RECOMMANDATIONS DE SECURITE POUR LE SYSTEME TELEPHONIQUE OMNIPCX OFFICE

« Cette communication technique décrit les paramètres de configuration qui permettent une protection optimale contre les risques et tentatives de détournement de fonctions visant à établir des appels sortants illicites comme par exemple de l'assistant personnel ou de la configuration à distance de la boîte vocale. »

1 Introduction

Cette communication technique rappelle les recommandations élémentaires de sécurité sur l'OmniPCX et plus précisément, les paramètres de configuration qui permettent une protection optimale contre les risques et tentatives de détournement de fonctions visant à établir des appels sortants illicites. Ces fonctions sont protégées par le mot de passe usager.

Ce mot de passe unique autorise l'accès aux fonctions suivantes :

- configuration de la boîte vocale,
- configuration de l'assistant personnel,
- gestion du mot de passe,
- configuration du mode nomadic,
- activation d'un renvoi,
- substitution distante,
- accès à la boite vocale,
- connexion de PIMphony avec l'OXO,
- verrouillage du poste,
- My IC Web for Office,
- My IC Mobile.

2 Description générale

Lorsqu'il se trouve hors de l'entreprise, un usager du PABX peut utiliser la fonction "Personnalisation à distance de sa messagerie vocale". Par le biais d'un appel téléphonique et des fonctions de l'Assistant personnel, il peut alors configurer puis activer le renvoi de son numéro d'entreprise vers un destinataire externe.
La mise en oeuvre du renvoi d'assistant personnel est assujettie à plusieurs contrôles par le système. Elle implique également que l'appelant externe connaisse la procédure d'accès au paramétrage de l'assistant personnel (code occulte non délivré par le guide vocal de l'OmniPCX Office) ainsi que le numéro de poste et le mot de passe personnel de l'usager interne.

Lorsque le renvoi externe d'assistant personnel est validé dans le système, tout appel externe vers le numéro d'usager concerné est automatiquement mis en relation avec le destinataire de renvoi précédemment défini (aboutement ligne à ligne).

L'OmniPCX Office dispose de plusieurs paramètres de configuration permettant de contrôler la mise en place de ces renvois.

3 Gestion du mot de passe usager

Pour la protection des services sensibles, le mot de passe individuel est un élément clé : une personne qui accède à l'assistant personnel ou à la DISA transit au moyen d'un mot de passe valide est implicitement un utilisateur autorisé du système.
Cependant, la responsabilité étant partagée par l'ensemble des utilisateurs et intervenants (usagers, administrateur, installateur), la protection globale est vraiment efficace si elle est accompagnée d'une stratégie de sécurité complémentaire et efficace au sein de l'entreprise.

Les recommandations élémentaires d'Alcatel-Lucent en matière de sécurité sont les suivantes :

- définir et appliquer une stratégie d'entreprise rigoureuse vis-à-vis des usagers internes.
- obliger les utilisateurs à changer régulièrement leur mot de passe.
- proscrire l'usage de mots de passe dits triviaux, tels que 1234, 0000, 1111, etc...
- l'OmniPCX Office force l'utilisateur à modifier le mot de passe par défaut avant l'initialisation de sa boite vocale.
- veiller à ce que les personnes ne se communiquent pas les mots de passe entre elles (autres personnes/collègues, etc ...).
- veiller à ce que les personnes verrouillent au besoin leur poste en dehors des périodes d'utilisation (vacances, week-ends, etc...).

Important

Les mots de passe dits triviaux sont contrôlés par le système à partir des versions R410/065.001, R510/059.001, R610/047.001, R710/052.007, R800/030.002, R810/045.003, R820/026.007, R900/033.002 et R910/021.001.
A partir des versions R800/043.001 et R810/047.001 la liste des mots de passe dits triviaux a été étendue.
Lors de la saisie d'un mot de passe considéré par l'OmniPCX Office comme étant trivial le message « Saisie non valide » est diffusé.

