Plan d'Assurance Sécurité Annexe « Service Télécoms Téléphonie »

1. Introduction

Cette annexe est liée et indissociable à l' « ***ANNEXE CGV_PAS Dispositions du Plan d'Assurance Sécurité*** ».

2. Description du système

Ce document fait référence aux systèmes de téléphonie et Télécoms déployés par la Société.

Nous identifions les systèmes de téléphonie d'entreprise par leur fonction primaire de gestion des appels entrants / sortants. Ces systèmes peuvent être de marque et de modèle différents et ils sont composés de :

- ✓ Un serveur de téléphonie qui concentre l'intelligence et la programmation dudit système ;
- ✓ Périphériques comme les téléphones fixes / mobiles (DECT) ;
- ✓ Infrastructures filaires ou de fréquences associées ;
- ✓ Applicatifs étroitement liés au système de téléphonie pouvant permettre la traçabilité des appels ;
- ✓ Petits périphériques portatifs (casque, …).

Outre ces systèmes voix, nous pouvons aussi associer les systèmes de visioconférence à cet ensemble. Tous ces derniers orchestrés par une couche logique LAN (Local Area Network) constituée de commutateurs.

Pour permettre une interaction extérieure des différents systèmes, sont identifiés Télécoms les dispositifs d'accès opérateur, basés sur la technologie xDSL ou fibre optique. Ils permettent les échanges Data/Voix en entrée et sortie. Nous appelons Trunk SIP le service Voix proposé, calibré par un nombre de canaux. Ces systèmes Télécoms sont supportés par un ensemble de matériel de type routeur ou modem, jusqu'au pare-feu augmentant la sécurisation d'une infrastructure globale connectée à Internet.

Outre ces technologies IP en croissance, il existe encore des technologies VGA Analogique ou ISDN (T0 ou T2) pouvant être proposées pour le transport des flux Voix. Ces technologies plus sommaires sont supportées sur des équipements opérateurs et directement connectées à un système de téléphonie, il s'agit d'un service exclusivement Voix et non IP.

Les solutions proposées étant liés aux systèmes et réseaux de son infrastructure, l'annexe « ANNEXE PAS Service Infogérance » est également applicable.

3. Mesures de sécurité

3.1. Transfert

La Société se porte garant de l'intégrité et de la confidentialité des données qui lui sont confiées pendant la phase de transfert du système de téléphonie.

Dans un premier temps, le Client doit fournir à la Société, un relevé d'information en provenance de son ancien prestataire. Ces documents et fichiers de configuration sont à envoyer par voie électronique sécurisée.

La Société réalise un relevé d'informations techniques ainsi que des sauvegardes du ou des systèmes si ce/ces derniers le permettent. Aussi, pendant toute la durée du transfert la Société bénéficie d'un accès permanent à distance sur le système.

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 à minima les éléments suivants :

- ✓ La liste des équipements ;
- ✓ Les mots de passe pour accéder aux équipements (accès sécurisé et crypté) ;
- ✓ La configuration des équipements et des systèmes de téléphonie ;
- ✓ L'ensemble des licences dont le Client aura fait l'acquisition ;
- ✓ Le contrat de maintenance ou assurance logicielle en cours avec le constructeur.

3.2. Exploitation

La Société présente dans ce paragraphe les mesures mises en place pour assurer la protection des systèmes de téléphonie et télécoms.

➢ ***Protection antivirale / EDR***

La Société conseille la mise en place d'une politique antivirale / EDR stricte pour les serveurs de téléphonie sous environnement Windows. La mise à jour des signatures doit être automatique et réalisée à fréquence régulière.

➢ ***Mises à jour, correctifs de sécurité sur les systèmes de téléphonie sous maintien opérationnel***

Le Client doit avoir souscrit aux assurances logicielles constructeurs ou extension de garantie afin d'avoir accès et bénéficier des téléchargements des correctifs.

La Société préconise l'application des correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur tous les matériels dont il a la charge.

La Société propose d'assurer le déploiement de ces mises à jour lors de la souscription à un contrat de service ou via une prestation complémentaire.

La Société rappelle que plus votre système téléphonique est ancien, plus il est vulnérable aux piratages car les failles de sécurité y sont nombreuses et souvent connues des hackers.

➢ ***Authentification***

La Société s'engage à changer le mot de passe par défaut des équipements pour des raisons de sécurité (piratage des lignes téléphoniques…).

La Société préconise de changer régulièrement les mots de passe des boîtes vocales et incite fortement les utilisateurs à ne pas utiliser des mots de passe trop simples (0000, 1234 par exemple).

