MD Evolution – Rappels de sécurité

Contenu

1 Introduction

De nos jours, l'Internet met l'attirail du parfait hacker à portée de main. En effet des sites facilement accessibles recensent les failles des serveurs de téléphonie, des logiciels permettent de scanner les serveurs pour détecter des comptes, et d'autres encore vous offrent la possibilité de trouver les mots de passe associés.

Le piratage téléphonique, communément appelé « phreaking », est l'exploitation des infrastructures téléphoniques dans un but malveillant. La multiplication des opérateurs dans le monde et l'augmentation du taux d'équipements en téléphones a créé un nouveau marché pour les pirates : détourner des communications pour les revendre.

Par ailleurs, la multiplication de services (jeux, paris, voyance, etc.) proposés via un numéro de téléphone à appeler dont le titulaire encaisse un revenu à chaque appel (numéros surtaxés ou à revenus partagés) incitent l'appelant comme le propriétaire du numéro surtaxé à pirater des communications soit pour accéder au service (joueur, parieur, etc.) soit pour encaisser le revenu généré par chaque appel (titulaire du numéro surtaxé).

Nous constatons un accroissement significatif de ces détournements et toutes les entreprises, des grands comptes aux TPE/PME, sont confrontées à ce risque.
Nous constatons également que les attaques se multiplient, que les systèmes téléphoniques ne sont pas toujours bien protégés contre ces attaques et que les conséquences sont importantes (financières…).

Toutes ces considérations nous conduisent à produire ce document pour rappeler les principes de sécurité indispensables.

2 Principe généraux de sécurité

La téléphonie doit faire partie de la politique de sécurité du système d'information de l'entreprise.

Il existe des solutions faciles à mettre en place pour sécuriser l'architecture téléphonique et les autocommutateurs, les principales étant synthétisées ci-dessous :

- Contrôler l'administration et l'utilisation des équipements télécoms
  - En attribuant des droits avec des niveaux d'accès différents en fonction du niveau d'habilitation du ou des administrateurs.
  - En restreignant les droits à l'utilisation de certaines fonctions sensibles, par exemple en interdisant ou limitant l'utilisation des transferts et renvois vers l'extérieur (aboutement réseau), aussi bien pour les postes que pour la messagerie vocale.
- Sensibiliser le personnel de l'entreprise
- Installer une solution d'analyse et d'observation du trafic → taxation

3 Recommandations particulières – MD Evolution

Cette communication technique rappelle les recommandations élémentaires de sécurité sur le MD Evolution 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.

3.1 Description générale

Lorsqu'il se trouve hors de l'entreprise, un usager du PABX peut, s'il est autorisé, personnaliser à distance 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 œuvre du renvoi d'assistant personnel est soumise à divers contrôles par le système. Elle implique également que l'appelant externe connaisse la procédure d'accès au paramétrage de l'assistant personnel ainsi que le numéro de poste et le mot de passe personnel de l'usager interne.

Lorsque le renvoi externe de l'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 défini (aboutement ligne à ligne).

LE MD Evolution dispose de plusieurs paramètres de configuration permettant de contrôler la mise en place de ces renvois.

3.2 Gestion du mot de passe système

Les recommandations élémentaires d'Aastra en matière de sécurité sont de modifier les mots de passe par défaut :

- Mot de passe TLG (télégestion)
- Administration des boites vocales et standard automatique (boite 0000)
  - Accessible de l'extérieur pendant le message d'accueil (standard automatique ou boite vocale)
  - Attention ce mot de passe ne doit pas être réinitialisé, sa perte conduirait à repartir sur une configuration usine
- Boite vocale 0001 – Boite vocale du PO

3.3 Gestion du mot de passe usager

Les utilisateurs disposent d'un mot de passe individuel et leur responsabilité est importante dans la sécurisation d'un système. Un utilisateur qui utilise son assistant personnel doit impérativement gérer son mot de passe selon les règles usuelles de gestion des mots de passe rappelées ci-dessous :

- Un mot de passe est strictement personnel : ne le confiez à personne.
- Un mot de passe est unique : n'utilisez pas votre code deux fois, sur deux systèmes ou services différents
- Un mot de passe doit être changé régulièrement.
- Un mot de passe ne doit pas être accessible sans protection (par exemple affiché sur un post-it collé sur le tableau ou bien en vue sur le bureau …)
- Proscrire les mots de passe tels que 1234, 0000, 1111, etc...
- Un mot de passe doit être changé dès que l'on soupçonne sa compromission

