Plan d'Assurance Sécurité Annexe « Infogérance »

1. Introduction

Cette annexe est liée et indissociable au Plan d'Assurance Sécurité.

2. Description du système

Le Système d'Information du Client est exposé à de possibles attaques extérieures ou mauvaises manipulations internes. La mise en œuvre de mesures de sécurité est nécessaire pour parer aux conséquences potentielles sur les données : perte d'intégrité, perte de disponibilité, perte de confidentialité, fuite de données…

3. Mesures de sécurité

3.1. Transfert

Avant le transfert de gestion du Système d'Information du Client, la Société doit pouvoir profiter d'un dossier technique de la solution actuellement en place pour une prise en main rapide et optimale de la solution. Il doit contenir les éléments suivants :

- ✓ La liste des équipements ;
- ✓ Les mots de passe pour accéder aux équipements (accès sécurisé et crypté) ;
- ✓ L'ensemble des licences dont le Client aura fait l'acquisition ;
- ✓ Le contrat de maintenance en cours avec le constructeur ;
- ✓ Le plan de sauvegarde et la reprise d'activité.

Vous faciliter l'IT

3.2. Exploitation

La Société présente dans ce paragraphe les mesures mises en place pour assurer la protection du système.

➢ ***Protection antivirale***

Une gestion centralisée via une console d'administration est généralement utilisée au-dessus de 5 postes, et est installée sur un serveur ou un poste professionnel. Nous préconisons son installation.

Elle facilite la gestion des taches, la gestion des stratégies et l'administration en général.

Un agent est installé, sur chaque matériel, afin d'exécuter les commandes envoyées par la console, et permet d'avoir un état du périphérique protégé.

Une solution antivirale est installée en fonction des systèmes d'exploitation du poste/serveur :

- ✓ Une solution antivirale adaptée est installée pour les systèmes d'exploitation maintenus par les éditeurs
- ✓ Pour les systèmes d'exploitation obsolètes, non maintenus par l'éditeur, la Société installe, dans la mesure du possible, une version compatible même si cela ne garantira pas un niveau de sécurité optimal.

Gestion des postes

Installation à minima des modules suivants, fournis par l'éditeur :

- ✓ Module protection en temps réel,
- ✓ Module protection courrier,
- ✓ Module protection Internet,
- ✓ Module comportemental.

La stratégie de réglage de ces modules, les tâches de mises à jour et les tâches d'analyses programmées sont programmées pour être répliqués sur tous les postes via la console d'administration.

Configuration des tâches :

Tâches de mises à jour	Tâches d'analyses programmées
Exécution automatique à minima 2 fois par jour	Exécution automatique à minima 1 fois par semaine

Gestion Serveurs

Installation à minima des modules suivants, fournis par l'éditeur :

- ✓ Module protection en temps réel
- ✓ Module comportemental.

La stratégie de réglage de ces modules, est répliquée sur tous les serveurs via la console d'administration.

Configuration des tâches :

Tâches de mises à jour	Tâches d'analyses programmées
Exécution automatique à minima 1 fois par jour	Exécution automatique à minima 1 fois par semaine

Préconisations

Il est préconisé de mettre à jour régulièrement les versions de tous les produits :

- ✓ Console centralisée
- ✓ Antivirus des postes
- ✓ Antivirus des serveurs

Certains modules proposés par les éditeurs peuvent être implémenté, pour augmenter la performance des solutions.

La Société préconise d'installer la version des produits adaptés aux applications déjà en place (ex : RDS > Il existe un produit dédié consommant moins de ressources).

Les serveurs de messagerie nécessitent une attention particulière car ils peuvent limiter la diffusion de messages corrompus. Il est très fortement conseillé d'installer la version dédiée. La Société préconise également vivement d'installer une solution antispam en amont du serveur de messagerie.

Il faut privilégier une version antivirale avec un module contre les cryptos virus.

La Société recommande très fortement d'avoir un système d'exploitation à jour (voir ***Mises à jour, correctifs de sécurité***). Seule la dernière version de la protection antivirale propose une sécurité optimale pour les attaques connues. Les systèmes d'exploitation obsolètes sont plus fragiles et résistent moins bien aux attaques.

- ***Sauvegardes et restauration***

Le choix du logiciel de sauvegarde est à effectuer en fonction du type de sauvegarde à effectuer : sauvegarde de serveurs virtuel et/ou sauvegarde de serveurs physiques ou de données dans une machine virtuelle.

