Annexe CGV - Devoir de Conseils : Recommandations

1 Objet

Le client a souscrit ou envisage de souscrire un contrat avec La SOCIETE pour l'intégration de solutions professionnelles liées aux compétences et métiers proposés par cette dernière. De plus, le client fait appel ou envisage de faire appel aux services de La SOCIETE afin d'assurer le maintien en condition opérationnelle de tout ou partie de son système d'information et de communication. Dans un monde de plus en plus connecté, la sécurité des systèmes d'information est devenue une priorité absolue pour toutes les organisations.

Aussi, dans le cadre de ses activités, La SOCIETE qui fournit des services IT se doit de fournir des conseils avisés et pertinents à ses clients afin de les aider à atteindre leurs objectifs technologiques et commerciaux. Ce devoir de conseil repose sur plusieurs principes fondamentaux détaillés ci-dessous.

Chaque item abordé ci-dessous est associé à un identifiant unique (ID) : dans le cadre de l'élaboration d'une offre commerciale au Client, les ID liés à cette dernière sont alors précisés. Le Client doit alors se référer à ce présent document pour prendre connaissance des recommandations.

ID	Recommandation

A la demande du Client, ces recommandations sont associées à une analyse plus approfondie avec l'assistance d'un professionnel en mesure d'expliquer ces éléments quelque fois techniques, et de conseiller sur les bonnes pratiques à mettre en œuvre. Cette étude fait alors l'objet d'un nouveau livrable « ANNEXE CGV_ Devoir de Conseils Synthèses ».

2 Nos recommandations

2.1 Sensibilisation et Formation

2.1.1 *Former les employés :*

PHISH01	Organiser des sessions de formation régulières pour sensibiliser les employés aux risques de cybersécurité et aux bonnes pratiques.

2.1.2 *Simulations d'attaques :*

PHISH02	Réaliser des exercices de simulation d'attaques pour préparer les équipes à réagir efficacement en cas d'incident.

2.2 Protection des Systèmes et des Données

2.2.1 *Mises à jour régulières :*

PATCH01	Assurer la mise à jour régulière des logiciels et systèmes d'exploitation pour corriger les vulnérabilités (sur les serveurs physiques et virtuels, les postes de travail)

2.2.2 *Antivirus, EDR, xDR :*

XDR01	Installer et maintenir à jour des solutions antivirus EDR xDR pour protéger les systèmes contre les malwares et autres menaces.

2.2.3 *Pare-feu :*

FW01	Installer et maintenir à jour des pares-feux **qualifiés** pour protéger les systèmes contre les malwares et autres menaces.

Un pare-feu qualifié doit répondre à plusieurs critères techniques pour garantir une protection optimale des systèmes d'information, dont voici quelques caractéristiques essentielles :

- *Inspection approfondie des paquets (DPI) : Capacité à analyser le contenu des paquets de données pour détecter et bloquer les menaces.*

- *Gestion des accès : Contrôle strict des accès aux ressources réseau, basé sur des règles définies par l'administrateur.*
- *Détection et prévention des intrusions (IDS/IPS) : Intégration de systèmes pour détecter et prévenir les tentatives d'intrusion.*
- *Journalisation et reporting : Enregistrement détaillé des événements et génération de rapports pour l'analyse et la conformité.*
- *Mises à jour régulières : Capacité à recevoir et appliquer des mises à jour de sécurité pour contrer les nouvelles menaces.*
- *Certification et qualification : Conformité aux normes de sécurité telles que la qualification ANSSI, la certification critères communs, ou la certification CSPN.*

Ces caractéristiques permettent de renforcer la sécurité des systèmes d'information en assurant une protection contre une large gamme de menaces.
Un routeur qui fait office de pare-feu a généralement juste la fonctionnalité de gestion des accès, et la plupart du temps, de manière assez limitée, et n'est pas efficace face à la gestion du risque.

2.2.4 *Email Protection :*

EP01	Installer et maintenir à jour une solution d'Email Protection type antispam pour la protection des vos emails reçus et envoyés.

EP02	Renforcer la sécurité des courriels et protéger les domaines contre les usurpations d'identité et les activités frauduleuses (DMARC)

DMARC (Domain-based Message Authentication, Reporting, and Conformance) est un outil puissant pour améliorer la sécurité des courriels, protéger contre les fraudes et maintenir la réputation de votre domaine. Cet outil permet notamment :

- ***Authentification des courriels** : DMARC permet aux propriétaires de domaines de définir des politiques spécifiques sur la manière dont leurs courriels doivent être authentifiés. Il s'appuie sur deux protocoles existants, SPF (Sender Policy Framework) et DKIM (DomainKeys Identified Mail), pour garantir que seuls les expéditeurs autorisés peuvent utiliser un domaine.*
- ***Réduction du spam et des attaques par hameçonnage** : En vérifiant les expéditeurs et en fournissant des rapports détaillés sur l'activité des courriels, DMARC aide à réduire le spam et à prévenir les attaques par hameçonnage.*
- ***Protection de la réputation du domaine** : En définissant des politiques d'authentification strictes, DMARC aide à protéger la réputation du domaine en s'assurant que seuls les courriels légitimes sont envoyés au nom du domaine.*
- ***Rapports et conformité** : DMARC permet aux organisations de recevoir des rapports sur les tentatives d'usurpation d'identité et les échecs d'authentification, ce qui aide à surveiller et à améliorer la sécurité des courriels.*

2.3 Gestion des Accès et des Identités

2.3.1 *Politiques de mots de passe :*

Les recommandations précises peuvent être consultées sur le site Recommandations relatives à l'authentification multifacteur et aux mots de passe | ANSSI

MDP01	Imposer des mots de passe forts et leur changement périodique.

