REGISTRE DES QUESTIONS

INFORMATIONS CONCERNANT L'ANNONCE

Collectivité : Commune de Les Noës-près-Troyes

Type d'annonce : Avis d'appel à la concurrence

Type de procédure : Procédure adaptée ouverte pour un montant compris entre 90 000 HT et 221 000 euros HT

Référence : 2025-02

Date de mise en ligne : Le lundi 07 avril 2025 à 13:00:01

Date de clôture : Le lundi 19 mai 2025 à 12:00:00

Titre : Souscription de contrats d'assurance

REGISTRE DES QUESTIONS / REPONSES REPONDUES

Questions / Réponses

[23/04/2025 à 09:07:04] Bonjour,
Lot 4 DAB : serait-il possible de communiquer les PV des commissions de sécurité de vos ERP ? A minima, merci de confirmer les avis favorables et ne transmettre que les éventuels "défavorables".
Cordialement

[24/04/2025 12:10:11] Mesdames, Messieurs,

Je vous prie de bien vouloir trouver en pièce jointe l'ensemble des PV des commissions de sécurité des ERP.

Vous en souhaitant bonne réception,

Cordialement,

Nathalie PONTABRY, Responsable de la Commande Publique

[15/04/2025 à 14:45:40] LOT CYBER
Merci de nous indiquer le budget de fonctionnement (VILLE + CCAS)
Merci de nous indiquer l'effectif (VILLE + CCAS)

Questions / Réponses

[23/04/2025 10:46:50] Mesdames, Messieurs,

Je vous informe que :
- Le budget de fonctionnement de la ville s'élève à : 3 746 656,81 €.
- Le budget de fonctionnement du CCAS s'élève à : 70 000 €.

Concernant les effectifs:
- Pour la ville : 46 agents à ce jour avec une fluctuation possible jusqu'à 49 en fonction des besoins.
- Pour le CCAS : Aucun agent n'est recruté par le CCAS.

Questions / Réponses

[09/04/2025 à 10:37:16] LOT CYBER
Bonjour

Nous avons pris soin d'analyser votre questionnaire et de le croiser avec celui de la compagnie,
Il nous reste quelques questions sans réponse , sans un questionnaire complet et détaillé nous ne pouvons pas demander un devis à la compagnie d'assurance,
Je vous prie de bien vouloir compléter le questionnaire complémentaire ci-dessous.

En vous remerciant par avance,
Cordialement,

Merci de lister les entités juridiques rattachées à la structure à assurer :
.....
.....

Ces entités partagent-elles le même système d'information que la structure principale à assurer ?
OUI ? NON ?

Au cours des 5 derniers années, avez-vous déjà été victime de cyber attaques vous ayant causé des préjudices financiers ?
OUI ? NON ?
Si oui, décrivez la nature, les conséquences, et les coûts de ces cyber attaques, ainsi que les mesures prises depuis :
.....
.....

Combien de postes informatiques possédez-vous ? ? De 0 à 20 ?De 21 à 50 ? Plus de 50

Avez-vous un site internet ou un extranet ?
OUI ? NON ?
Si OUI :
- Le contrat d'hébergement de votre site intègre-t-il une solution anti-DDoS ?
OUI ? NON ?

- Votre site est-il un point d'accès pour vos salariés et/ou vos partenaires ?
OUI ? NON ?

- Votre site intègre-t-il des services de vente de produits et/ou de services en ligne ?
OUI ? NON ?
Si OUI à cette question, répondre aux questions suivantes :
- Votre site internet est-il sécurisé via un protocole HTTPS ?
OUI ? NON ?

- Conservez-vous les données bancaires de vos clients ou fournisseurs ?
OUI ? NON ?
-Etes-vous référencé comme sous-traitant / fournisseur dans des grandes entreprises ou des administrations ?
OUI ? NON ?

- Détenez-vous des informations soumises à une obligation de confidentialité renforcée (*) (secret des affaires, secret professionnel ou secret médical) dans votre système informatique ?
OUI ? NON ?
(*) C'est-à-dire :
L'attaque d'un système informatique aura des conséquences majeures si celui-ci contient des données très sensibles protégées par le secret des affaires (au sens de la directive européenne sur le secret des affaires, votée en avril 2016). A titre d'exemple, des secrets de fabrication dans le monde industriel ou des données relatives à une affaire chez un avocat constituent des données à caractère confidentiel.

Si OUI à cette question, répondre à la question suivante :

- Ces informations concernent-elles des tiers (par exemple, vos clients, vos sous-traitants ou vos fournisseurs…) ?
OUI ? NON ?

