Piratage téléphonique :

comment lutter contre la malveillance ? Des solutions simples et efficaces existent pour toutes les entreprises.

Handbooks

Sommaire

Introduction

De nos jours, l'Internet met l'attirail du parfait hacker à portée de main. En effet des sites facilement accessibles recensent les failles des serveurs de téléphonie, des logiciels permettent de scanner les serveurs pour détecter des comptes, et d'autres encore vous offrent la possibilité de trouver les mots de passe associés.

Ainsi le mercredi après-midi de préférence, Kevin 15 ans, du fond de sa chambre peut venir prendre le contrôle de votre serveur VoIP. Et usurper une identité, téléphoner gratuitement à sa copine aux US, ou même revendre les communications.

Le phénomène semble d'ailleurs s'accentuer, Claire Chazal au 13h de TF1 s'en est même fait l'écho le 20 novembre 2011, c'est dire ! Il devient donc nécessaire de se poser quelques bonnes questions : quels sont les risques liés à une indisponibilité de mon infra-structure voix et combien cela peut-il coûter à mon entreprise ?

Toutefois si il est déjà trop tard, et comme le conseille d'ailleurs le très complet site http://sos-piratage.com : dans les départements 75, 92, 93, 94 ce sont les commissariats qui sont compétents pour recevoir les plaintes relatives aux détournements de trafic téléphonique entre autres. Ces dernières sont ensuite transmises pour instruction à la Brigade d'Enquête sur les Fraudes aux Technologies de l'Information (BEFTI), une unité spécialisée de Police judiciaire de la Préfecture de Police. Dans les autres départements métropolitains, il faut entrer en contact avec le SRPJ (Service Régional de Police Judiciaire). Des agents spécialisés possédant le statut d'ESCI («Enquêteur Spécialisé sur la Criminalité Informatique «) enregistrent la plainte.

Ce Handbook se propose donc de vous éclairer. Alexandra Thomas (Cogis Networks), en chef de projet, accompagnée de Bruno Husson (Aastra France) et Guy Tétu (Ficome) dressent un panorama du piratage téléphonique et de ses remèdes.

Jean-Denis Garo

Directeur Communication
et Marketing Support Aastra
Twitter : @JeanDenisG

Piratage téléphonique : des solutions simples et efficaces existent pour toutes les entreprises

Le Piratage en question

Les enjeux liés à la téléphonie ne sont pas toujours bien identifiés. Ils sont à la fois techniques, organisationnels et fonctionnels.

Au niveau **technique**, il s'agit principalement de la disponibilité et de la fiabilité du service, de la sécurité et de la qualité de service. En effet, le téléphone reste avant tout le meilleur moyen pour joindre quelqu'un.

Au niveau **organisationnel**, avec l'arrivée de la téléphonie IP (ToIP), le poste de responsable informatique a évolué : il fournit non seulement des services informatiques mais aussi télécoms.

Enfin, au niveau **fonctionnel**, il s'agit de déterminer de quelle manière le poste de travail doit être pensé pour permettre aux collaborateurs de travailler efficacement tout en prévenant les risques de piratage.

Définition

Le piratage téléphonique, communément appelé « phreaking », est l'exploitation des infrastructures téléphoniques dans un but malveillant. Le mot se compose des termes «phone» et «freak», qui se traduisent respectivement «téléphone» et «anomalie». Le « phreaking » est né dans les années 60 aux Etats-Unis.

A l'époque, les « phreakers » se contentaient de pénétrer dans les systèmes téléphoniques afin de téléphoner gratuitement pour leur propre compte. Le phénomène restait donc limité.

Aujourd'hui, la multiplication des opérateurs dans le monde et l'augmentation du taux d'équipements en téléphones a créé un nouveau marché pour les pirates : détourner des communications pour les revendre (marché de la terminaison d'appels). A la différence du « phreaker » traditionnel, l'appelant et l'appelé qui utilisent le trafic détourné ne savent souvent pas qu'ils utilisent une ressource piratée.