La politique de sauvegarde est un élément important à prendre en compte. Il faut déterminer la période tolérable de perte de données (PDMA : Perte de Données Maximale Admissible) qui pourra définir les équipements, les rétentions, les fréquences des sauvegardes. La Société se tient à disposition du Client pour l'accompagner à définir cette politique.

Le Client peut préciser une liste de données qu'il juge sensibles, pour une sauvegarde adaptée.

La Société préconise de planifier une sauvegarde complète (Système + Données) une fois par semaine.

La Société conseille d'exécuter à minima les sauvegardes quotidiennement. La fréquence peut être plus courte en fonction des besoins du client.

Les NAS étant des espaces de stockage plus volumineux, ils peuvent conserver plusieurs points de sauvegarde et augmenter le temps de rétention de ceux-ci. La Société préconise une sécurité accrue des partages des NAS de sauvegarde. Pour éviter toute contamination par un éventuel virus, ces NAS doivent être accessibles uniquement par le logiciel de sauvegarde (ex :ne pas le partager pour stocker d'autres données).

Le nombre de support amovible utilisé détermine l'échéance de restauration d'une sauvegarde. Plus il y a de support, plus la restauration depuis une sauvegarde ancienne sera possible. Une gestion de sauvegarde quotidienne, hebdomadaire et mensuelle est possible.

La Société préconise une surveillance du résultat des travaux de sauvegarde (via Do'Supervision ou bien via un rapport envoyé).

Une supervision optionnelle est préconisée afin de détecter d'éventuelles défaillances de l'infrastructure de sauvegarde.

La description des éléments physiques de la sauvegarde est détaillée dans le dossier technique pour les clients infogérés.

La Société préconise de chiffrer les sauvegardes afin de les sécuriser.

Tolérance de pannes

Pour limiter les incidents, La Société préconise de suivre la règle des 3, 2, 1 :

- ✓ 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)

La Société propose en option des solutions de sauvegarde sécurisées et externalisées : Do'BaaS, Do'DRaaS.

Restauration

En fonction du paramétrage, du résultat et du contenu des sauvegardes, il est possible de restaurer un serveur dans sa globalité ou uniquement un fichier.

La Société préconise de permettre aux techniciens lors des journées préventives de pouvoir procéder à des tests de restaurations granulaires afin de vérifier le bon fonctionnement des sauvegardes.

La Société préconise de maintenir à jour les logiciels de sauvegarde présents sur l'infrastructure installée chez Client (voir ***Mises à jour, correctifs de sécurité***).

➢ ***Mises à jour, correctifs de sécurité, licences, garanties***

La Société préconise :

- ✓ D'appliquer les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles, prioritairement ceux concernant la sécurité des produits ;
- ✓ D'appliquer les mises à jour de produits proposés par les éditeurs ou constructeurs, tout en ayant préalablement consulter la documentation sur le contenu de ces mises à jour. Appliquer également en priorité celles concernant la sécurité des produits ;
- ✓ De conserver tous ces produits sous licences et garanties afin de pouvoir continuer à bénéficier de tous les services et support acquis initialement sur les solutions installées ;
- ✓ De ne plus conserver en exploitation des produits non maintenus par l'éditeur ou le fournisseur afin d'éviter tout risque de sécurité.

La Société peut exécuter ces tâches sur des Horaires Non Ouvrés (HNO) à la demande.

Certains produits se mettent à jour automatiquement mais un redémarrage est souvent nécessaire pour que les mises à jour s'appliquent. Ces tâches peuvent être exécutées en HNO.

Dans ces cas, le Client s'engage à fournir une adresse mail, un numéro de téléphone et les périodes correspondantes d'opération pour lui permettre de suivre le traitement d'une alerte éventuelle

Le technicien appliquant une mise à jour, la déclare dans son compte rendu.

La Société préconise avant toute mise à jour, une sauvegarde du logiciel ou système concerné par cette mise à jour.

Les prestations HNO sont majorées selon la politique commerciale de la SOCIETE.

➢ ***Continuité d'activité***

La Société prend toutes les mesures nécessaires pour assurer la disponibilité du Système d'Information.

La Société met en place les mesures techniques, organisationnelles, procédurales suivantes pour assurer la continuité d'activité du système, ou en cas de sinistre la reprise d'activité. En voici la description :

- ✓ Démarche optionnelle

  Le Client décide ou non de s'inscrire dans la continuité d'activité ou plus précisément dans le Plan de Continuité d'Activité Informatique (PCAi). Celui-ci est exposé au travers de notre mission de conseil.