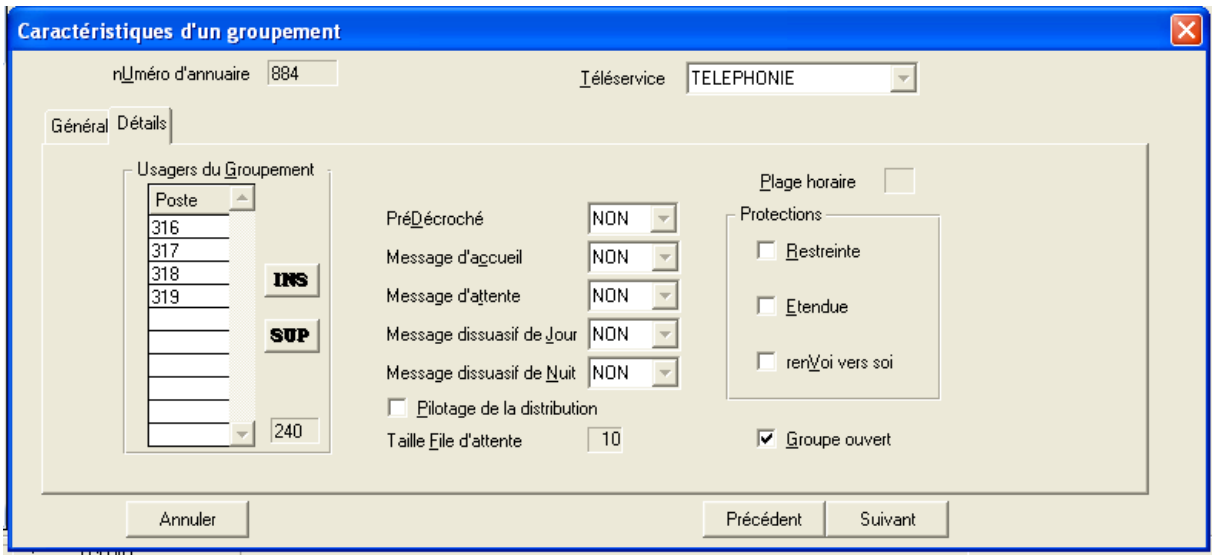
3.4 Recommandations complémentaires

Si une boite vocale est en mode Assistant Personnel nous vous recommandons d'interdire :

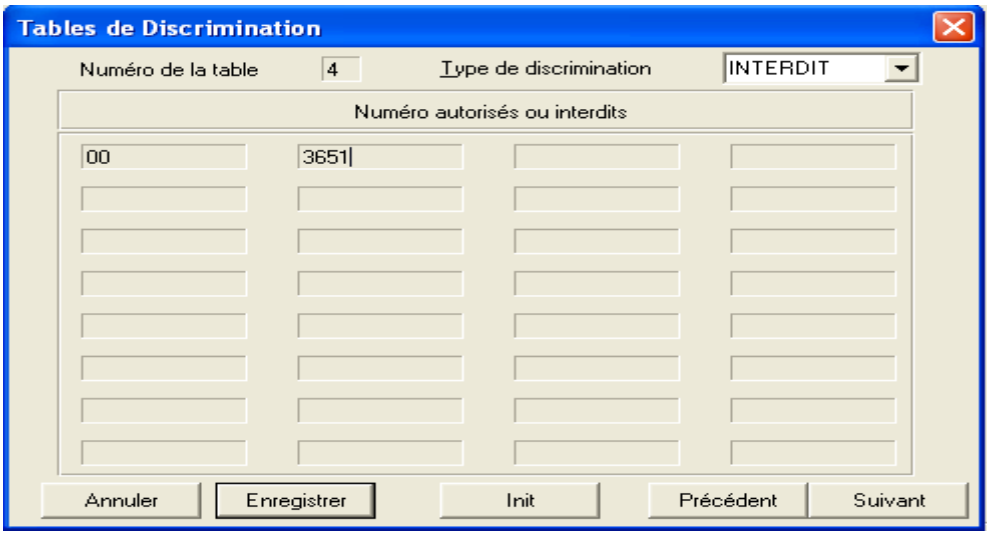
- le renvoi vers un numéro international
- Le préfixe 3651 (masquage du numéro)

Exemple de programmation avec TLG :
Le groupement des boites vocales (884 en standard) contient des usagers.
Il faut affecter à ces usagers (316, 317, 318 et 319 dans notre exemple) une classe de service ayant une table de Discrimination qui interdit l'international et le 3651.

- Groupement 884 :



- Table de Discrimination affectée aux postes du groupement 884 :



3.5 Versions logicielles

Par ailleurs comme pour tout équipement intégrant une dimension logicielle, Il est très fortement recommandé de mettre à jour les systèmes dans **le dernier état technique de chaque version.**

Au fur et à mesure de leur disponibilité, ces versions sont accessibles via l'extranet à l'adresse suivante :
http://support.aastra.fr/extra/Support/Soft%20MDE/DLSoft.php?action=Browse&lang=fr&target=/10%20-%20MDE

À la date d'édition du présent document, les versions à jour sont :

- R9.2 g030
- R10.0 h007
- R10.2 i042
- R11.0 SP2 (J025)