cogeco | AFFAIRES

Directives sur la sécurité de la Téléphonie hébergée pour les clients de la solution de Liaisons SIP

Découvrez comment optimiser la sécurité de votre système téléphonique avancé. Protégez votre entreprise contre les imprudences et aidez à prévenir les accès non autorisés en suivant ces directives.

Accès à distance

Registres des accès à distance

- Pour assurer l'identification de tous les utilisateurs de l'accès à distance, un registre détaillé doit être maintenu.
- Ces registres doivent inclure une trace de contrôle permettant d'identifier les personnes qui ont accédé à la Téléphonie hébergée, y compris l'heure, la date, les identifiants des utilisateurs et, si possible, les historiques des événements (les transactions qui ont eu lieu).
- Bien qu'il ne soit pas nécessaire de vérifier ces registres quotidiennement, ils devraient être examinés périodiquement. Ces registres sont particulièrement importants lors d'enquêtes sur des activités inhabituelles.
- Tenez compte des personnes qui accèdent à votre Téléphonie hébergée à distance (par exemple, les vendeurs, les administrateurs ou le personnel d'assistance technique de l'entreprise).

Procédés d'authentification

- Les dispositifs d'authentification tels que les cartes à puce ou tout autre dispositif d'authentification au moyen de jetons procurent une protection supplémentaire.

Affichage d'informations sur l'accès à distance

- Les numéros de téléphone d'accès à distance, ainsi que les protocoles de connexion et les mots de passe, ne doivent jamais être affichés ou publiés.

Tentatives de connexion répétées

- La Téléphonie hébergée doit mettre fin à l'appel après 3 tentatives de connexion échouées afin de dissuader les utilisateurs non autorisés.

Gestion de l'accès DISA

- Si l'accès direct au système (DISA) est utilisé pour accéder à la Téléphonie hébergée, le code d'accès ou le mot de passe doit rester confidentiel, être modifié souvent et supprimé immédiatement s'il n'est plus requis. Nous vous recommandons également d'utiliser le nombre maximum de caractères (de 10 à 15 autant que possible).

Gestion des appels

Profil d'appels

- Il est essentiel de définir les habitudes d'appel au sein de l'entreprise. Par exemple, les appels internationaux sont-ils requis pour tous, ou seulement pour quelques utilisateurs sélectionnés ?
- Un système de recueil des profils d'appels (Call Detail Recorder ou CDR) fournit un aperçu actualisé des habitudes d'appel et permet de déterminer si des restrictions sont nécessaires et si elles fonctionnent lorsqu'elles sont activées.

Activation des restrictions

- Au besoin, bloquez tous les indicatifs de pays inutiles et les autres NNX de votre choix, ainsi que la ligne 1 900.

Numéros sans frais

- Si votre entreprise utilise des numéros sans frais (tels que 1-800, 1-866, 1-877 ou 1-888), nous vous recommandons de bloquer tous les indicatifs régionaux et nationaux qui ne sont pas nécessaires afin d'éviter les appels frauduleux.

Systèmes de messagerie vocale

Sécurité des mots de passe

- Les mots de passe ou les NIP doivent comporter un minimum de 6 caractères (ce nombre peut être défini dans le système). Il est préférable d'utiliser le nombre maximal de caractères.
- Les mots de passe ne doivent pas être faciles à deviner, et ne doivent jamais être affichés ou partagés. N'utilisez pas de combinaisons de chiffres telles que l'emplacement du téléphone ou le numéro de téléphone à 7 chiffres. Il est recommandé d'utiliser, si possible, des logiciels qui testent la sécurité des mots de passe.
- Lors de la création d'un nouvel utilisateur, les mots de passe doivent être générés de façon aléatoire et ne doivent jamais correspondre à l'emplacement du téléphone.
- Un logiciel doit être utilisé pour inviter les employés à changer leurs mots de passe à intervalles d'au moins 90 jours (un intervalle de 30 jours est préférable). Si le logiciel n'est pas disponible, des politiques doivent être mises en place pour informer tous les employés de l'importance de changer fréquemment leurs mots de passe.

Boîtes vocales inutilisées

- Toutes les boîtes vocales vides ou inutilisées doivent être supprimées. Les boîtes vocales inactives peuvent être utilisées à des fins frauduleuses.

Boîtes vocales partagées

- Pour les boîtes vocales partagées ou collectives, une personne doit être désignée pour en assurer la gestion, notamment pour supprimer les messages et s'assurer que le message d'accueil est inchangé.

Composition abrégée

- Si la composition abrégée n'est pas nécessaire, cette fonction doit être désactivée, en raison du nombre important de fraudes commises à l'aide de cette fonction dans le système de messagerie vocale.

- Si cette fonction doit être utilisée, les relevés quotidiens de composition abrégée doivent être surveillés, surtout après les heures de bureau.
- Les codes d'accès aux lignes sortantes typiques ne doivent pas être utilisés, tels que 9, 8, 9+0, 9+1, 9+011, 9+1-800/866/877/888.

Rapports d'activité des ports

- Les ports du système de messagerie vocale doivent être surveillés au moyen de rapports d'activité pour vérifier qu'aucun accès non autorisé n'a eu lieu. Ceci permettra de détecter les tentatives d'accès non autorisées au système de messagerie vocale, ainsi que les abus de services téléphoniques.

Codes d'accès

Sélection des codes d'accès

- Tous les codes d'accès utilisés doivent être choisis au hasard, et non dans un ordre séquentiel, afin qu'ils ne soient pas faciles à deviner. Autant que possible, un minimum de 6 caractères doit être utilisé pour les codes d'accès ou les mots de passe.

Codes d'accès inactifs

- Veuillez désactiver, dans le système, les codes qui ne sont pas utilisés par les employés en poste.

Renvoi d'appel

Restrictions applicables au renvoi d'appel

- Le renvoi d'appel doit être limité à 4 chiffres, si possible, afin d'éviter le renvoi vers un numéro externe. Cela permet d'éviter les abus et frais chargés qui pourraient être liés à la fonction de renvoi d'appel.

Salle téléphonique

Sécurité des équipements

- Pour protéger les appareils de Téléphonie hébergée et leurs périphériques, la salle téléphonique ou la salle d'équipement doit être fermée à clé et faire l'objet de rapports sur les personnes qui y ont accédé.
- Les dispositifs d'accès par carte permettant à vos employés de scanner une carte pour accéder à la salle sont efficaces à cet égard.

Autres ressources

Si vous avez des questions sur les risques de fraude ou sur la sécurité de la Téléphonie hébergée, nos experts sont là pour vous aider et répondre à toutes vos questions au **1 855 494-5853**.