- ✓ Sauvegarde externalisée des données informatiques

  C'est la préconisation de base. Le Client a la responsabilité de s'assurer que les supports amovibles (disques durs, support magnétique, etc.) ou tout autre moyen dont il a la charge opérationnelle, sont externalisés par un collaborateur du Client désigné.

  Si le Client et la Société l'ont défini, la Société peut être responsable du contrôle et de la surveillance du bon fonctionnement de la sauvegarde.

  La Société propose des méthodes d'externalisation optionnelles exploitées et appartenant à la Société de type Backup As A Service pour lesquelles la Société est responsable du bon fonctionnement.

- ✓ Disponibilité du Système d'Information

  La Société distingue plusieurs briques définissant la mise en œuvre globale d'un plan de continuité d'activité informatique (PCAi) :

  - Plan de reprise d'activité informatique (PRAi)
  - Plan de continuité d'activité informatique (PCAi)
  - Plan de crise informatique (PCi)

  En fonction des attentes du Client concernant la disponibilité de son Système d'Information, le périmètre d'exécution de la Société est différent. Cela entraine une gestion et une priorisation des risques également différentes.

- ✓ Séparation des infrastructures

  Les mesures techniques définies sont propres à chaque Client, cependant la Société applique une règle commune concernant la localisation des moyens de production et de reprise d'activité. Ces moyens techniques (serveurs, baies, NAS, switch, etc.) doivent être géographiquement externalisés des équipements de production au même titre que les supports de sauvegarde. La Société met à disposition, sur son extranet, le schéma technique et les adresses IP des équipements mis en œuvre.

  Dans le cadre de sa mission d'infogérance, la Société est amenée à tester le fonctionnement des outils de sauvegarde (restauration de fichiers et de dossiers) et à simuler le démarrage de serveurs virtuels dans un contexte de production limitant la portée des tests.

- ✓ Prestations complémentaires optionnelles

  La Société propose des prestations complémentaires optionnelles : le PCAi, le PRAi, la journée PCAi, et le Plan de Crise informatique.

  Le Plan de Continuité d'Activité informatique (PCAi), a pour but de garantir la survie de l'entreprise en anticipant les risques d'un sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données.

  - Etude des impacts liés à une panne informatique pour le Client.

- Elaboration d'une architecture informatique.
- Elaboration des scénarios à tester face à un certain nombre de risques.
- Réalisation des tests et rédaction des procédures.
- Mesure des impacts et conséquences en termes de délai (PDMA et DMIA).
- Organisation du retour à la situation initiale.

Le Plan de Reprise d'Activité informatique (PRAi) est un ensemble de procédures (techniques, organisationnelles, sécurité) qui permet à une entreprise de prévoir par anticipation, les mécanismes pour reconstruire et remettre en route un Système d'Information en cas de sinistre ou incident informatiques importants.

- Elaboration des scénarios à tester face à un certain nombre de risques
- Réalisation des tests et rédaction des procédures
- Organisation du retour à la situation initiale

La journée PCAi permet de tester les outils du PCAi et/ou du PRAi en conditions réelles en suivant un scénario, d'en mesurer l'efficacité et d'apporter des améliorations futures. Elle est réalisée selon la fréquence définie dans le contrat et avec accord préalable du Client. Si des procédures existent, elles sont également éprouvées.

Le Plan de Crise informatique est une prestation ponctuelle d'une ou plusieurs journées permettant la structuration et la formalisation d'un livrable décrivant les points suivants :

- Constitution d'un COPIL « Plan de crise informatique »
- Organisation de la gestion de crise par une approche pragmatique et fonctionnelle
- Elaboration des scénarios à tester face à un certain nombre de risques
- Réalisation des tests et rédaction des procédures
- Mesure des impacts et conséquences en termes de délai (PDMA et DMIA)
- Organisation du retour à la situation initiale

La Société met à disposition du client les rapports de la journée PCAI et la documentation du plan de crise.

➢ ***Confidentialité et intégrité des flux***

Tous les flux d'administration sont chiffrés par des procédés fiables (SSH, SSL, IPSec, etc.), garantissant la confidentialité et l'intégrité des données.

De façon générale, tous les flux contenant des informations sensibles et circulant sur un réseau public sont chiffrés par des procédés apportant ces mêmes garanties.

➢ ***Contrôle et filtrage des flux***

Conformément aux exigences de sécurité, la Société préconise la mise en place de zones, chacune étant protégée par un dispositif de filtrage :

- ✓ Une zone publique regroupant les machines qui hébergent des services ayant vocation à communiquer avec l'extérieur (Reverse Proxy, Serveur Web, FTP, Serveur de mail, DNS, etc.) ;
- ✓ Une zone privée regroupant les machines n'ayant pas vocation à communiquer avec l'extérieur ;
- ✓ Une zone dédiée au WiFi avec si possible des VLAN entre les SSID interne et visiteurs ;
- ✓ Un réseau dédié à l'administration des machines et des équipements à partir de postes de travail situés dans le domaine d'administration de la Société.

