

QUESTIONNAIRE ANALYSE RISQUES CYBER

INFORMATIONS GENERALES

Informations générales

Nom/Raison sociale :		
N° Siren/Siret :		
Adresse du risque principal :		
NAF :		
Activité principale :		
Autres activités :		
Site Internet ou Nom de domaine :		
Chiffre d'affaires (CA) :€	<input type="checkbox"/> N/A
Budget de fonctionnement : (hors investissement)€	<input type="checkbox"/> N/A
Le taux de marge brute		
Nombre de salariés :		
Nombre de postes de travail :		

Traitement des données

Est-ce que vous collectez, traitez et stockez :	OUI <input checked="" type="checkbox"/> NON <input type="checkbox"/>
---	--

Moins de 250 000 données à caractère personnel au sens du RGPD ; et
 Moins de 250 000 données bancaires (numéros de cartes bancaires ou RIB) ; et
 Moins de 250 000 données à caractère sensible au sens du RGPD (notamment les données médicales)

SI REPONSE NEGATIVE MERCI DE PRECISER LA VOLUMETRIE

.....

.....

Antécédent

Avez-vous (ou tout autre proposant, y compris tout administrateur, dirigeant ou employé) connaissance d'un fait, d'une circonstance, d'une situation, d'un événement ou d'une transaction qui pourrait donner lieu à une réclamation, à une perte ou à l'obligation de notifier une violation dans le cadre de l'assurance proposée	OUI <input checked="" type="checkbox"/> NON <input type="checkbox"/>
---	--

Au cours des cinq dernières années, avez-vous :

Reçu des réclamations ou des plaintes concernant la protection de la vie privée, la violation d'informations, la violation de la sécurité du réseau ou la divulgation non autorisée d'informations ?	OUI <input type="checkbox"/> NON <input checked="" type="checkbox"/>
Fait l'objet d'une action gouvernementale, d'une enquête ou d'une citation à comparaître concernant la violation présumée d'une loi ou d'un règlement relatif à la protection de la vie privée ?	OUI <input type="checkbox"/> NON <input checked="" type="checkbox"/>

Notifié vos clients ou toute autre tierce partie d'une violation de données ?

OUI ☐ NON ☒

Fait l'objet d'une demande d'extorsion réelle ou d'une tentative d'extorsion (y compris par un rançongiciel) en ce qui concerne vos systèmes informatiques ?

OUI ☐ NON ☒

Informations complémentaires

Acceptez-vous les cartes de paiement pour les biens vendus ou les services rendus ?	OUI <input checked="" type="checkbox"/> NON <input type="checkbox"/>
Si OUI, *Assurez-vous le chiffrement bout en bout des données relatives aux cartes de paiement ?	OUI <input checked="" type="checkbox"/> NON <input type="checkbox"/>
*Conservez-vous les données relatives aux cartes de paiement sur votre réseau ?	NON <input checked="" type="checkbox"/> OUI, sans chiffrement <input type="checkbox"/> OUI, avec jeton ou chiffrement <input type="checkbox"/>
Avez-vous, au cours des 12 derniers mois, réalisé ou accepté une fusion, une acquisition ou une consolidation ?	<input type="checkbox"/> OUI <input checked="" type="checkbox"/> NON Si « oui », veuillez fournir des détails :
Merci de lister l'ensemble des noms de domaine utilisés par votre organisation. -univ-montp3.fr -umpv.fr - - - - - -	

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 ☐

VOTRE CYBER GOUVERNANCE

1. Quelles mesures de sécurité sont mises en place pour les e-mails entrants ?

- ☒ Filtrage des pièces jointes malveillantes
☒ Filtrage des liens malveillants
☐ Marquage des e-mails externes

2. A quelle fréquence conduisez-vous la formation suivante pour tous les employés ?

- | | | | |
|----------------------------|---|--|--|
| E-learning sur le phishing | <input type="checkbox"/> Jamais/pas régulièrement | <input checked="" type="checkbox"/> Annuellement | <input type="checkbox"/> >2x par an |
| Campagne de phishing | <input type="checkbox"/> Jamais/pas régulièrement | <input type="checkbox"/> Annuellement | <input checked="" type="checkbox"/> >2x par an |

3. Exigez-vous une authentification multifacteur (MFA) pour accéder à distance à votre réseau (hébergé dans le cloud et sur site, y compris via des réseaux privés virtuels [VPN])?

- ☐ OUI ☒ NON ☐ ACCES A DISTANCE NON AUTORISE

Si NON, est ce prévu prochainement ? OUI ☒ NON ☐

Planning prévisionnel ? ...second semestre 2025.....

4. L'accès à l'e-mail professionnel via une application Web nécessite-t-il une authentification multifacteur (MFA)?

- ☐ OUI ☒ NON ☐ ACCES A DISTANCE NON AUTORISE/ PAS DE WEBMAIL

Si NON, est ce prévu prochainement ? OUI ☒ NON ☐

Planning prévisionnel ? second semestre 2025.....

