Comment protéger votre téléphonie d'entreprise contre les fraudes?

Toutes les entreprises, des PME aux Multinationales, sont des cibles potentielles de fraudes téléphoniques.
Factures téléphoniques exorbitantes pouvant potentiellement financer des organisations malveillantes, détérioration de votre image de marque et conflits juridiques ne sont que quelques conséquences des dommages que vous pourriez subir.

Les fraudeurs savent que les entreprises consacrent une partie importante de leur budget IT à la sécurité informatique mais négligent parfois leurs systèmes de téléphonie. Les PABX et les messagerie vocales sont souvent des proies faciles...

nxo
NEXTIRAONE

Le Piratage Téléphonique

Le piratage téléphonique est appelé « Phreaking ». Il s'agit d'une contraction de *phone* (téléphone) et de *freak* (marginal ou personne appartenant à une contre-culture).

EN QUOI CONSISTE-T-IL?

Le phreaking consiste à pirater les réseaux téléphoniques via Internet ou le réseau RTC, avec l'intention de frauder et d'en retirer des avantages personnels ou des gains financiers.

Dans la majorité des cas, cette fraude se limite à percer les systèmes téléphoniques afin de téléphoner gratuitement.

LES DIFFERENTS TYPES DE MENACES

Nous distinguons 3 ensembles de méthodes d'attaques:

Le déni de service:

En interrompant le service de communication, le « phreaker » interrompt l'activité de l'entreprise et détériore son image vis-à-vis de ses clients et partenaires.

L'intrusion dans l'entreprise:

Dans le but de collecter des informations, le « phreaker » procède à des écoutes illégales ou accède aux SI aux travers de systèmes de communication ou de PC hébergeant des soft phones.

Les fraudes téléphoniques:

Afin de tirer illégalement profits du système téléphonique d'une entreprise, le « phreaker » peut: utiliser de façon abusive le service de téléphonie, pirater des messageries vocales, effectuer des renvois vers des numéros surtaxés, ou encore revendre des communications à des tiers.

QUAND CELA SE PASSE-T-IL?

La plupart du temps, ce genre d'attaques s'effectuent la nuit ou en week-end afin d'éviter toutes interventions humaines ou repérages.

Nous avons repéré pour vous certains signes qui doivent vous alerter sur une éventuelle fraude, et mettons à votre disposition quelques bonnes pratiques de préventions afin de réduire les risques d'attaques sur les systèmes de téléphonie d'entreprise.

4 signes précurseurs d'une potentielle fraude

1. Une **augmentation des appels internationaux** en dehors des heures de bureau, vers un pays avec lequel vous ne faites pas affaire.

2. Un **volume important d'appels** placés vers des numéros internationaux à partir du même poste interne.

3. Une **facture inattendue** équivalente à plusieurs années de dépenses.

4. Une **notification de votre opérateur**, montrant des appels multiples, réguliers et de courte durée vers un numéro surtaxé.

Les bonnes pratiques pour diminuer les risques de fraude

Mise à jour des équipements

- Garantir les dernières améliorations et évolutions en terme de sécurité.
- Renouveler les équipements obsolètes

Politique de sécurité utilisateurs

- Changer les mots de passe utilisateurs régulièrement (1 fois par trimestre)
- Proscrire les mots de passe de types 1234, 0000, n° du poste… Il est préférable d'avoir une casse complète (majuscule, minuscule, caractère spécial…)
- Veiller à ce que les utilisateurs verrouillent leur poste en dehors des périodes d'utilisation (absences, vacances…)
- Renforcer la sensibilisation interne autour de la sécurité

Politique de sécurité système

- Pour chaque poste, paramétrer ses possibilités de renvoi, de transfert, de messagerie vocale…
- Vérifier ses droits d'appel à l'international, ne conserver que ce qui est utile à l'activité.
- Définir des mots de passe administrateurs complexes

Surveillance

- Auditer les équipements

Maintenance intégrateur / constructeur

- Accéder aux alertes et mises à jour
- Bénéficier d'un support technique

Les solutions NextiraOne

Pour réduire les risques de piratage téléphonique, **NextiraOne** peut vous aider concrètement en se basant sur son expérience et sur une gamme complète de services et de solutions. Ces solutions et services sont plus particulièrement disponibles sur les systèmes de téléphonie d'entreprise de marque Alcatel-Lucent Enterprise, Cisco et Microsoft.

1 - L'AUDIT DE VOTRE INSTALLATION TÉLÉPHONIQUE

Il est une première solution qui permet de détecter les éventuelles failles de sécurité matérielles et logicielles. Le service **Checkup** de NextiraOne permet ainsi de vérifier, à la demande, l'état général de votre installation (accès de télémaintenance, sauvegardes, énergie, versions, composants, environnement…). Les techniques de piratage évoluant constamment, nous vous conseillons d'effectuer un audit complet de votre système, **au moins 1 fois par an**.Le service **Prevent** de NextiraOne vous permet de programmer cette maintenance préventive systématiquement.

