FRAUDE TÉLÉPHONIQUE

SÉCURISER LES SYSTÈMES DE COMMUNICATION DES ENTREPRISES EST UNE NÉCESSITÉ

NOTE D'APPLICATION

Alcatel·Lucent Enterprise

TABLE DES MATIÈRES

INTRODUCTION

La fraude aux dépends des fournisseurs de services de téléphonie, des opérateurs, des abonnés et des entreprises ne cesse de s'étendre. Le développement de ces pratiques est dû à la possibilité qu'ont les fraudeurs de gagner de l'argent en exploitant l'absence d'une autorité internationale de régulation des télécommunications efficace ou de mécanismes de contrôle, combinée aux failles dans la sécurité organisationnelle des systèmes de télécommunication.

SCÉNARIOS CLIENTS

1. Le responsable informatique d'une entreprise découvre un pic d'appels vers un pays avec lequel la société ne travaille pas – en dehors des heures de bureau normales.
2. Le rapport de taxation mensuel d'une autre entreprise indique un important volume d'appels vers des numéros internationaux – provenant du même téléphone interne.
3. Un magasin de 20 employés reçoit une facture téléphonique mensuelle équivalente au cumul de ses communications sur les 3 dernières années.
4. Une organisation reçoit une alerte à la fraude de son opérateur de téléphonie – au moment même où elle détecte des appels multiples, réguliers et de courte durée vers un numéro surtaxé.

Les pertes dues aux fraudes ont augmenté de 15,4 % depuis 2011

QUE S'EST-IL PASSÉ ?

Ces scénarios sont des exemples de fraude téléphonique subie par des clients. Toutes les organisations, depuis les plus petites entreprises jusqu'aux sociétés multinationales, sont des victimes potentielles, et ceci quel que soit le fournisseur de leur système de communications. Qui plus est, le nombre d'attaques est en augmentation rapide.

La fraude téléphonique se définit comme l'utilisation non autorisée d'un service de communication par un tiers inconnu. Elle peut se présenter sous forme de revente de minutes de communication à travers une entité insoupçonnée (comme par exemple un PABX piraté). La fraude aux numéros surtaxés est un autre exemple, un système ou un service de communication étant dans ce cas exploité pour passer des appels vers des numéros surtaxés internationaux qui reversent de l'argent par minute ou par appel à l'abonné.

Avant d'être détectée, la fraude peut entrainer de très conséquentes pertes financières. Dans le pire des cas, il peut s'écouler un mois complet avant que le rapport de taxation ne permette d'identifier la fraude. La fraude peut même porter atteinte à la réputation d'une marque : dans certains cas, des clients qui appelaient leur conseiller personnel ont été mis en communication avec un service surtaxé sans aucun rapport et potentiellement embarrassant. En outre, en surchargeant le serveur de communication, ces fraudes peuvent affecter la disponibilité des services téléphoniques, conduisant potentiellement à une interruption de service.

Pertes estimées dues aux fraudes par piratage de PABX en 2013 :

4,4 milliards de dollars (USD)*

Pourquoi la fraude dans les télécoms se développe-t-elle ?

L'essor des réseaux et des médias sociaux a grandement facilité la diffusion de guides pratiques – des vidéos et des tutoriels de courte durée qui expliquent comment compromettre des systèmes de communication. Très peu de compétences en télécommunications suffisent pour accéder à des services non autorisés et gagner de l'argent en exploitant les moyens de communication d'une entreprise ciblée.

De plus, bien que des mécanismes de protection soient intégrés aux systèmes de communication, les recommandations des constructeurs en matière de sécurité ne sont souvent pas entièrement implémentées et les configurations pas optimisées en raison d'un manque de sensibilisation. Ces omissions dans la sécurité peuvent faciliter le piratage.

Enfin, les entreprises disposant de systèmes anciens sont potentiellement plus exposées à ces types de menace.

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 systèmes, 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.

Restriction d'appels

En plus d'exploiter une politique déficiente en matière de mots de passe, les pirates peuvent tirer parti de contrôles d'appels peu rigoureux, leur logiciel de composition automatique de numéros pouvant ainsi passer en toute tranquillité un nombre illimité d'appels vers des numéros surtaxés ou longue distance.

Accès direct au système (DISA)

Ce service, conçu pour les personnes travaillant à distance, permet aux collaborateurs d'accéder aux services de téléphonie interne à partir de sites distants. Il est possible à des utilisateurs malveillants d'exploiter totalement ou partiellement à distance les fonctionnalités d'un PABX si le service DISA est insuffisamment protégé (par ex. code d'accès unique, pas de contrôle de l'identifiant de l'appelant).

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.

QU'EST-CE QUI MOTIVE LES FRAUDEURS ?

Bien que la fraude téléphonique puisse être utilisée pour porter atteinte à la santé financière d'une entreprise ou altérer la réputation d'un concurrent, elle est le plus souvent motivée par l'appât du gain. Alcatel-Lucent a été témoin de fraudes ayant rapporté 20 000 USD en quatre heures à leurs auteurs – de l'argent rapide et facile. Les fraudeurs peuvent aussi se trouver au sein de l'entreprise, comme dans le cas de salariés malhonnêtes attirés par la perspective de détourner à leur profit les ressources de la société.

La principale méthode de fraude émergeante est le piratage de PABX*

ÉVALUER LA VULNÉRABILITÉ DE L'ORGANISATION

Les mêmes mots de passe système sont-ils utilisés depuis plus d'un an ?

Les utilisateurs finaux utilisent-ils pour leur messagerie vocale des mots de passe par défaut ?

Des modems sont-ils connectés au serveur de communication ?

Les utilisateurs finaux ont-ils tous accès aux numéros internationaux ?

Les services de téléphonie sont-ils fournis aux utilisateurs à l'extérieur de l'entreprise ?

Y a-t-il eu récemment des mouvements de personnel au sein de l'équipe d'administration système ?

RÉPONDRE « OUI » À L'UNE QUELCONQUE DE CES QUESTIONS RÉVÈLE UN RISQUE POTENTIEL.

PROTÉGER LES SYSTÈMES DE COMMUNICATION

L'application des mécanismes de protection et des bonnes pratiques Alcatel-Lucent aux systèmes de communication contribue à optimiser à la fois la configuration et la sécurité, ainsi qu'à éviter de nombreux scénarios de fraude téléphonique.

Prenez des mesures de sécurité appropriées

- Restriction d'appel : restreignez les appels sortants hors des heures de bureau, exigez des mots de passe pour les appels longue distance 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 (par ex. tous les mois).
- Mettez en place une protection pour les transferts et les renvois externes.
- Réexaminez les responsabilités et les droits d'administration.
- 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.
- Appliquez les derniers correctifs de sécurité du constructeur.
- Évaluez régulièrement la sécurité des systèmes de communication et notamment l'exposition aux fraudes téléphoniques.

* Source : Communications Fraud Control Association, enquête 2013

Alcatel·Lucent Enterprise