L'option firewall de vos postes de travail est-elle activée ?
OUI ? NON ? Ne Sait Pas ?

Avez-vous des outils de filtrage réseau sur votre système informatique ?
OUI ? NON ? Ne Sait Pas ?

Avez-vous mis en place un plan de continuité d'activité (PCA) traitant de l'indisponibilité de votre système informatique ?
OUI ? NON ? Ne Sait Pas ?

A quelle fréquence les sauvegardes de l'ensemble des données nécessaires à votre activité sont-elles effectuées ?

Une seule réponse possible
? Quotidiennement
? Hebdomadairement
? Moins fréquemment

Comment les sauvegardes de l'ensemble des données nécessaires à votre activité sont-elles effectuées ?
Plusieurs réponses possibles
• Sur des supports de stockage conservés en dehors des locaux de l'entreprise ?
OUI ? NON ?

• Sur des services sur internet configuré pour réaliser des sauvegardes en ligne (ex : cloud) ?
OUI ? NON ?

Utilisez-vous un antivirus payant, à jour et dont la licence est en cours de validité ?
OUI ? NON ?

Imposez-vous une mise à jour trimestrielle des mots de passe de vos collaborateurs ?
OUI ? NON ?

Avez-vous mis en place des règles de sécurisation des mots de passe ?
OUI ? NON ?

Vos collaborateurs sont-ils sensibilisés aux risques numériques et à leurs conséquences ?

Plusieurs réponses possibles
- Des simulations d'attaques par phishing (hameçonnage) ? OUI ? NON ?

- Des formations présentiels ou e-learning ? OUI ? NON ?

- La diffusion de guide de bonnes pratiques ? OUI ? NON ?

Avez-vous mis en place une politique ou une charte de sécurité informatique formalisée, pilotée et régulièrement communiquée à l'ensemble de vos collaborateurs ?
OUI ? NON ?

Questions / Réponses

[11/04/2025 11:45:32] Madame, Monsieur,

Veuillez trouver ci-après les réponses apportées aux questions qui nous ont été transmises. Vous en souhaitant bonne réception,

Merci de lister les entités juridiques rattachées à la structure à assurer :
Le Centre Communal d'Action Sociale (CCAS) et la commune

Ces entités partagent-elles le même système d'information que la structure principale à assurer ?
OUI X NON ?

Au cours des 5 derniers années, avez-vous déjà été victime de cyber attaques vous ayant causé des préjudices financiers ?
OUI ? NON X
Si oui, décrivez la nature, les conséquences, et les coûts de ces cyber attaques, ainsi que les mesures prises depuis :
.....
.....

Combien de postes informatiques possédez-vous ? ? De 0 à 20 xDe 21 à 50 ? Plus de 50

Avez-vous un site internet ou un extranet ?
OUI X NON ?
Si OUI :
- Le contrat d'hébergement de votre site intègre-t-il une solution anti-DDoS ?
OUI X NON ?

- Votre site est-il un point d'accès pour vos salariés et/ou vos partenaires ?
OUI ? NON ? S'il s'agit d'envoyer des messages via le site, oui. Si ce n'est pas la réponse attendue, veuillez mieux formuler la question SVP.

- Votre site intègre-t-il des services de vente de produits et/ou de services en ligne ?
OUI ? NON X
Si OUI à cette question, répondre aux questions suivantes :
- Votre site internet est-il sécurisé via un protocole HTTPS ?
OUI X NON ?

- Conservez-vous les données bancaires de vos clients ou fournisseurs ?
OUI ? NON X
-Etes-vous référencé comme sous-traitant / fournisseur dans des grandes entreprises ou des administrations ?
OUI ? NON X

- Détenez-vous des informations soumises à une obligation de confidentialité renforcée (*) (secret des affaires, secret professionnel ou secret médical) dans votre système informatique ?
OUI ? NON X
(*) C'est-à-dire :
L'attaque d'un système informatique aura des conséquences majeures si celui-ci contient des données très

sensibles protégées par le secret des affaires (au sens de la directive européenne sur le secret des affaires, votée en avril 2016). A titre d'exemple, des secrets de fabrication dans le monde industriel ou des données relatives à une affaire chez un avocat constituent des données à caractère confidentiel.

Si OUI à cette question, répondre à la question suivante :

- Ces informations concernent-elles des tiers (par exemple, vos clients, vos sous-traitants ou vos fournisseurs…) ?
OUI ? NON X

L'option firewall de vos postes de travail est-elle activée ?
OUI X NON ? Ne Sait Pas ?

