REGISTRE DES QUESTIONS

INFORMATIONS CONCERNANT L'ANNONCE

Collectivité :	Commune de Xertigny
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 :	M06-2024
Date de mise en ligne :	Le vendredi 02 août 2024 à 17:50:01
Date de clôture :	Le vendredi 20 septembre 2024 à 12:00:00
Titre :	Renouvellement des Contrats d'Assurance de la Ville de Xertigny
Descriptif :	La présente consultation concerne le renouvellement en 5 lots des contrats d’assurance de la Ville de Xertigny pour une durée de 5 ans à compter du 01/01/2025.

REGISTRE DES QUESTIONS / REPONSES REPONDUES

Questions / Réponses

Questions / Réponses

[11/09/2024 à 11:46:45] 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,

La commune et son CCAS partagent-elles le même système d'information que la structure 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 ?
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 ?

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 ?

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 ?

Utilisez-vous un antivirus payant, à jour et dont la licence est en cours de validité ?
OUI ? NON ?
Si non, utilisez-vous un antivirus gratuit avec mise à jour régulière ?
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 ?
OUI ? NON ?
Si OUI, précisez les dispositifs déployés dans votre entreprise :
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

[12/09/2024 11:57:13] Bonjour,
Pour répondre à de nouvelles questions qui nous ont été posées concernant le lot Cyber-Risques, vous trouverez ci-dessous un complément d'informations :

La commune et son CCAS partagent-elles le même système d'information que la structure à assurer ?
OUI X NON ? (à noter que le CCAS de Xertigny n'est pas une entité propre en tant que telle, la gestion est faite directement par les mêmes agents que la commune / il y a certes un budget indépendant, toutefois assez réduit à hauteur de 21 576 € en fonctionnement) / les documents sont sauvegardés sur le même serveur que la mairie (l'activité étant très restreinte).

Au cours des 5 derniers années, avez-vous déjà été victime de cyber attaques vous ayant causé des préjudices financiers ?
OUI ? NON X

Combien de postes informatiques possédez-vous ? ? De 0 à 20 X De 21 à 50 ? Plus de 50
A l'hôtel de ville, il y en a 12 / 1 aux ateliers municipaux / 4 à l'école maternelle / une dizaine à l'école primaire

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 ? NON ?
Ne sait pas, toutefois le site internet devrait entièrement remodelé d'ici la fin d'année avec un nouveau prestataire.

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

- 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 ? 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 ?
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 ?

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 ?

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

Si non, utilisez-vous un antivirus gratuit avec mise à jour régulière ?
OUI ? NON ?

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

Avez-vous mis en place des règles de sécurisation des mots de passe ?
OUI ? NON X
Suivi de ce qui est imposé par les plateformes directement (pour certaines, il y a lieu de changer régulièrement, pour d'autres, effectivement les mots de passe ne sont pas changés régulièrement).

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

Si OUI, précisez les dispositifs déployés dans votre entreprise :
Plusieurs réponses possibles
- Des simulations d'attaques par phishing (hameçonnage) ? OUI ? NON X

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

- 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 ? NON X
Toutefois souhait de pouvoir y procéder (en cours de rédaction d'un document en la matière)

Vous en souhaitant une bonne réception, ainsi qu'une bonne journée,

La Ville de Xertigny

Questions / Réponses

[06/08/2024 à 12:57:51] 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 ;
- Divertissements pour adultes ;
- Vente d'armes, de drogue, vente de substances et produits illicites ;
- 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

[22/08/2024 17:36:09] Bonjour,

Merci de bien vouloir trouver, ci-après, la réponse à un questionnaire relatif aux Cyber-Risques qui nous a été transmis.

Fiche de Déclaration du Risque
Société / Collectivité : Commune de Xertigny
SIRET : 21880530700012
Nombre d'employés : 35 employés et 23 élus (dont 1 Maires et 9 Adjoints et Conseillers Délégués)
Chiffre d'affaires / Budget de fonctionnement : 4 194 000 €
Code NAF : 8411Z
Nom de domaine : https://www.mairie-xertigny.fr/ / @mairie-xertigny.fr
Nom du représentant dûment autorisé par la société : Véronique MARCOT, Maire

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 ;
- Divertissements pour adultes ;
- Vente d'armes, de drogue, vente de substances et produits illicites ;
- 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.
NON aucune de ces activités.

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 ?
? Vos postes de travail Windows ? OUI
? Vos serveurs Windows ? OUI

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.
Antivirus ESET + Filtrage Pare-feu Zyxell avec Abonnement UTM

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

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.
Mises a jour automatiques Windows
Sur les PC, les MAJ sont automatiques, sur le serveur aussi mais nous avons aussi une alerte en cas de MAJ non effectuée (qui nécessiterait un redémarrage à faire avant le redémarrage hebdomadaire).

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.
Sauvegardes Quotidiennes Acronis (Serveur distants basés en France)

7) A quelle fréquence effectuez-vous des tests de restauration à partir de vos sauvegardes ? Précisions éventuelles sur les tests de restauration.
1x par semaine – systématiquement en cas d'erreur

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

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.
A notre niveau (réponse du prestataire informatique) a priori pas de système critique (hors Cosoluce)

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.
S'agissant du partage de fichiers, les droits sont mis en place en fonction des niveaux communiqués par la collectivité au prestataire informatique.

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 ?
OUI

16) L'ensemble de vos mots passe sont-ils robustes (min 15 caractères incluant des capitales, minuscules, chiffres et caractères spéciaux.) ?
NON, suivi des instructions que chaque plateforme demande avec assez régulièrement la réutilisation des mêmes mots de passe par les agents

17) Les ports RDP (Remote Desktop Protocol) de votre réseau sont-ils fermés ?
OUI pour le serveur.
NON pour les postes, ils sont utilisés depuis l'extérieur en VPN.

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 ?
• Volumes donnés à caractère personnel sensibles ?
? Volume données bancaires ? à travers notre logiciel compta et paie (COSOLUCE)
? Volume données de santé ? à travers des plateformes mises en place par les partenaires (uniquement liées aux agents)

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.)
Hormis la sauvegarde cryptée, il n'y en a pas.

Vous souhaitant une bonne réception du présent questionnaire rempli et restant à votre disposition si besoin,

La Ville de Xertigny