5. Parmi les solutions de cloud suivants, lesquels sont utilisés par vous?

- ☒ Active Directory
☐ AWS
☐ GCP
☐ Azure
☐ Autre

6. Quelles solutions de sécurité utilisées pour détecter ou empêcher les activités malveillantes sur votre réseau ?

- ☐ Antivirus (plate-forme de protection des terminaux - EPP) →
☒ Détection et réponse des terminaux (EDR) →SentinelOne.....
☐ Déploiement d'un XDR →
☒ Outil de Gestion des informations et des événements de sécurité (SIEM) →Siem ELK.....

7. Avez-vous un service SOC (Centre Opérationnel de Sécurité) ?

- ☐ OUI, 24/7 ☐ OUI, heures de travail seulement ☒ NON
☐ Interne ☐ Externe

Si NON, avez-vous paramétré votre EDR en mode détection automatique afin d'isoler automatiquement les postes en cas d'alerte de sécurité ?

- ☐ OUI ☒ NON

8. Fréquence de sauvegardes des données critiques :

- ☒ Journalier
☒ Hebdomadaire
☒ Mensuelle

9. Vos sauvegardes sont hébergées :

- ☒ Sur votre réseau d'entreprise
☐ Sur le cloud
☐ hors ligne, complètement déconnectées
☐ Autres

Si « sur cloud »,

a. Votre service de sauvegarde basé sur le cloud est-il un « service de replication automatique » (syncing services) ? (Par exemple, DropBox, OneDrive, SharePoint, Google Drive)

☐ OUI ☐ NON

10. Vos sauvegardes sont -elles ?

- | | | |
|-------------|---|--|
| Sécurisées* | <input checked="" type="checkbox"/> OUI | <input type="checkbox"/> NON |
| Immuables | <input checked="" type="checkbox"/> OUI | <input type="checkbox"/> NON |
| Chiffrées | <input type="checkbox"/> OUI | <input type="checkbox"/> PARTIELLEMENT <input checked="" type="checkbox"/> NON |

** Une copie des données et éléments critiques du système informatique, réalisée sur un élément physique vous appartenant et isolé de l'Active Directory, dont l'accès est restreint au travers d'un pare-feu n'autorisant que :
un flux d'envoi de sauvegardes depuis une liste limitée de serveurs ; et
un accès aux sauvegardes par une interface web protégée par une authentification multi-facteur (MFA).*

11. À quelle fréquence effectuez-vous un test de restauration à partir des sauvegardes ?

- ☐ Jamais/non régulièrement ☒ 1 fois par an ☐ 2 à 3 fois par an ☐ Chaque trimestre ou plus souvent

12. Est-ce qu'un Plan de Reprise d'Activité (PRA) couvrant le risque cyber :

- est formulé et documenté avec des indications claires sur le processus de restauration des sauvegardes déconnectées, immuables ou sécurisées ; et
- prévoit un délai de reprise inférieur à 72 heures ?

☐ OUI ☒ NON

13. La gestion des accès et des identités de vos utilisateurs est-elle strictement basée sur le principe du "moindre privilège" ?

OUI ☒ NON ☐

14. Vos utilisateurs sont-ils administrateurs de leurs postes de travail ?

OUI ☐ NON ☒

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

OUI ☒ NON ☐

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

OUI ☒ NON ☐

17. Votre environnement intègre-t'il une technologie opérationnelle (OT) ?

☒ OUI

☐ NON

SI OUI

a. Votre SI industriel (OT) est-il segmenté du reste du réseau informatique (IT)?

☒ OUI

☐ NON

b. Votre SI industriel (OT) est-il isolé d'Internet?

☐ OUI

☒ NON

c. Vos employés utilisent-ils une authentification multifacteur pour accéder à distance à votre environnement OT?

☐ OUI

☒ NON

☐ ACCES DISTANT NON AUTORISE

d. Les tiers utilisent ils une authentification multifacteur pour accéder à distance à votre environnement OT?

☐ OUI

☒ NON

☐ ACCES DISTANT NON AUTORISE

QUESTION FRAUDE CYBER

Les employés chargés de débloquer ou de transmettre des fonds reçoivent-ils une formation anti-fraude, notamment en matière de détection de l'ingénierie sociale, d'hameçonnage, de compromission des e-mails professionnels et d'autres escroqueries, au moins une fois par an ?

OUI ☒

NON ☐

Lorsqu'un fournisseur ou un sous-traitant demande à modifier les données de son compte (y compris les numéros d'acheminement et les numéros de compte), confirmez-vous les changements demandés par une authentification hors bande (une autre méthode que celle de la demande initiale) ? Par exemple, lors d'une demande par e-mail, un appel téléphonique de suivi permet de confirmer que le fournisseur ou le sous-traitant en est bien à l'origine.

OUI ☒

NON ☐

Veuillez utiliser l'espace ci-dessous pour clarifier les réponses ci-dessus qui pourraient être incomplètes ou nécessiter des détails complémentaires. Veuillez également décrire toutes les mesures prises par votre organisation pour détecter, prévenir et remédier aux attaques rançongiciels (par exemple, segmentation de votre réseau, contrôles de sécurité logiciels supplémentaires, services de sécurité externes, etc.).

.....

.....

.....

.....