

**Marché N° : 2024-12**

**MARCHÉ DE PRESTATIONS DE SERVICES D'ASSURANCE**

## **QUESTIONS/REPONSES N°1**

Des questions ont été posées par un opérateur économique pour le marché cité en objet. Veuillez prendre connaissance des réponses apportées.

**Question du vendredi 17 mai 2024 - 13:32:**

LOT CYBER

Bonjour,

Dans le cadre du lot Cyber nous vous remercions de répondre aux questions suivantes, indispensables afin d'analyser le risque :

- Budget de fonctionnement de l'entité publique à couvrir (ou ensemble des collectivités dans le cadre d'un groupement d'achat) : .....
- Activité de l'entité publique à couvrir : .....
- Avez-vous les compétences de la production, distribution d'électricité et d'eau potable : oui/non
- Détenez-vous les données personnelles sensibles de plus de 100 000 (cent mille) personne ?
- Réalisez-vous des sauvegardes de tous vos systèmes et données ?
- Quelle est votre solution de sauvegarde ?
  - ☐ En une sauvegarde physique maintenue déconnectée de ses systèmes à un moment donnée
  - ☐ En une sauvegarde cloud
  - ☐ En une sauvegarde sur un serveur NAS
- Le délai de rétention de vos sauvegardes est-il au moins de 30 jours ?
- L'accès à vos sauvegardes est-il possible qu'aux comptes avec des droits administrateurs ?
- Dans la négative, l'accès est-il contrôlé avec une authentification multifactorielle ?
- Mettez-vous à jour vos logiciels et systèmes (y compris anti-virus et pare-feu) dans les 30 jours suivants la mise à disposition de patchs par le fabricant ?
- Utilisez-vous les systèmes d'exploitation dont les mises à jour ne sont plus supportées par leur fabricant ?
- Dans la positive avez-vous prévu une migration de ces systèmes avant la prise de garantie de l'assurance du présent lot ?
- Limitez-vous les privilèges administrateurs aux seuls utilisateurs qui en ont besoin ?
- Les administrateurs possèdent-ils tous deux comptes : un pour leurs missions d'administrateurs et un pour les usages quotidiens ?
- Si vous acceptez-vous les paiements par carte bancaire en ligne, vos prestataires de paiement externalisés ont-ils le niveau PCI correspondant ?



**Bouillargues**

en costières

- Dans le cadre d'un GIE, détenez-vous un accès à distance au réseau informatique de vos membres/clients ?
- Si votre budget de fonctionnement est supérieur à 10 000 000€, avez-vous recours à l'authentification multifactorielle pour les administrateurs pour gérer les connexions à distance ?
- Si votre budget de fonctionnement est supérieur à 25 000 000€, avez-vous recours à l'authentification multifactorielle pour l'ensemble des utilisateurs pour gérer les connexions à distance ?
- Avez-vous subi un sinistre cyber au cours des cinq dernières années ?
- Avez-vous fait l'objet d'une ou plusieurs enquêtes administratives ?
- Avez-vous connaissance d'événements ou circonstances pouvant donner lieu à la mise en jeu de la garantie ?

#### Fiche de Déclaration du Risque

Société / Collectivité :

SIRET :

Contact Société / Collectivité :

Nombre d'employés :

Chiffre d'affaires / Budget de fonctionnement :

Code NAF :

Nom de domaine :

Nom du représentant dûment autorisé par la société :

Sécurité des applications :

1) Les logiciels et OS que vous utilisez sont-ils toujours maintenus par leurs éditeurs ? (ex : pas de version Windows antérieure à Windows 10) ? Si Non, pouvez-vous lister les éventuels systèmes non maintenus avec la politique de sécurité associée.

2) Tous vos équipements sont-ils équipés d'un antivirus à jour ?

☐ Vos postes de travail Windows ?

☐ Vos serveurs Windows ?

3) Avez-vous mis en place une solution d'anti-phishing (ex : identification et blocage des emails de phishing) ? Si oui, précisez la solution utilisée.

4) Avez-vous activé un pare-feu sur tous vos systèmes exposés à l'extérieur de votre réseau ? Si oui, précisez la solution utilisée.

5) A quelle fréquence effectuez-vous les mises à jour de sécurité pour l'ensemble des logiciels que vous utilisez ? Précisions des logiciels qui ont une politique de mise à jour moins fréquente.

Sauvegarde des données et restauration :



## Bouillargues

en costières

6) A quelle fréquence effectuez-vous des sauvegardes de vos données sur des supports déconnectés et isolés de votre réseau une fois les sauvegardes effectuées ? Précisions éventuelles sur votre système de sauvegarde.

7) A quelle fréquence effectuez-vous des tests de restauration à partir de vos sauvegardes ? Précisions éventuelles sur les tests de restauration.

Sécurité des systèmes :

8) Disposez-vous d'une journalisation (logs) des événements de sécurité (ex : accès des utilisateurs aux applications, attribution de nouveaux droits d'accès, création de nouveaux utilisateurs, etc.) pour l'ensemble de vos ordinateurs et serveurs sur une durée d'au moins 15 jours ?

9) Avez-vous mis en place une solution centralisée de remontée et de corrélation des événements de sécurité (logs) pour vos ordinateurs et serveurs (ex : EDR, XDR, etc.) ?

Sécurité des accès :

10) Avez-vous mis en place une authentification multi facteurs (MFA) pour l'ensemble de vos systèmes critiques internes et externes et vos accès distants ? Si Non, listez les systèmes critiques qui ne disposent pas de MFA et la politique d'accès associée.

11) Avez-vous mis en place différents niveaux de droits d'accès en fonction des besoins métier de vos utilisateurs sur l'ensemble de vos systèmes critiques ? Si Non, listez les systèmes critiques sans droits d'accès limités et la politique de sécurité associée.

12) Limitez-vous les privilèges "administrateurs" exclusivement aux utilisateurs qui en ont besoin ?

13) Confirmez-vous que vos utilisateurs ne sont pas administrateurs de leurs postes de travail ?

14) Chaque utilisateur dispose-t-il de compte nominatif pour se connecter au système d'information, aux applications métier et aux systèmes critiques de l'entreprise ?

15) Imposez-vous une connexion par VPN pour tous les accès distants à vos systèmes critiques ?

16) L'ensemble de vos mots passe sont-ils robustes (min 15 caractères incluant des capitales, minuscules, chiffres et caractères spéciaux.) ?

17) Les ports RDP (Remote Desktop Protocol) de votre réseau sont-ils fermés ?

Gouvernance :

18) Avez-vous inventorié l'ensemble de votre parc informatique (équipements, logiciels, données, accès, interconnexions avec l'extérieur, etc.) ?

19) Quel volume de données traitez-vous ?

- Volumes donnés à caractère personnel sensibles ?

- ☐ Volume données bancaires ?



**Bouillargues**

en costières

☐ Volume données de santé ?

20) Listez les mesures de protection mises en place pour sécuriser vos données (DLP, chiffrement des données, classification des données, blocage des ports USB, etc.)

**Réponse :**

*Veuillez-vous référer au document du DCE intitulé : Questionnaire Appréciation Risques Cyber 2024*