

Protégez votre PBX!

Le vol de service interurbain et de services de télécommunications ainsi que la fraude téléphonique prennent de nombreuses formes. Bien comprendre votre système de télécommunications et les techniques utilisées par les criminels vous permettra de réduire le risque d'être victime de ce type de crime.

1. Renseignez-vous sur votre système de télécommunications

- Familiarisez-vous avec les mesures de protection, les mécanismes de défense et les caractéristiques de sécurité.
- Identifiez les failles.
- Assurez-vous que le personnel connaît bien les mesures de protection et les procédures.

2. Sachez quelles voies d'accès ouvrent la porte à la fraude

- Accès direct au système (ADAS)
- Système de messagerie vocale
- Administration à distance du système (ports de maintenance)
- Sélection directe à l'arrivée
- Lignes de jonction et services de réseau de transit
- Modems

3. Surveillez et analysez l'information concernant vos systèmes

- Consultez les enregistrements des données d'appel et les données de facturation (les rapports d'exception peuvent contenir des indices révélateurs).
- Familiarisez-vous avec les habitudes d'appel et passez-les en revue.
- Consultez les rapports du système de messagerie vocale.
- Surveillez les tentatives d'appel valides et non valides, dans la mesure du possible.

4. Sachez reconnaître les signes d'une atteinte à la sécurité

- Plaintes concernant des lignes toujours occupées
- Changement soudain des habitudes d'appel, par exemple l'augmentation du nombre de faux numéros, de communications rompues sans parler, d'appels effectués la nuit, la fin de semaine ou les jours fériés, d'appels 800 et WATS, d'appels interurbains ou bizarres (mauvaises plaisanteries/obscénités)
- Appels interurbains provenant de la messagerie vocale
- Longues durées de mise en attente
- Appels 900 (lignes de bavardage) non expliqués
- Nombre élevé d'interurbains provenant d'un poste non autorisé

5. Assurez la sécurité de vos systèmes

Configuration des systèmes

- Limitez l'accès à des périodes précises (pendant les heures de bureau) et limitez les indicatifs régionaux de destination permis.
- Bloquez tous les interurbains faits la nuit, la fin de semaine et les jours fériés.
- Limitez le renvoi automatique aux appels locaux seulement.
- Bloquez tous les appels 10XXXX faits à partir de votre PBX si vous n'avez pas besoin de ce service.

- Bloquez le service outre-mer, limitez-en l'accès ou exigez l'assistance de la réceptionniste.
- Adoptez des politiques précisant dans quels cas accepter les appels à frais virés et fournir l'accès aux lignes externes.
- Informez les téléphonistes et les employés sur l'« ingénierie sociale » (ruses de fraudeurs qui tentent d'obtenir l'accès au système téléphonique ou le transfert d'appels par l'intermédiaire du PBX).
- Assurez la sécurité des salles d'équipement (verrouillez l'accès à l'équipement téléphonique et aux armoires de répartition).

PBX (commutateur privé) et ADAS (accès direct au système)

- Modifiez les codes par défaut après l'installation de nouvel équipement.
- Ne publiez jamais vos numéros de téléphone ADAS.
- Modifiez périodiquement votre numéro de téléphone ADAS.
- Produisez un code d'autorisation ADAS distinct pour chaque utilisateur et avertissez les utilisateurs de ne pas les noter sur papier.
- N'utilisez pas de numéros d'accès séquentiels.
- Utilisez des codes ADAS plus longs (au moins 7 caractères) et modifiez-les régulièrement.
- Débranchez les postes téléphoniques non utilisés.
- Limitez l'accès ADAS la nuit, la fin de semaine et les jours fériés (périodes de pointe pour la fraude).
- Bloquez ou limitez l'accès au réseau outre-mer.
- Programmez votre système de manière à ce qu'il réponde silencieusement après cinq ou six sonneries (les pirates ciblent les systèmes qui répondent en produisant une tonalité constante).
- Détectez les tentatives d'accès non valides à votre ADAS et acheminez-les à un téléphoniste.
- Installez des ports ADAS qui rompent la communication lorsqu'un code non valide est entré.
- Programmez votre PBX pour qu'il émette une alarme lorsqu'un nombre inhabituel de tentatives non valides est effectué et pour que le port soit désactivé après un nombre donné de tentatives non valides.

Systèmes de messagerie vocale

- Adoptez des procédures pour la création et la modification des mots de passe.
- Modifiez régulièrement les mots de passe.
- Utilisez des mots de passe de longueur maximale pour la boîte du gestionnaire du système et les ports de maintenance.
- Interdisez l'utilisation de mots de passe trop simples (p. ex. 222, 123, nom de famille, etc.)
- Limitez le nombre de tentatives de connexion infructueuses à cinq ou moins.
- Modifiez tous les mots de passe par défaut.
- Bloquez l'accès aux circuits du service interurbain et les options d'appel à frais virés de la fonction de réception automatique.
- Bloquez ou, idéalement, supprimez toutes les boîtes vocales inactives.
- Limitez l'envoi de messages hors système.
- Si le système permet à un appelant de réacheminer son appel vers un autre poste, bloquez tous les chiffres qu'un pirate pourrait utiliser pour obtenir une ligne externe, plus particulièrement les codes d'accès au réseau interurbain.
- Effectuez des vérifications de routine de l'état et de l'utilisation de votre système.

Ports d'accès à distance

- Bloquez l'accès aux ports de maintenance à distance et aux ports de gestion du système.
- Utilisez des codes d'accès d'une longueur maximale et modifiez-les régulièrement.

Modems

- Utilisez des mots de passe d'une longueur maximale et modifiez-les régulièrement.
- Supprimez la conférence à trois sur tous les postes qui utilisent des modems.
- Débranchez les modems non utilisés.