2 - LA MISE À JOUR DE VOTRE VERSION DE PABX.

Chaque version a une durée de vie d'environ 18 mois et les anciennes versions ne sont plus supportées par les éditeurs après 24 mois suivant cette fin de vie en moyenne. Nous vous conseillons donc de procéder à la migration de votre PABX ou IPBX à la dernière version en vigueur. Ceci permet, dans de nombreux cas, de mieux se protéger contre le piratage, les éditeurs n'apportant des améliorations que sur les versions en cours de commercialisation.

3 - LA MISE EN PLACE D'UNE MÉTHODE DE TÉLÉMAINTENANCE SÉCURISÉE.

Les modems sont aujourd'hui à bannir de par les risques qu'ils représentent. Privilégiez les solutions de télégestion qui utilisent les technologies d'authentification fortes de type **IP VPN**, avec changement de mots de passe systématiques ou Token. Nextiraone vous propose pour cela son accès sécurisé : **PACS.** Nous vous conseillons d'y souscrire si ce n'est déjà fait.

Les solutions NextiraOne

4 - LE REMPLACEMENT DE VOTRE ACCÈS OPÉRATEUR RTC

Remplacez votre opérateur RTC Analogique ou Numérique de type T0 ou T2, par un accès **SIP Trunking** associé à la mise en place d'une passerelle de sécurité et de routage de type SBC (Session Border Controller). Cette solution présentera un double avantage pour vous : sécuriser votre accès opérateur en gardant les mêmes services de téléphonie, mais également anticiper la disparition des lignes RTC annoncées pour les prochaines années par l'opérateur historique. **Nextiraone** vous propose son offre de SIP Trunking appelée **LinkerSIP** pour bénéficier de ce double avantage.

5 - LES SOLUTIONS SPÉCIFIQUES DE SÉCURISATION DES FLUX VOIX

Pour les clients pour qui la sécurité de la voix et des données est vitale, nous mettons en place des solutions type **Firewall voix** sur des architectures de téléphonie traditionnelles ou IP **.** NextiraOne s'est associé avec les leaders de la sécurité IT tels que Cisco, Checkpoint, Checkphone, Oracle, Audiocodes, Sonicwall ou encore Thales, pour vous proposer la solution la mieux adaptée à votre besoin.

6 - LE REMPLACEMENT DU WAN PUBLIC PAR UN WAN DÉDIÉ ET SÉCURISÉ

Nous accompagnons les entreprises multi sites, en concevant et déployant des solutions de WAN sécurisés en cœur de réseau et adaptés à vos spécificités de gestion des flux. Les solutions **One Build** et **linker connect** de NextiraOne ont été conçues pour vous apporter ces services en mode sur mesure ou opéré.

7 - LA SOLUTION DE COMMUNICATION ET COLLABORATION DANS LE CLOUD.

Enfin, NextiraOne propose aux entreprises une **solution globale** entièrement sécurisée et basée sur le Cloud. Nous la contrôlons de bout en bout et vous offrons ainsi une garantie supplémentaire de sécurité. **Easycollab cloud** est une solution où tout est compris : services, matériels, logiciels, accès et trafic sécurisés. Vous souscrivez ainsi à un services payés à la consommation toujours l'état de l'art, qui vous garantit le plus haut niveau de sécurité.

En savoir plus : ICI

NextiraOne

A Propos:

NextiraOne est une société française indépendante, leader sur son marché et spécialisée dans l'intégration et la gestion des flux digitaux des entreprises. Elle conçoit, déploie et exploite des solutions et services pour plus de 20 000 clients des secteurs privé et public,. Très présente localement avec 44 implantations en métropole et dans les DOMTOM, NextiraOne compte aujourd'hui près de 1 400 employés, dont 850 experts qualifiés. Forte de ses expertises en matière de Communication & Collaboration, Infrastructures digitales, Sécurité & Services, NextiraOne accompagne les entreprises dans leur transformation digitale et s'appuie pour cela sur 400 collaborateurs certifiés et près de 900 certifications actives chez les plus grands acteurs technologiques. NextiraOne est également créatrice de talents. Elle porte notamment une attention particulière à l'évolution de ses équipes et mène une politique active autour de l'alternance avec plus de 100 alternants, soit près de 10% de ses effectifs. Pour en savoir plus, nextiraone.eu

Joindre NextiraOne (NXTO France) :

STANDARD
0 821 201 201 (0,18€ TTC/min)

CENTRE DE SERVICE CLIENT
0 825 030 020 (0,09€ TTC/min)

contact@nextiraone.eu