

PABX

PABX : Les PABX ou PBX sont des autocommutateurs téléphoniques privés (définition anglaise : Private Automatic Branch eXchange) destinés à alimenter et à mettre en relation une certaine quantité de postes téléphoniques internes dans une entreprise ou dans une administration.

DE QUOI PARLE T-ON ?

Souvent oublié dans la lutte contre le piratage, le taux d'effraction des autocommutateurs croît en toute impunité et cause un préjudice important (plusieurs milliers d'euros).

Ainsi des mesures de sécurité s'imposent pour sécuriser ce système de communication.

Bon nombre d'entreprises et d'administrations ignorent que leur PABX sert, de tremplin à des personnes malintentionnées pour amorcer des communications téléphoniques sur de longues distances.



Explications :

Les attaques les plus connues sont :

- Le phreaking : Cette méthode consiste à pénétrer dans les autocommutateurs privés et les systèmes de messagerie vocale. L'auteur se voit obtenir un accès gratuit au réseau téléphonique.
- Appropriation de la fonction « Outdial » : Il s'agit d'une méthode supportée sur certains PABX afin de commuter un utilisateur vers le réseau téléphonique. Cette fonction également désignée par "Thrudial" dans le jargon des spécialistes s'avère peu connue des usagers. Par ce biais, il est possible de réaliser un appel à partir de l'étranger avec le coût d'une communication locale.
- La messagerie vocale : Il s'agit d'une entrée utilisée par des pirates. Malgré une protection par mot de passe le pirate, averti par une abondante documentation qui circule sur Internet, entre en possession de la boîte vocale et n'a plus qu'à entamer la procédure d'accès à la fonction Outdial. Hormis l'obstacle du code confidentiel, le système de messagerie vocale s'avance comme un cheval de troie idéal pour accéder au PABX puis au réseau téléphonique.

Précautions :

Quelques règles simples permettent de se prémunir de ces attaques très connues des pirates :

- Vérifier quelles sont les prestations incluses dans le contrat de maintenance et principalement les mises à jours sécuritaires régulières.
- Le changement de mot de passe (MDP) système est impératif à l'installation du matériel. Le renouvellement du MDP doit être annuel. Sa complexité limitera fortement les intrusions.
- Les droits des utilisateurs doivent être gérés drastiquement.
- Attention aux offres « Lowcost » qui ne prennent en compte que rarement, la sécurité du PABX.

Réactions :

Que faire en cas de doute d'attaque ou si l'attaque est avérée :

- Des vérifications et une mise à jour des systèmes s'imposent (aide du prestataire de service).
- Sensibiliser les utilisateurs sur les événements survenus.
- En cas d'attaque avérée, déposer plainte auprès des services de police ou gendarmerie.

Si une plainte est déposée, elle couvrira juridiquement le titulaire du PABX et son prestataire, et elle permettra aussi de sensibiliser les fabricants et utilisateurs sur ce type d'attaque. La faille de sécurité découverte pourra être ainsi supprimée rapidement.