Avez-vous des outils de filtrage réseau sur votre système informatique ?
OUI X NON ? Ne Sait Pas ?

Avez-vous mis en place un plan de continuité d'activité (PCA) traitant de l'indisponibilité de votre système informatique ?
OUI ? NON X Ne Sait Pas ?

A quelle fréquence les sauvegardes de l'ensemble des données nécessaires à votre activité sont-elles effectuées ?

Une seule réponse possible
X Quotidiennement
? Hebdomadairement
? Moins fréquemment

Comment les sauvegardes de l'ensemble des données nécessaires à votre activité sont-elles effectuées ?
Plusieurs réponses possibles
• Sur des supports de stockage conservés en dehors des locaux de l'entreprise ?
OUI X NON ?

• Sur des services sur internet configuré pour réaliser des sauvegardes en ligne (ex : cloud) ?
OUI X NON ?

Utilisez-vous un antivirus payant, à jour et dont la licence est en cours de validité ?
OUI X NON ?

Imposez-vous une mise à jour trimestrielle des mots de passe de vos collaborateurs ?
OUI X NON ?

Avez-vous mis en place des règles de sécurisation des mots de passe ?
OUI X NON ?

Vos collaborateurs sont-ils sensibilisés aux risques numériques et à leurs conséquences ?

Plusieurs réponses possibles
- Des simulations d'attaques par phishing (hameçonnage) ? OUI ? NON X

- Des formations présentiels ou e-learning ? OUI X NON ?

- La diffusion de guide de bonnes pratiques ? OUI X NON ?

Avez-vous mis en place une politique ou une charte de sécurité informatique formalisée, pilotée et régulièrement communiquée à l'ensemble de vos collaborateurs ?
OUI X NON ?

[08/04/2025 à 10:35:49] LOT CYBER
Merci de répondre aux questions ci-dessous :
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 :

Activités :
Exercez-vous une activité dans les domaines suivants :
- Plateformes de monnaie virtuelle et de crypto-monnaie ;
- Organisations de jeux de hasard et d’argent ;
- Transports aériens ou maritimes (y compris aéroports et ports) ;
- Entreprises de production et de distribution d'eau ;
- De gaz et d'électricité ;
- Sociétés de télécommunications.

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 :
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 évènements 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 évènements 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 ?
? 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.)

Questions / Réponses

[24/04/2025 17:36:30] Mesdames, Messieurs,

Veuillez trouver ci-après les réponses aux questions concernant le lot Cyber :

Société / Collectivité : Mairie de Les Noës-près-Troyes
Siret : 211 002 571
Nombre d'employés : 46
Chiffre d'affaires / Budget de fonctionnement : 3 746 656.81 €
Code NAF :
Nom de domaine : lesnoes.com
Nom du représentant dûment autorisé par la société : Le Maire, Philippe LEMOINE

Activités :
Exercez-vous une activité dans les domaines suivants :
- Plateformes de monnaie virtuelle et de crypto-monnaie : NON
- Organisations de jeux de hasard et d'argent : NON
- Transports aériens ou maritimes (y compris aéroports et ports) : NON
- Entreprises de production et de distribution d'eau : NON
- De gaz et d'électricité : NON
- Sociétés de télécommunications : NON

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.
OUI
2) Tous vos équipements sont-ils équipés d'un antivirus à jour ?
X Vos postes de travail Windows ?
X 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.
OUI Mailinblack

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

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.
Toutes les mises à jour recommandées sont réalisées.

Sauvegarde des données et restauration :
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.
4 sauvegardes par jour dans le cloud. 2 serveurs (dont un externalisé : 1 sauvegarde par jour)

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

Sécurité des systèmes :
8) Disposez-vous d'une journalisation (logs) des évènements 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 ?
OUI 90 jours de rétention.

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

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.
OUI

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.
OUI

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

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

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 ?
OUI

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

16) L'ensemble de vos mots passe sont-ils robustes (min 15 caractères incluant des capitales, minuscules, chiffres et caractères spéciaux.) ?
Préconisations de l'ANSSI appliquée à savoir 12 caractères minimum

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

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

19) Quel volume de données traitez-vous ? Environ 1 To
• Volumes donnés à caractère personnel sensibles ?
X Volume données bancaires ? OUI stockés sur les serveurs externalisés du prestataire et correspondant à environ 5/6Go
? Volume données de santé ? NON

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.)
Bitlocker sur les principaux postes