QUESTIONS CYBER

Société / Collectivité : Commune de Névez

SIRET : 21290153200011

Contact Société / Collectivité : DGS, Madeleine BOUGUENNEC

Nombre d'employés : 47

Chiffre d'affaires / Budget de fonctionnement : 4 195 560,00 €

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 ; NON
- Organisations de jeux de hasard et d'argent ; NON
- Divertissements pour adultes ; NON
- Vente d'armes, de drogue, vente de substances et produits illicites ; 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 nous avons un suivi du parc qui comprend le maintien des systèmes sur des versions à jour par les editeurs tel que microsoft et autres.

2) Tous vos équipements sont-ils équipés d'un antivirus à jour ?
   - ☐ Vos postes de travail Windows ?
   - ☐ Vos serveurs Windows ?

Oui, nous sommes en cours de migration sur l'EDR ESET.

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 nous utilisons Vade secure sur notre système de messagerie.

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, nous utilisons des firewalls de marque fortinet.

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.

   Ces mises à jour sont faites automatiquement pour les systèmes d'exploitation.

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.

Nous respectons la regle 3-2-1 recommandée en terme de stratégie de sauvegarde (3 jeux de sauvegarde, 2 supports, 1 externalisé).

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

Uniquement à la demande des utilisateurs, à peu près 2 à 3 fois par an pour des simples restaurations de fichiers.

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 nous avons l'activation de l'audit de journalisation sur les serveurs ainsi qu'une solution type SIEM. Nous avons aussi une journalisation sur les parefeux.

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.) ?

Nous sommes en cours de déploiement du nouvel EDR Eset et nous avons différents systèmes de journalisation sur les serveurs, firewalls et autres.

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.

Nous sommes en cours de déploiement d’un système MFA pour les accès des administrateurs de la DSI sur l’infra serveur critique.

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 pour les serveurs gérés par la DSI.

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

Oui cela est en place, aucun utilisateur n’a de droits administrateurs. Seule la DSI possède ces droits avec des comptes séparés.

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 pas encore, aujourd’hui c’est 12 caractères mais le passage à 15 est prévu au 1er janvier 2025.

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

Oui depuis l’exterieur.

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 ?

X Volumes donnés à caractère personnel sensibles ? oui

☐ Volume données bancaires ? non

☐ 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.)

Nous menons un plan d'action de conformité suite à un audit de sécurité réalisé en 2021. Nous suivons le guide de préconisation ANSSI également.

De nombreuses mesures sont mises en places sur la sécurisation du réseau informatique de la mairie. En 2025 , nous prévoyons la mise en place de coffre fort des mots de passe et augmenter la complexité des mots de passe.

Une PSSI a également été validée à l'échelle du territoire de CCA car le service DSI est commun.