On peut préciser notamment, qu'un mot de passe doit respecter une certaine longueur selon son niveau de sensibilité (faible à moyen entre 9 et 11 caractères, moyen à fort entre 12 et 14 caractères, fort à très fort au moins 15 caractères). Il ne faut pas imposer une longueur maximale sur le mot de passe dans la mesure du possible. Au moment de la création ou du renouvellement d'un mot de passe par un utilisateur, il est recommandé de mettre en œuvre des règles de complexité tout en proposant un jeu de caractères le plus large possible. Un délai d'expiration doit être convenu pour les mots de passe sensibles. Enfin, l'utilisateur doit utiliser un mot de passe différent pour chaque service.

MDP02	Utiliser des gestionnaires de mots de passe pour sécuriser les accès.

2.3.2 *Authentification multi-facteurs (MFA) :*

MDP02	Mettre en place l'authentification multi-facteurs pour renforcer la sécurité des accès aux systèmes sensibles.

*Le MFA est une composante essentielle de toute politique de gestion des accès et des identités (IAM) solide, offrant une protection accrue contre les cyberattaques et les activités frauduleuses. C'est une méthode de sécurité qui exige que les utilisateurs fournissent au moins deux formes de vérification pour accéder à une ressource, comme une application, un compte en ligne ou un VPN. Cela permet notamment d'**améliorer la sécurité** en exigeant plus qu'un simple nom d'utilisateur et mot de passe et réduit considérablement la probabilité qu'une cyberattaque réussisse, **réduit** efficacement le **risque d'activités frauduleuses**, et **empêche les accès non autorisés** même si un mot de passe est compromis.*

2.4 Sauvegardes, Restauration, continuité et reprise d'Activité

2.4.1 *Sauvegardes régulières des données :*

SAUV01	Effectuer des sauvegardes régulières des données critiques et les stocker dans des emplacements sécurisés et hors ligne ou immuable, en s'assurant d'aucune erreur et la possibilité de restaurer (selon la règle 3 2 1 1 0).

Pour limiter les incidents, et garantir une bonne tolérance de panne, La Société préconise de suivre la règle des 3, 2, 1, 1, 0 :

- *Garder 3 copies des données*

- *Sur 2 types de médias (espaces de stockage internes, supports amovibles, NAS, Cloud…)*
- *Dont 1 copie à l'extérieur du site principal contenant les serveurs de production (Do'BaaS, Do'DRaaS, stocker le NAS, si existant, dans une autre pièce que les serveurs de production)*
- *Avec 1 copie hors ligne, air-gapped ou immuable (Stockez une copie de vos données sur un support non connecté à Internet ou inaltérable c'est-à-dire impossibles à modifier, écraser ou supprimer)*
- *Et 0 erreur de sauvegarde avec la vérification de la récupération automatique et/ou via des tests de restauration réguliers*

2.4.2 Sauvegardes régulières Digital Workspace:

SAUV02	Effectuer des sauvegardes régulières de vos données stockées dans votre Digital Workspace (Microsoft 365, Google Workspace, Dropbox …)

Les données (mail, Sharepoint, OneDrive, google Drive, …) stockées dans ces environnements ne sont pas sauvegardées par l'éditeur. Il est donc primordial de les sauvegarder et de les stocker sur un support et lieu différent, pour avoir ainsi la capacité de les restaurer en cas de nécessité.

2.4.3 Plan de reprise d'activité :

PRA01	Élaborer un Plan de Reprise d'Activité en correspondance avec les enjeux du Client en cas de panne.
PRA02	Tester le plan de reprise d'activité pour assurer la continuité des opérations en cas de sinistre.

2.5 Surveillance et Détection

2.5.1 Surveillance continue :

SOC01	Mettre en place des systèmes de surveillance (SOC) pour détecter les activités suspectes et les incidents de sécurité.

SOC (Security Operation Center) est un Centre opérationnel de Sécurité qui permet d'assurer la sécurité des systèmes d'information d'une organisation en détectant, analysant et répondant aux menaces de manière proactive et réactive. Le SOC s'appuie généralement sur un SIEM (Security Information and Event Management) pour détecter, analyser et répondre aux incidents de sécurité en temps réel.

2.5.2 Réponse aux incidents :

CSIRT01	Développer un plan de réponse aux incidents pour gérer efficacement les cyberattaques et minimiser leur impact.

