**QUESTION ANALYSE RISQUES CYBER**

|  |  |  |
| --- | --- | --- |
| **Informations générales** | | |
| Nom/Raison sociale : | Université Bretagne Sud | |
| N° Siren/Siret : | ***19561718800600*** | |
| Budget de fonctionnement global : (hors investissement) | 23,5M€ dont 8,6 M€ d’amortissement | N/A |
| Nombre de salariés : | Environ 2000, et 15 000 étudiants | |
| Nombre de postes de travail : | Environ 3000 | |
|  |  | |

|  |  |
| --- | --- |
| **Traitement des données** | |
| Est-ce que vous collectez, traitez et stockez : | OUI  NON |

*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** | |
| Au cours des 5 derniers années, avez-vous déjà été victime de cyber attaques vous ayant causé des préjudices financiers ? | OUI  NON |
| Si oui, précisez pour chacune d’elles :  Date : ……………………  Nature de l'intrusion ............................................................................................................................................  Dommages subis ? ...................................................................................................................................................  Montant Préjudices financiers ? ..............................................................................................................................  Pourriez-vous nous préciser les conséquences de cette tentative d’attaque / attaque sur votre système d’information ?  Arrêt du système d’information ? Si oui pendant quelle durée ?  Est-ce que le sinistre était garanti par un autre assureur ? Montant de l’indemnisation ?  Merci de nous préciser tout ce qui a été mis en place afin d'éviter que cela ne se reproduise ?  ………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… | |

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

*UBS (sauf si les composantes en BPI disposent d’une identité juridique propre ?).....................................................................................................................................................................................................................................................................................................*

*Ces entités partagent-elles le même système d’information que la structure principale à assurer ?*

*OUI  NON*

VOTRE EXPOSITION

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, vos clients ou vos fournisseurs ?

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

(\*) 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.

VOTRE CYBER GOUVERNANCE

1. Merci de confirmer quelles solutions techniques sont déployées pour protéger l'ensemble des postes de travail et serveurs (sélectionner l’ensemble des mesures en place) :

|  |
| --- |
| Solution Antivirus payante mise à jour régulièrement **(sous 15j)**  Solution firewall  Solution de Filtrage réseau  Solution EDR  Solution EDR managé au sein d’un SOC , Si SOC est-il INTERNE EXTERNE24/7  Aucune des mesures de protection listées ci-dessus |
|  |

1. Merci de confirmer quelles mesures de sécurité de la messagerie sont en place

(Sélectionner l’ensemble des mesures en place) :

|  |
| --- |
| Solution anti SPAM (2)  Service de quarantaine pour les emails suspects  Capacité d'ouvrir les pièces jointes et les liens dans un Bac à sable (solution sandboxing)  Aucune des mesures de protection listées ci-dessus |

1. Est-il possible d’accéder à distance à tout ou partie du réseau (y compris votre service de messagerie) de la société proposante et ses filiales ?

OUI  NON

Si OUI,

* Utilisez-vous une solution VPN pour l’ensemble de ces accès à distance ?

OUI  NON

* Avez-vous recours à la vérification en deux étapes - A2F/MFA - pour l’ensemble de ces accès à distance ?

OUI  NON

1. Exigez-vous l’authentification multifacteur (MFA) pour l’accès à distance à la messagerie Web ?

OUI PARTIELLEMENT NON ACCES A DISTANCE NON AUTORISE

1. Les accès à distance au système informatique au réseau de l’entreprise, aux emails dans le **Cloud** et à tout compte d’administration d’un environnement **Cloud** nécessitent-ils tous une authentification à deux facteurs (2FA) ?

OUI  NON

Préciser si à nuancer Comptes administrateurs uniquement………………………………………………………………………………………………………………………………………………

Si NON, est ce prévu prochainement ? OUI  NON

Planning prévisionnel ? Projet en cours de généralisation du MFA………………………………………………………………………………………………………

1. Utilisez-vous de systèmes d'exploitation dont les mises à jour ne sont plus supportées par leur fabricant (par exemple Windows XP et Windows 7) ?

OUI  NON

1. A quelle fréquence sensibilisez-vous tous les employés ?

Diffusion de guide de bonnes pratiques  pas régulièrement  Annuellement >2x par an

E-learning sur le phishing  pas régulièrement  Annuellement >2x par an

Campagne de phishing pas régulièrement Annuellement >2x par an

1. 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

1. 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

1. Imposez-vous une mise à jour trimestrielle des mots de passe de vos collaborateurs ?

OUI  NON

1. Avez-vous mis en place des règles de sécurisation des mots de passe ?

OUI  NON

1. Avez- vous un système d'information industriel ?

OUI NON

**SI OUI,**

1. 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

1. Effectuez-vous au moins des sauvegardes avec une rétention minimale de 2 semaines, pour les données et les éléments critiques de votre système informatique ?

OUI NON

Fréquence de vos sauvegardes ?

JOURNALIERE  HEBDOMADAIRE  AUTRE (préciser)   
……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………..

1. Vos sauvegardes sont-elles :

Sur des supports de stockage conservés en dehors des locaux de l'entreprise ?

OUI  NON

Avec des services sur internet configurés pour réaliser des sauvegardes informatiques ?

OUI  NON

Sécurisées (4)  OUI  NON

Déconnectées OUI  NON

Externalisée, hors site OUI  NON

Sur Cloud service OUI  NON  Nom de la solution ……………

Immuables OUI  NON

Air-gapped (5) OUI  NON

Testées au moins une fois par an  OUI  NON

Quel est votre délai de rétention des sauvegardes ?

3 mois en moyenne

Autres précisions :

…………………………………………………………………………………………………………………………………………………………….

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

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

**DEFINITIONS**

1. SOLUTION EDR

Détection et réponse des terminaux (EDR) est une solution de sécurité des terminaux qui inclut la surveillance en temps réel et la collecte des données de sécurité des terminaux avec un mécanisme de réponse automatisée aux menaces.

1. SOLUTION ANTI SPAM

Pour une entreprise, l’utilisation d’un filtre anti-spam est bénéfique en termes de sécurité, de rentabilité et de commodité. Les logiciels anti-spam servent à filtrer les messages reçus sur un compte de messagerie électronique en vue de supprimer les courriers indésirables. Ils peuvent filtrer les emails de phishing, les spams commerciaux et autres arnaques par email.

1. A2F/MFA

L’authentification multi-facteurs (MFA), est un processus de sécurité qui nécessite deux ou plusieurs facteurs de vérification pour prouver l’identité d’un utilisateur. Le plus souvent, cela implique de se connecter à un réseau, une application ou une autre ressource sans se contenter d’une simple combinaison ID + mot de passe.

L'authentification multi Facteurs comprend, sans s'y limiter, les éléments suivants : appel, SMS, notification push, mot de passe à usage unique basé sur le temps, jeton OATH, jeton matériel, applications d'authentification, biométrie ou clé FIDO2 (par exemple, YubiKey, RSA SecurID).

1. Sauvegardes sécurisées :

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).

1. Air-gapped :

Ressource dont l'accès par une connexion externe est impossible, nécessitant un accès physique (par exemple un média isolé tel qu'une bande ou un disque extractible)