Media Communication IDF

CONDITION GENERALES DE VENTES V1.2

CONDITIONS MAINTENANCE V1.2

NOTE SUR LE PIRATAGE V1.2

ARTICLE 1 : Objet de la note

La Société MEDIA COMMUNICATION IDF (MCI) et l'ensemble de la profession constatent une recrudescence des fraudes associées à la téléphonie. Les conséquences engendrées par ces fraudes peuvent être le détournement de vos accès téléphoniques via différentes fonctions de vos systèmes téléphoniques, et donc, une augmentation des coûts de communications téléphoniques à votre charge.

Les nouvelles générations de systèmes téléphoniques sont interfacées avec les réseaux de données. Cette optimisation des flux voix-données apporte des services de communication unifiés fluides, rapides et efficaces. Certes les systèmes de TOIP sont plus ouverts vers l'extérieur et sur internet, mais sont aussi fragiles face aux attaques frauduleuses diffusées via Internet.

Quand aux anciennes technologies de téléphonie dites « traditionnelles », ces dernières sont installées sur des systèmes de raccordement dissociés du réseau de l'entreprise et des accès internet. Semblant être plus « sécurisées », ces installations sont néanmoins attaquées par des moteurs d'appels automatiques vers notamment des téléphones portables.

Afin de limiter les risques d'attaques et les conséquences techniques et économiques associées, il vous appartient de mettre en place certaines actions simples.

ARTICLE 2 : Les risques liés au piratage

La société MCI a identifié à ce jour cinq grands risques liés au piratage :

Déni de service : Cette attaque a pour but de rendre inefficace le système de téléphonie en saturant le PABX ou l'IPBX. Les téléphones servent également de cible.

Fraude téléphonique & piratage : L'objectif est de prendre le contrôle du PABX ou de l'IPBX et de le reconfigurer pour faire émettre des appels au nom de la société qui a été détournée. La méthode la plus utilisée est d'essayer de pénétrer sur une boite vocale d'un PABX et de se servir des fonctionnalités de transfert d'appels pour ressortir vers l'extérieur.

Intrusions : Elles se traduisent notamment par l'envoi de codes trompeurs via internet qui brisent les barrières de sécurité, les mots de passes des autocommutateurs et des postes téléphoniques. Ils ralentissent l'usage du réseau et polluent le bon fonctionnement de la navigation et récupération des habitudes (Virus, Trojan, Spyware, Malware, Vers).

Ecoute téléphonique : Elle est liée à la surveillance, l'espionnage ou le vol d'informations. L'utilisateur manipule les configurations de l'autocommutateur pour s'introduire lors des conversations ou explorer les messages vocaux.

L'usurpation d'identité : Les différentes fonctions des autocommutateurs (PABX, IPBX) permettent de se présenter sur le réseau téléphonique avec une fausse identité. Il est également possible de détourner les appels vers l'extérieur de l'entreprise sur des GSM ou d'autres lignes téléphoniques fixes. Ces pratiques permettent de montrer les « arnaques » qui détériorent l'image de l'entreprise.

ARTICLE 3 : Les recommandations

Pour palier à ces risques la société MCI recommande à ses clients de penser à la sécurité de leur réseau dans sa globalité, tant de manière corrective que de manière préventive avec sensibilisation des utilisateurs et des administrateurs.

Sécurité du réseau : Firewall, segmentation des flux et contrôle, cryptage et VPN sont des minimums pour garantir la sécurité de votre réseau.

Gestion des accès utilisateur : Authentification, mise à jour des mots de passe utilisateurs

Le client doit également définir et appliquer une stratégie de sécurité rigoureuse dans ses établissements, se traduisant pour les utilisateurs par les obligations suivantes :

- Interdire aux personnes non autorisées l'accès physique aux équipements,
- Conserver en lieu sûr les informations confidentielles relatives aux équipements installés (paramétrages, configuration, identifiants, mots de passe, etc.) et ne les communiquer qu'aux seules personnes autorisées,
- Saisir des identifiants / mots de passe personnels à compter de la recette des équipements et/ou à la première utilisation,
- Changer régulièrement le(s) mot(s) de passe
- Proscrire l'usage de mots de passe « simplistes », tels que 1234, 0000, 1111, 4 derniers chiffres du numéro du poste ou de l'entreprise, etc.
- Veiller à ne jamais communiquer les mots de passe (autres personnes/collègues, etc.)
- Veiller à verrouiller au besoin le poste en dehors des périodes d'utilisation (vacances, week-ends, etc.)

Sécurité des systèmes : Mise à jour des mots de passe matériel et administrateur, sécurité des serveur (antivirus, filtrage, authentification), paramétrage des activations, désactivations des messageries, SVI, renvois, substitution de postes.

Dévalidation des fonctions « renvoi » ou « messagerie vocale » des postes téléphoniques des collaborateurs qui n'en ont pas besoin.

Sensibilité du personnel : Chaque utilisateur doit protéger l'accès à sa boîte vocale avec un mot de passe non trivial. Proscrire l'usage des mots de passe « simplistes » tels que 1234, 0000, etc… Remplacer le mot de passe régulièrement. Ne jamais communiquer ce mot de passe, ni en interne ni à l'extérieur de l'entreprise.

Restriction d'accès sur les pays étrangers et les mobiles pour les collaborateurs qui n'en ont pas besoin.

Si vous souhaitez mettre en œuvre une ou plusieurs de ces actions, ce que nous vous recommandons, nous vous invitons à contacter notre service technique au : 01 34 35 19 79. Si des failles de sécurité sont identifiées, nous vous proposerons une intervention.

Ceci ne garantit en rien l'immunité totale en cas d'attaques mais diminuera fortement la probabilité que vous en soyez victime.

L'attention de l'entreprise et de l'utilisateur est attirée sur l'impératif de définition et d'application d'une stratégie d'entreprise de sécurité rigoureuse, se traduisant pour les utilisateurs par les obligations suivantes :

ARTICLE 4 : Fiche process de la société MCI

Pour simplifier les démarches de sécurisation des installations téléphoniques de ces clients, la société MCI a mis en place une fiche de process dédiée à la modification de la discrimination téléphonique (PROC03)et une fiche de process dédiée à la modification des aboutements et :ou renvois (PROC02). Ces fiches de process sont impérativement à remplir en cas de modification d'installation.

Le client reconnaît avoir été informé et avoir accepté les obligations contractuelles mentionnées ci-dessus et s'engage à les mettre en œuvre.

Dés lors, la société MCI décline toute responsabilité concernant le préjudice direct ou indirect, matériel ou immatériel, susceptible de résulter de l'intrusion dans le système installé, ainsi que de l'utilisation dudit système, par des tiers non autorisés, causées par l'inexistence, l'insuffisance ou défaut de respect des procédures de sécurité et de contrôle de l'accès au système installé dont il préconise la mise en œuvre par le Client.