**QUESTIONNAIRE ANALYSE RISQUES CYBER**

**INFORMATIONS GENERALES**

Organisation : MAIRIE DE BOUILLARGUES

N°Siret : 213 000 474 00014

ape : 84 11z

~~Date de création : ……………………….~~

Site Internet ou Nom de domaine : www.bouillargues.fr

Adresse du risque principal : …………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

Activité principale :

Collectivité locale, échelon communale

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

Autres activités :

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

Nombre de salariés : entre 50 et 70

Budget de fonctionnement : 9 millions (€) de l’année 2024 (y compris opérations d’ordre)

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

OUI  NON

**GOUVERNANCE RISQUES CYBER**

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

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

**MOYENS DE PROTECTION ET DE SECURITE NUMERIQUES**

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

Pour les clients avec un chiffre d’affaires inférieur à 50 000 000 €

* 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

* Sur des supports **déconnectés** des postes informatiques ?

OUI  NON

~~Si chiffre d’affaires supérieur à 50 000 000 € :~~

* ~~Sur des~~ **~~supports sécurisés par chiffrement ou par multiplication~~** ~~des supports ?~~

~~OUI  NON~~

* ~~Sur des supports~~ **~~testés~~** ~~au moins une fois par an ?~~

~~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 ?~~

~~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 complémentaires pour les entreprises avec un chiffre d’affaires supérieur à 50 000 000 € :~~

~~Les autorisations d'accès de vos utilisateurs privilégiés sont-elles tracées, contrôlées et tenues à jour ?~~

~~OUI  NON~~

~~Utilisez-vous une authentification mutificateurs (MFA) afin de protéger les comptes d’utilisateurs privilégiés ou des administrateurs ?~~

~~OUI  NON~~

~~Avez-vous déployé un Endpoint Detection and Response (EDR) ou un Managed Detection and Response~~

~~(MRD) sur l’ensemble des équipements informatiques de votre entreprise ?~~

~~OUI  NON~~

~~Un inventaire des actifs du parc informatique (équipements, logiciels, données, accès, etc.) a-t-il été réalisé et maintenu à jour ?~~

~~OUI  PARTIELLEMENT  NON~~

~~Listez les mesures mises en place pour sécuriser les données sensibles de votre entreprise (ex: données chiffrées, blocage des ports USB, etc.) ?~~

~~....................................................................................................................................................................................................................................................................................................................................................................~~

~~Avez-vous mis en place l'authentification multi facteurs (MFA) à minima sur l'ensemble des :~~

~~- populations à privilèges (privilèges techniques et / ou métiers),~~

~~- accès à distance au réseau (hébergé dans le cloud et sur site, y compris via des réseaux privés virtuels (VPN)),~~

~~- accès des prestataires ?~~

~~OUI  PARTIELLEMENT  NON~~

~~La gestion des accès et des identités de vos utilisateurs est-elle strictement basée sur le principe du “moindre privilège” ?~~

~~OUI  NON~~

~~Vos utilisateurs sont-ils administrateurs de leurs postes de travail ?~~

~~OUI  NON~~

~~Chaque utilisateur dispose-t-il de compte nominatif pour se connecter aux applications métier et aux systèmes critiques de l'entreprise ?~~

~~OUI  NON~~

~~Vos accès distants sont-ils sécurisés par un VPN ou dispositif équivalent ?~~

~~OUI  NON~~

~~L'ensemble des mots de passe sont-ils robustes (min 12 caractères incluant des capitales, minuscules, chiffres et caractères spéciaux) ?~~

~~OUI  NON~~

~~Les logiciels et OS que vous utilisez sont-ils toujours maintenus par leurs éditeurs ? (ex : pas de version Windows antérieure à Windows 10) ?~~

~~OUI  PARTIELLEMENT  NON~~

~~Vos PC Windows et serveurs Windows sont-ils équipés d'un antivirus maintenu à jour ?~~

~~OUI  PARTIELLEMENT  NON~~

~~Avez-vous activé un pare-feu sur tous vos systèmes exposés à l'extérieur de votre réseau ?~~

~~OUI  PARTIELLEMENT  NON~~

~~Précisez la solution utilisée………………..~~

~~Avez-vous mis en place une solution d'anti-phishing ?~~

~~OUI  NON~~

~~Quelle est la fréquence de mise en œuvre des correctifs de sécurité après sa publication par les éditeurs ?~~

~~Automatiquement ou sous 7 jours quand il n’y a pas de màj automatique~~

~~Sous 15 jours quand il n’y a pas de màj automatique~~

~~Sous 30 jours quand il n’y a pas de màj automatique~~

~~Pas de procédure de màj automatique ou moins d’1 fois par mois~~

~~Avez-vous mis en place des règles qui empêchent l’utilisation du protocole RDP pour se connecter aux postes de travail ?~~

~~OUI  NON~~

~~Avez-vous mis en place une solution de collecte et de corrélation des logs permettant de retracer l'historique d'une attaque (ex: SIEM) ?~~

~~OUI  NON~~

~~Avez-vous mis en place des systèmes de sécurité des points d'accès (ex: EDR, MDR, etc.) qui permettent de prévenir et détecter les activités malveillantes sur votre réseau ?~~

~~OUI  NON~~

~~Indiquez la solution utilisée………………….~~

~~À quelle fréquence vos données sont-elles sauvegardées sur des supports déconnectés de votre réseau (ex : bandes, Cloud, etc.) ?~~

~~Moins de 24h~~

~~Moins de 7j~~

~~Moins de 15j~~

~~Moins de 30j~~

~~Jamais ou moins d’une fois par mois~~

~~Précisez votre système de sauvegarde………………~~

~~À quelle fréquence effectuez-vous des tests de restauration de vos sauvegardes ?~~

~~Plusieurs fois par an~~

~~Une fois par an~~

~~Moins d’une fois par an~~

~~Pas de tests de restauration~~

AFC Consultants – 345 Rue Pierre Seghers – Le concorde – 84000 Avignon

Sarl au capital de 50 000 € - RCS AVIGNON – SIRET 487 785 545 00012 – ORIAS 07028063 - NAF 7022Z - TVA FR00 487 785 545

Exerçant dans le cadre des articles L521-2-II-1-c & L521-2-II-2-a du Code des Assurances sans encaissement de fonds destiné à payer/rembourser des primes/cotisations d'assurance ou à l'indemnisation d'un préjudice/sinistre

Assurance de responsabilité civile professionnelle conforme aux articles L.512-6 R.512-14 & A.512-4 du Code des Assurances

Profession réglementée par les articles 4 & 10 de l'ordonnance 2018-361 du 16/05/2018 ainsi que par l'article 59 de la Loi n° 71-1130 du 31/12/1971

Procédure de réclamation : contact@afc-consultants.fr - recours au processus de médiation : lemediateur@cnscra.fr

Sous le contrôle de l'ACPR 4 Place de Budapest CS 92459 75436 PARIS CEDEX 09 - Inscription au registre unique tenu par l’ORIAS vérifiable sur www.orias.fr