➢ ***Sauvegardes et restauration***

Sauvegarde Appliance PBX :

A la fin du déploiement de la solution, la Société effectue une sauvegarde globale de l'installation qui sera externalisée dans les locaux de la Société.

Dans le cadre d'une télémaintenance ou d'une migration, une sauvegarde est également effectuée et stockée dans les locaux de la Société.

Sauvegarde IPBX Virtuel :

Si le système de téléphonie est déployé sur l'infrastructure matérielle Client (HyperV, VMware…), la sauvegarde et le contrôle sont de la responsabilité du Client.

La Société recommande une récurrence journalière des sauvegardes.

Si le système de téléphonie est déployé sur une infrastructure matérielle infogérée ou sous maintien opérationnel par la Société, cette dernière conseille et propose :

- ✓ Un contrôle au minimum une fois par an, des équipements matériels sur site ;
- ✓ Un contrôle de l'exécution des sauvegardes (sans tests de restauration) ;
- ✓ Une supervision en temps réel des équipements infogérés afin d'anticiper les dysfonctionnements ;
- ✓ Différents niveaux de services pour les sauvegardes :
  - Sauvegarde de la configuration ;
  - Sauvegarde de l'intégralité du serveur ;
  - Externalisation de la sauvegarde

L'ensemble de ces mesures, paramétrages et options de prestation sont proposées dans le contrat de service et décrit dans les Conditions Générales Particulières.

Dans tous les cas, le contrôle quotidien ainsi que les tests de restauration restent sous la responsabilité du Client.

La Société peut assurer ses tâches dans le cadre de prestations complémentaires.

➢ ***Protection électrique***

La Société préconise la mise sous protection électrique des équipements de téléphonie.

- ✓ 1er Niveau de protection :

  Installation d'une protection parafoudre des équipements électriques.

- ✓ 2ème Niveau de protection :

  Installation d'onduleurs et/ou de batteries calibrés à la puissance nécessaire aux besoins de l'installation.

  L'installation électrique devra être en conformité (prise 16A).

La mise en œuvre de ces protections n'engage en rien la responsabilité de la Société en cas de dysfonctionnement électrique qui surviendrait sur l'installation.

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

Sécurisation de vos liens Télécoms (Data/Voix) :

La Société recommande l'activation, le paramétrage du pare-feu de votre routeur et la bonne configuration du filtrage des adresses IP externes. Vos adresses IP sources et destinations doivent être spécifiées. Elles seront les seules autorisées à se connecter à votre système téléphonique et votre réseau informatique.

Lors de la mise en place d'un lien dédié (xDSL) pour la Voix, la Société met en place une restriction d'adresses IP Publiques afin que seuls les équipements installés chez le Client puissent échanger des données avec notre plateforme Voix.

Lors de la mise en place d'un lien dédié Data ou Data/Voix, un pare-feu (ainsi qu'un système de conservation des journaux de navigation, obligatoire à la lecture du Décret n°2011-219 du 25 février 2011) est très vivement préconisé afin de sécuriser votre Système Informatique des attaques extérieures. Dans le cas où la Société n'infogère pas le pare-feu, elle ne pourra pas être tenue responsable d'une utilisation frauduleuse de l'accès.

Dans le cadre d'une mise en place d'un pare feu par la Société, un contrat de services sera proposé et fortement conseillé. Un pare feu doit obligatoirement être mis à jour afin de répondre aux bonnes pratiques liées à la sécurité (voir l'annexe : PAS – Annexe Infogérance).

Sécuriser vos applications nomades

La Société propose en option au Client possédant un système de téléphonie sur site (On Premise), la possibilité de se connecter à son système depuis l'extérieur. Les utilisateurs nomades ont, pour ce faire, plusieurs possibilités :

- ✓ Via un softphone (natif ou non en fonction de la solution) en ayant préalablement lancer un client VPN
- ✓ Via un softphone ou un téléphone physique avec la mise en place d'un proxy SIP

Fixer un plafond journalier à votre consommation téléphonique

La Société propose de déterminer un plafond journalier ou horaire pour vos coûts de communication. Au-delà de ce seuil, le compte du Client est automatiquement bloqué pour les appels sortants (les appels entrants continuent de fonctionner) afin de le protéger d'abus ou d'attaques potentielles. Ce plafond n'est pas possible sur les solutions Centrex Do'UCall.

La Société est alertée en temps réel et prend contact avec le Client afin de déterminer si l'appel est frauduleux ou non.

Le seuil paramétré se basant sur les conversations terminées et sur la base des prix d'achat de la Société, le Client doit prendre en compte ces éléments pour le déterminer.

- ➢ ***Formations et sensibilisations dans le domaine de la sécurité 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.