et est mis à jour au plus tard 15 jours après qu'une mise à jour soit disponible ?

Oui. Un antivirus/antimalware est déployé sur l'ensemble des postes de travail et serveurs, avec des mises à jour automatiques en continu.

Disposez-vous d'une solution EDR/XDR ? Si oui, est-il managé en interne ou en externe ?

Oui. Deux solutions EDR/XDR couvrent l'ensemble du parc (serveurs, postes de travail, appareils mobiles, équipements réseau). Elles sont managées en interne par la DSI.

3/ Les accès à distance au système informatique (VPN, SaaS, O365, Citrix, etc) nécessitent-ils tous une authentification à deux facteurs (2FA)

pour tous les dirigeants ? et tous les administrateurs informatique ?
pour tous les utilisateurs ?

Oui. L'authentification multifacteur (MFA) est activée pour l'ensemble des utilisateurs, dirigeants et administrateurs compris. Les comptes à privilèges font l'objet d'une surveillance renforcée avec blocage automatique dès un niveau de risque modéré.

SUR UN PLAN INSTITUTIONNEL

1/ Un autre établissement doté de sa propre personnalité juridique (CCAS, CDE…) partage-t-il votre SI observant par là même les mêmes règles de gestion / sécurisation du SI ?
Si oui merci de nous confirmer votre souhait de le prévoir comme assuré additionnel au marché à souscrire.
Dans l'affirmative, merci de nous communiquer son SIRET, son budget de fonctionnement global et son effectif total

A vérifier : Les antennes de Nantes et de Rodez, sans personnalité juridique distincte, utilisent le SI de Limoges avec le même niveau de sécurité. Nous ne souhaitons pas les ajouter en assuré additionnel.

2/ Exercez-vous une activité de gestion /exploitation d'un aéroport – aérodrome ?
Non.

3/ A défaut de pouvoir remettre un relevé de sinistralité pour n'être assuré au titre de ce risque, avez-vous subi un sinistre cyber d'un coût total supérieur à 50 000 €, que celui-ci ait été indemnisé ou non, durant les trois dernières années ? Si oui, merci de bien vouloir nous éclairer à son sujet.
Non.