Le trafic réseau en provenance et à destination du système fait l'objet d'un contrôle permanent afin de n'autoriser que les flux légitimes.

La Société conseille la définition d'une matrice de flux (inventaire des flux légitimes).

Le service global est protégé contre les attaques classiques sur IP et les protocoles associés notamment :

- ✓ Attaque en déni de service (TCP SYN Flood, Ping Flooding, SMURF, Ping of Death, large packet attacks, etc.) ;
- ✓ IP options (source routing, etc.).

La Société préconise plusieurs mesures techniques :

- ✓ Mettre en place un parefeu afin de filtrer les flux transitant sur le réseau ;
- ✓ Configurer les dispositifs de filtrage de façon bloquante par défaut, tout ce qui n'est pas explicitement autorisé étant interdit ;
- ✓ Limiter les accès depuis l'extérieur (interfaces de management, réponses au ping, SNMP) ;
- ✓ Modifier, si possible, les ports d'administration par défaut ;
- ✓ Bannir l'utilisation des ports non chiffrés ;
- ✓ Identifier les utilisateurs par le procédé de SSO dès que possible ;
- ✓ Mettre en place un collecteur de journaux d'événements pour les tracer et les analyser (Analyzer, etc…) ;
- ✓ Activer, configurer, contrôler et adapter régulièrement les options des équipements de sécurité en fonction des nouveautés (Miners, Ransomware, etc…) ;
- ✓ Restreindre les horaires d'utilisation de l'Internet (surtout pour la zone dédiée au WiFi) ;
- ✓ Configurer le mode furtif, si disponible, pour ne pas répondre aux demandes extérieures de scans de ports) ;
- ✓ Configurer du VPNSSL pour les accès nomades (RDP, FTP, etc…).

➢ ***Imputabilité, traçabilité***

Les informations suivantes sont enregistrées :

- ✓ Entrée en session d'un utilisateur : date, heure, adresse IP, réussite ou échec de la tentative avec quinze (15) jours de rétention ;
- ✓ Entrée en session d'un utilisateur distant via NetExtender (si utilisé) : date, heure, identifiant de l'utilisateur, réussite ou échec de la tentative avec quinze (15) jours de rétention.

La Société préconise l'enregistrement et la conservation pour au moins six (6) mois (sauf obligation légale, nécessitant une conservation plus longue) des informations suivantes :

- ✓ Actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits : date, heure, identité de l'utilisateur, nom de l'objet, type de la tentative d'accès, réussite ou échec de la tentative

; création/suppression d'un objet soumis à l'administration des droits : date, heure, identifiant de l'utilisateur, nom de l'objet, type de l'action ;

- ✓ Actions d'utilisateurs autorisés affectant la sécurité de la cible : date, heure, identité de l'utilisateur, type de l'action, nom de l'objet sur lequel porte l'action.

- ➢ ***Formations et sensibilisations dans le domaine de la sécurité du Système d'Information des personnels en charge des prestations***

La fréquence et le contenu des formations et des sensibilisations du personnel aux enjeux de sécurité sont réalisés par un plan de formation défini chaque année.

- ➢ ***Surveillance et contrôle des accès aux locaux d'hébergement du système d'information***

La Société préconise un filtrage des accès aux salles hébergeant des matériels liés au Système d'Information.

La Société conseille les moyens de sécurité d'accès aux locaux suivant :

- ✓ Moyens de surveillance, dispositifs anti-intrusion ;
- ✓ Contrôle et enregistrement des accès (moyen d'identification, etc.) ;
- ✓ Protection physique des équipements (verrouillage des baies, etc.).

- ➢ ***Intervention des sociétés de maintenance ou de support de solutions informatiques (matérielles ou logicielles)***

La Société préconise au Client de s'assurer du respect des exigences de sécurité lors d'interventions de sous-traitants (éditeurs de logiciel, constructeurs matériels…) amenés à intervenir dans le cadre du support et de la maintenance sur son Système d'Information.

Cette préconisation est étendue aux différentes institutions intervenant dans le cadre de prestations récurrentes comme :

- ✓ Société de nettoyage
- ✓ Prestataire de gestion des moyens généraux (chauffage, climatisation, électricité etc..).