

Liste de contrôle de la conformité – Transmission de la voix

PBX (autocommutateur privé)

Accès à distance

Qui a accès à votre autocommutateur privé à distance ? Ex. : fournisseurs, soutien technique interne, administrateurs.

- ⌚ Vous devriez tenir un registre exhaustif pour être sûr que tous les utilisateurs distants sont identifiés.

Y a-t-il une piste de vérification vous permettant de déterminer qui a eu accès à l'autocommutateur privé ? Le rapport indique-t-il l'heure, la date et l'identification de l'utilisateur ?

- ⌚ Vous devriez tenir des registres indiquant qui a accédé à distance à l'autocommutateur privé. Ils devraient identifier l'utilisateur, la date et l'heure et, si possible, contenir le journal des événements (transactions effectuées). Bien qu'il ne soit pas nécessaire d'examiner ces registres tous les jours, vous devriez le faire régulièrement. Ces registres sont particulièrement utiles lorsque vous enquêtez sur des activités inhabituelles.

Quelle méthode d'authentification est utilisée lorsqu'on accède à l'autocommutateur privé ?

- ⌚ Des dispositifs d'authentification, comme des cartes à puce ou autres jetons d'authentification, représentent une couche de sécurité supplémentaire.

Les numéros de téléphone d'accès à distance sont-ils publiés ?

- ⌚ Les numéros d'accès, les procédures d'ouverture de session et les mots de passe ne devraient jamais être affichés.

L'autocommutateur privé met-il fin à l'appel après trois tentatives infructueuses d'accès ?

- ⌚ Il est recommandé de mettre fin à l'appel après trois tentatives infructueuses d'accès à l'autocommutateur privé. Ceci prévient les multiples tentatives non autorisées.

L'ADAS (accès direct au système) est-il utilisé pour l'accès à l'autocommutateur privé ? Si oui, comment le code d'accès est-il géré ?

- ⌚ Si l'ADAS est nécessaire, les codes d'accès ou mots de passe doivent être gardés secrets, être changés souvent, compter le nombre maximum de caractères (on recommande d'en utiliser de 10 à 15) et être supprimés immédiatement lorsqu'ils ne sont plus requis.

Restriction de l'accès à l'interurbain

Quel niveau d'interurbain est nécessaire dans l'entreprise ?

- ⌚ Il est important de déterminer les besoins d'interurbain dans l'entreprise. Est-ce que tout le monde a besoin de faire des appels à l'étranger ou seulement quelques personnes ?

Des restrictions de l'accès à l'interurbain adéquates ont-elles été mises en place ?

- ⌚ Bloquez tous les indicatifs régionaux, indicatifs de pays et indicatifs de central inutiles, de même que les numéros 1 900, au besoin.

Existe-t-il une piste de vérification ou un enregistrement permettant de déterminer les habitudes d'appel ? Un système d'enregistrement des données d'appel est-il utilisé pour les appels interurbains ?

- ⌚ L'enregistrement détaillé des appels donnera un aperçu des habitudes d'appel interurbain; il aidera à déterminer si les tables de restriction sont utilisées de manière appropriée.

L'entreprise utilise-t-elle des numéros sans frais comme 1 800/866/877/888 ? Les appels entrants sont-ils toujours permis quelle que soit leur origine ?

- ⌚ Bloquez tous les indicatifs régionaux et indicatifs de pays inutiles dans la mesure du possible. Un grand nombre de fraudes émanent de New York, en particulier des codes régionaux 212 et 718.

Systemes de messagerie vocale

Les mots de passe comptent-ils au moins six caractères ?

- ⌚ Les mots de passe et NIP devraient compter au moins six caractères. Il serait souhaitable d'utiliser le nombre maximal de caractères. Le système devrait être programmé pour n'accepter qu'un minimum de six caractères.

Les mots de passe sont-ils faciles à deviner ou affichés ?

- ⌚ Les mots de passe ne devraient pas être faciles à deviner, et ils ne devraient jamais être affichés ni divulgués. N'utilisez pas de système de numéros courants comme le local ou le numéro de téléphone à sept chiffres. Des progiciels recherchant les mots de passe courants devraient être utilisés dans la mesure du possible.

Des mots de passe sont-ils générés automatiquement pour les nouveaux abonnés ?

- ⌚ On ne devrait jamais choisir le local comme mot de passe lorsqu'on fait la mise en service pour un nouvel abonné.

Le système de messagerie vocale est-il programmé pour exiger un changement de mot de passe tous les 30 à 90 jours ?

- ⌚ Il faudrait utiliser un logiciel invitant les employés à changer leurs mots de passe au moins tous les 90 jours. Si un tel logiciel n'est pas disponible, il faudrait mettre en place des politiques expliquant aux employés l'importance de changer fréquemment les mots de passe.

Les boîtes vocales non attribuées ont-elles été supprimées ?

- ⌚ Toutes les boîtes vocales qui sont vides ou qui n'ont pas été attribuées devraient être supprimées. Les boîtes vocales vides peuvent être utilisées à des fins frauduleuses. Seuls les employés actuels devraient disposer d'une boîte vocale.

Si des boîtes vocales partagées ou de groupes sont utilisées, comment sont-elles gérées ?

- ⌚ Une personne devrait se charger de gérer les boîtes vocales de groupe, c'est-à-dire d'en effacer les messages et de vérifier que le message d'accueil n'a pas été modifié.

La prise directe contrôlée du réseau est-elle utilisée ? Si oui, comment est-elle gérée ?

- ⌚ Si cette fonction n'est pas nécessaire, elle devrait être désactivée. Un nombre considérable de fraudes exploitent cette fonction du système de messagerie vocale. Si elle doit être utilisée, il faudrait surveiller les rapports quotidiens sur la prise directe contrôlée, surtout après les heures normales de bureau. De plus, les codes d'accès au réseau interurbain types (par exemple 9, 8, 9+0, 9+1, 9+011, 9+1 800-866-877-888, etc.) ne devraient pas être utilisés.

Y a-t-il une surveillance des ports du système de messagerie vocale visant à vérifier qu'il n'y a pas eu d'accès non autorisé ?

- ⌚ Les rapports sur l'activité des ports devraient être examinés souvent. Ceci déterminera si des tentatives d'accès non autorisé au système de messagerie vocale ou des appels interurbains frauduleux ont eu lieu.

Codes d'accès

Les codes d'accès utilisés sont-ils en ordre séquentiel ?

- ⌚ Tous les codes d'accès utilisés devraient être sélectionnés au hasard afin d'être plus difficiles à deviner. Les codes d'accès ou mots de passe devraient compter au moins six caractères dans la mesure du possible.

Y a-t-il des codes d'accès inactifs dans le système ?

- ⌚ Désactivez les codes qui ne sont pas utilisés par des employés actuels.

Caractéristiques

Des restrictions sont-elles appliquées au renvoi automatique lorsque c'est approprié ?

- ⊕ Le renvoi automatique devrait être restreint à quatre chiffres dans la mesure du possible pour empêcher le renvoi à un numéro externe. Ceci prévient les appels interurbains frauduleux par le biais de la fonction de renvoi automatique.

Salle d'équipement téléphonique

La salle d'équipement téléphonique est-elle verrouillée adéquatement pour protéger le matériel de l'autocommutateur privé et ses périphériques ?

La salle d'équipement devrait être verrouillée. Il faudrait aussi tenir une piste de vérification indiquant qui y a eu accès. Les dispositifs de contrôle d'accès à carte peuvent jouer ce rôle.