Le CSIRT (Computer Security Incident Response Team) est une équipe spécialisée qui se concentre sur la gestion des incidents de sécurité. Lorsqu'un incident est détecté, le CSIRT intervient pour analyser, contenir et résoudre le problème.

CSIRT02	Etudier la souscription à une assurance Cyber

2.6 Sécurisation des Réseaux

2.6.1 Segmentation des réseaux :

LW01	Segmenter les réseaux pour limiter la propagation des attaques et protéger les systèmes critiques.

2.6.2 Chiffrement des communications :

LW02	Utiliser des protocoles de chiffrement pour sécuriser les communications et les transferts de données.

2.7 Sécurisation accès Internet

2.7.1 Data

WWW01	Souscrire un lien d'accès Internet professionnel non mutualisé, avec débit garanti et avec des Garanties de Temps de Rétablissement (GTR) par l'opérateur (fibres FTTB, FTTO, à défaut FTTE)

Les liens Internet Grand Public type fibre FTTH sont des liens mutualisés sur un grand nombre de Client, sans débit garanti et sans GTR. En cas de panne, il n'y a aucun délai de rétablissement avec des pannes totales pouvant durer plusieurs jours, voire semaines. Un lien fibre FTTE est partiellement mutualisé mais offre généralement des débits garantis et une GTR opérateur.
Accès

2.7.2 Voix (trunk-SIP)

TRUNK01	Souscrire deux abonnements trunk-sip chez deux opérateurs différents.
TRUNK02	Souscrire un numéro SVA en 08xx pour sécuriser l'accessibilité du téléphone.

En cas de panne d'un trunk-SIP, les numéros de téléphone portés chez un opérateur ne sont plus accessibles (SDA géographique ou SDA en 09). Les appels entrants et sortants ne sont donc pas possibles. Un second trunk chez un autre opérateur permet au Client d'émettre des appels sortant uniquement. Un accès en 08xxx permet d'associer une SDA à ce numéro et de la changer en cas de nécessité pour utiliser un autre Trunk : le client devra communiquer ce nouveau numéro à ses contacts extérieurs. Un second 08xx ouvert chez un autre opérateur permet une sécurisation optimum, et impose de communiquer sur ces 2 SVA.

2.8 Sécurisation des Biens et des Personnes

2.8.1 Alarme, contrôle d'Accès et anti-intrusion

SUR01	Mettre en place un système professionnel pour la protection des biens et des Personnes selon les normes APSAD

2.8.2 Vidéoprotection, Vidéosurveillance

SUR02	Mettre en place un système professionnel de vidéo pour une protection optimum des biens et des personnes, selon les recommandations de l'APSAD

2.9 Résilience Infrastructure

La résilience du Système d'Information et des accès Internet est primordial pour les activités ayant une dépendance très forte au regarde de leur métier. Les Clients dont le métier est lié à la Santé (Médecin, pharmacie, centre radiologique, centre hospitalier, clinique …), dont les revenus ou relation client sont directement dépendant de leur SI (perte d'exploitation directe) … doivent réfléchir et investir sur des solutions résilientes.

2.9.1 Système d'information (SI)

RES01	Réaliser une étude de résilience de son Système d'Information (SI) face aux enjeux opérationnels du Client : étude PCAI permettant de déterminer les risques à couvrir* et les DMIA** PDMA*** du SI Client.

** Risques à couvrir tels que l'incendie, l'attaque Cyber, panne hardware totale ou partielle, eau, indisponibilité d'accès aux sites …*
*** DMIA = La durée maximale d'interruption admissible (DMIA, parfois DIMA), en anglais recovery time objective (RTO), est l'expression de besoin de disponibilité des différents métiers ou services, dans une organisation.*
**** PDMA = La perte de données maximale admissible (PDMA ou parfois PDAM), en anglais recovery point objective (RPO) quantifie les données qu'un système d'information peut être amené à perdre par suite d'un incident.*

RES02	Redonder son infrastructure pour assurer un Plan de Continuité d'Activité (PCAI) ou Plan de Reprise d'Activité (PRAI) en cas de panne majeure en répondant aux exigences de couverture de risques, de DMIA et PDMA exprimés par le Client.

2.9.2 Accès Internet

RES03	Redonder son accès Internet principal pour assurer un Plan de Continuité d'Activité (PCAI) ou Plan de Reprise d'Activité (PRAI) en cas de panne mineure ou majeure

Les liens Internet sont régulièrement sujets à coupure partielle ou totale. Idéalement, et selon les éligibilités, il est conseillé de prendre au moins un second lien chez un autre opérateur et sur un agrégateur d'opérateur différent du lien principal. Et si possible, de prendre un lien d'une autre technologie (Fibre, xG, Satellite).

2.10 Gestion des Risques

2.10.1 Évaluation des risques :

RISK01	Réaliser des évaluations régulières des risques pour identifier les vulnérabilités et mettre en place des mesures de mitigation.

2.10.2 *Conformité réglementaire :*

RISK02	S'assurer de la conformité avec les réglementations en vigueur, telles que le RGPD, pour protéger les données personnelles.