Important

Depuis les versions R820/026.007, R900/033.002 et R910/021.001 le système peut être configuré pour utiliser des mots de passe usager à 6 chiffres. Un nouveau système démarre automatique avec des mots de passe à 6 chiffres alors qu'un système mis à jour vers une des ces versions conserve les mots de passe à 4 chiffres mais dans ce cas à chaque connexion d'OMC un message recommandant de passer les mots de passe à 6 chiffres sera affiché.

Note

Après un swap avec data-saving, d'une version antérieure à une de celle mentionnée ci-dessus, si des mots de passe triviaux étaient utilisés ils seront restaurés dans le système. Dans ce cas il est de la responsabilité de l'utilisateur, l'administrateur ou de l'installateur de vérifier que nos recommandations de sécurités sont appliqués.

Note

Depuis la version R9.1 une nouvelle fonction du système permet de vérifier si des mots de passe triviaux sont utilisés. Une fonction supplémentaire permet de remettre à la valeur par défaut tous les mots de passe des utilisateurs ayant des mots de passe triviaux (voir la Documentation Expert pour plus de détails).

4 Gestion des mots de passe système

Des règles similaires doivent être appliquées pour les différents mots de passe utilisés par OMC pour se connecter au système. Il est recommandé de modifier le mot de passe par défaut **Installateur** pour OMC Expert, **Administrateur** pour OMC EasyPlus et **Opérateur** pour OMC Easy. Ces mots de passe sont également utilisés pour les connexions par DHM-Poste.

Les recommandations élémentaires d'Alcatel-Lucent en matière de sécurité sont les suivantes :

- définir et appliquer une stratégie d'entreprise rigoureuse vis-à-vis des usagers internes.
- changer régulièrement leur mot de passe.
- proscrire l'usage de mots de passe dits triviaux, tels que 12345678, 11111111, 00000000, etc...
- ne choisissez pas un mot du langage de tous les jours. Une intrusion peut être réalisée à l'aide de logiciels spécialisés utilisant des dictionnaires de mots.
- ne choisissez pas un mot en relation avec vous-même : le nom de votre société, votre nom, le nom de jeune fille de votre femme, le nom de vos enfants, de votre chien, de votre loisir favori, etc…
- prenez un mot de passe différent par mode de connexion.
- votre mot de passe est personnel et doit rester confidentiel, ne le divulguez jamais à personne.
- un mot de passe ne doit jamais être écrit quelque part. La première chose que fait une personne malveillante, est de fouiller dans vos affaires.

Warning

Les mêmes règles doivent être appliquées au mot de passe de la session **Téléchargement de logiciel**. Le mot de passe par défaut est identique à celui par défaut de la session Installateur. Mais la session Téléchargement possède un mot de passe spécifique qui peut être modifié avec OMC Expert.

Note

Un niveau supplémentaire de sécurité peut être réalisé en activant les fonctions « Rappel / Appelants Autorisés » dans le menu OMC « Gestion et Contrôle Réseau ». Ceci permet d'avoir le contrôle total sur qui est autorisé à se connecter au système (pour plus de détails voir la documentation expert).

Depuis la R9.1 tous les mots de passe de gestion du système (à l'exception du mot de passe Opérateur) doivent respecter de nouvelles règles (contrôlées par le système). Il faut au minimum:

- une lettre majuscule (A-Z),
- une lettre minuscule (a-z),
- un chiffre (0-9),
- une longueur fixe de 8 caractères,
- pas de caractères spéciaux.

Note

Depuis la version R9.1 une nouvelle fonction du système permet de vérifier si des mots de passe par défaut ou triviaux sont utilisés (voir la Documentation Expert pour plus de détails).

Important

Depuis la version R9.0 il faut impérativement fournir soit le numéro de série de la CPU ainsi que l'adresse MAC soit directement le CPU ID lors d'une demande (service request) de remise à la valeur par défaut du mot de passe installateur

Pour le Client	Pour STE
Date, signature, cachet	Date, signature, cachet

