Il suffit de quelques heures de piratage pour subir des préjudices de plusieurs dizaines de milliers d'euros.

Quelques chiffres :

• 15,4% d'augmentation des pertes dues aux fraude depuis 2011

• 4,4 milliards de dollars de pertes estimées dues aux fraudes en 2013

• La plus grande fraude recensée en France à provoquée un perte de 600 000 € à l'entreprise.

Comment les fraudeurs opèrent-ils ?

Généralement, les fraudeurs obtiennent l'accès au système de communication depuis l'extérieur de l'entreprise en exploitant des failles de sécurité. Les anciennes méthodes consistaient entre autres à pirater le PABX directement via le port de maintenance, mais les techniques ont évolué et comprennent désormais le détournement des applications voix et la tromperie de l'utilisateur final, rendant ainsi difficile la détection de l'appelant car l'appel semble provenir d'une « entité de confiance » et non du fraudeur.

Les méthodes les plus utilisées sont les suivantes :

Maintenance à distance

Les pirates détectent le modem relié au port de maintenance et essaient de se connecter en utilisant le mot de passe par défaut, que l'administrateur oublie souvent de changer. Une fois entrés dans le système, ils peuvent modifier la configuration à leur guise ainsi que les identifiants et les mots de passe de connexion.

Messagerie vocale

Cette méthode cible la messagerie vocale, qui est piratée en exploitant la faiblesse de la sécurisation par mot de passe. En général, l'attaque vise à utiliser la messagerie vocale pour émettre des appels sortants vers un numéro surtaxé ou longue distance. Les ponts de téléconférence dotés de plusieurs lignes constituent des cibles de choix.

Transfert externe, renvoi externe

Les droits d'appel externe des postes, s'ils ne sont pas configurés de façon appropriée, peuvent permettre aux pirates de mettre facilement en place des scénarios de fraude. Certains modes d'exploitation requièrent toutefois un complice au sein de l'entreprise

Protéger votre système de communications

Prendre des mesures de sécurité appropriées

• Restriction d'appel : restreindre les appels sortants hors des heures de bureau et interdisez l'appel de numéros surtaxés.

• Réévaluez les règles relatives aux mots de passe : changez les mots de passe système par défaut et continuez à les modifier régulièrement.

• Mettre en place une protection pour les transferts et les renvois externes.

• Mettez à jour la base de données du système en supprimant les informations concernant les anciens utilisateurs.

Renforcez la sensibilisation interne

• Sensibilisez les salariés aux pratiques élémentaires de sécurité et aux impacts associés (notamment les risques juridiques et financiers), ainsi qu'à leurs devoirs et responsabilités.

• Rappelez aux collaborateurs les pratiques de bon sens concernant les règles de confidentialité, comme ne jamais révéler de détails techniques sur les systèmes d'information et de communication à des interlocuteurs inconnus (par ex. codes personnels, noms, numéros directs de serveur vocal interactif et de messagerie vocale).

• Déployez des campagnes de sensibilisation à la fraude : encouragez les salariés à signaler des comportements ou des activités inhabituels concernant les services téléphoniques, notamment les messages étranges sur les boîtes vocales, les lignes occupées tôt le matin et la présence de nombreux appels hors des heures de bureaux dans les journaux d'appel.

Tirez parti de l'expertise de votre Business Partner et d'Alcatel-Lucent

• Maintenez à niveau les versions logicielles pour bénéficier des améliorations produit et des évolutions technologiques les plus récentes.

• Renforcez les solutions en mettant en œuvre les bonnes pratiques en matière de sécurité.

• Évaluez régulièrement la sécurité des systèmes de communication et notamment l'exposition aux fraudes téléphoniques.

N'hésitez pas à nous contacter pour toutes informations de sécurité pour votre installation Alcatel OMNIPCX Office.