Par ailleurs, la multiplication de services (jeux, paris, voyance, etc.) proposés via un numéro de téléphone à appeler dont le titulaire encaisse un revenu à chaque appel (numéros surtaxés ou à revenus partagés) incitent l'appelant comme le propriétaire du numéro surtaxé à pirate des communications soit pour accéder au service (joueur, parieur, etc.) soit pour encaisser le revenu généré par chaque appel (titulaire du numéro surtaxé).

Très rémunérateur, international, ce « marché » est donc vraisemblablement appelé à se développer.

D'autres attaques consistent à inonder et saturer les équipements pour les rendre inopérants, au détriment de l'entreprise, ou encore à récupérer des informations confidentielles dans les bases de données de ces systèmes ou par écoute des conversations téléphoniques.

Qui est concerné ?

Toutes les entreprises, des grands comptes aux TPE/PME, sont confrontées au risque de piratage téléphonique. Statistiquement, s'il est vrai que certains PABX et IPBX sont moins touchés que d'autres, le risque n'en demeure pas moins universel et permanent.

Le risque est d'autant plus avéré et les probabilités qu'il se réalise sont d'autant plus importantes que La conjonction de l'existence d'un marché très rémunérateur et de l'accès facile aux méthodes et outils de piratage fait déjà sentir ses conséquences : depuis quelques années, ce sont les TPE/PME, mal équipées et peu informées pour faire face, qui subissent une augmentation exponentielle de ces attaques entraînant des surfacturations téléphoniques parfois très importantes (par exemple plusieurs dizaines de milliers d'euros en un week-end), mettant en péril leur pérennité

Contexte

Souvent, pour les entreprises, la problématique de sécurité du système téléphonique n'est pas une préoccupation majeure, et la téléphonie n'est pas toujours bien intégrée dans la politique de sécurité du système d'information (« ah bon, un téléphone ça se pirate ? »). En effet, dans la plupart des cas, ces dernières ne prennent pas directement en compte la téléphonie, ou les moyens de communication voix.

En outre, les équipes responsables de la téléphonie (qu'il s'agisse des Services Généraux ou d'une équipe dédiée) ne sont pas toujours suffisamment sensibilisées à la sécurité

Par ailleurs, avec l'arrivée de la téléphonie IP, et son ouverture sur les réseaux, les spécialistes en charge de la sécurité dans les entreprises, doivent être formés pour monter en compétences et mieux appréhender les problématiques spécifiques à la téléphonie.

Piratage téléphonique : des solutions simples et efficaces existent pour toutes les entreprises

En ce qui concerne les équipements, les systèmes de téléphonie ont bien changé depuis leur création.

Autrefois, les PABX étaient des équipements fermés et difficilement appréhendables, avec des vulnérabilités spécifiques, connues des seuls experts et des pirates. Aujourd'hui, avec la VoIP, les PABX et IPBX sont aussi de véritables systèmes informatiques sur lesquels on trouve une application télécom, et connectés au réseau IP de l'entreprise, partagés avec d'autres applications, et potentiellement ouvert sur l'extérieur (Internet). Ils cumulent donc une double problématique de sécurité : la vulnérabilité de tout serveur informatique à laquelle vient s'ajouter la vulnérabilité de la téléphonie traditionnelle.

Nous pouvons donc dire que la vulnérabilité des équipements est aujourd'hui bien réelle et grandissante. Pour y remédier de manière efficace, la sécurité de la téléphonie doit s'inscrire dans le cadre de la politique de sécurité globale de l'entreprise.

Constats

- **Constat n° 1** : Les entreprises, quelle que soit leur taille, subissent régulièrement ces attaques entraînant des surfacturations téléphoniques importantes.
- **Constat n° 2** : Les systèmes téléphoniques (traditionnels aussi bien que VoIP) ne sont pas toujours dotés d'outils efficaces pour se protéger contre ces attaques.
- **Constat n° 3** : Les entreprises victimes d'attaques sont désarmées faute d'avoir identifié la menace, d'informations techniques sur la nature de l'attaque et le mode opératoire utilisé, et faute d'outils pour stopper rapidement l'attaque et s'en protéger.
- **Constat n° 4** : Les conséquences de ces attaques sont considérables :
  - Des préjudices financiers parfois extrêmement importants.
  - Une limitation des fonctionnalités du téléphone, qui peut engendrer une perturbation de l'activité de l'entreprise.
  - La création d'une situation de crise entrainant une forte mobilisation de ressources humaines et de la perte de temps.

Typologie des principales attaques

Nous avons relevé cinq principaux types d'attaques :

1/ Fraude téléphonique

Cette pratique consiste à téléphoner gratuitement en détournant puis reconfigurant le PABX ou l'IPBX, et pouvoir ainsi émettre des appels au nom de la société qui a été attaquée :

- Détournement de trafic et revente de communications.
- Renvois vers des numéros surtaxés et génération automatique de nombreux appels courts vers ces numéros.

La technique la plus répandue consiste à contacter la messagerie vocale de l'entreprise, entrer sur un compte de messagerie (par exemple en essayant les mots de passe par défaut) et configurer sur ce compte un renvoi vers un numéro extérieur, bien souvent situé à l'étranger. Il ne reste plus qu'à appeler cet utilisateur en entreprise pour voir son appel renvoyé vers l'extérieur au frais de l'entreprise piratée.

Certes, l'opérateur dispose en général de moyens de détection des comportements atypiques, mais les pirates agissent plutôt le week-end ou en période de congés, période pendant laquelle l'opérateur ne peut pas toujours réussir à joindre et alerter l'entreprise. Et le trafic détourné reste de toute façon facturé.

Impact : surfacturation téléphonique importante, temps perdu à rechercher la source du problème.

2/ Déni de service

Cette technique vise à rendre indisponible le service de téléphonie.

- Saturation de la capacité des liens opérateurs engendrant l'impossibilité de passer ou de recevoir des appels.
- Mise hors service du service de téléphonie au moyen d'attaques protocolaires.
- Augmentation du temps de réponse des équipements de téléphonie : atteinte à la qualité de service - QoS.

Impacts : indisponibilité du service de téléphonie, plainte de clients ou de tiers, atteinte à la notoriété, perte de chiffre d'affaires.

3/ Intrusions sur le système d'information

Ce sont des manœuvres visant à pénétrer sur le système informatique à partir du système téléphonique. Elles se traduisent principalement par l'envoi de codes trompeurs via Internet, qui brisent les barrières de sécurité, et les mots de passe des autocommutateurs et des postes téléphoniques.
Ils peuvent ralentir l'usage du réseau, polluer le bon fonctionnement des applications, et capter, modifier ou détruire de l'information :

- Depuis l'extérieur : piratage des modems de télémaintenance, ou des modems internes (Wardialing, puis pénétration du réseau)
- Depuis l'intérieur: utilisation des lignes analogiques (des fax, par exemple) pour établir des connexions pirates vers Internet dans le but d'outrepasser la politique de sécurité Internet (filtrage Web).
- Modems « fantômes » ou modems « oubliés », programmes « Dialers ».

Typologie des principales attaques

Impacts : création de porte dérobée (Backdoor), interconnexion clandestine d'Internet avec le réseau d'entreprise (porte d'entrée pour les pirates, virus, malwares, chevaux de Troie, etc…), fuites, détournement d'informations…

4/ Usurpation d'identité

Les différentes fonctions de l'autocommutateur peuvent permettre de se présenter sur le réseau téléphonique avec une fausse identité permettant ainsi à un pirate de nuire à un tiers sous l'identité de l'entreprise piratée.

Impacts : risques d'ordres financiers, sur l'image de la société, risques civils et pénaux pour le dirigeant de la société (détails ci-après)

5/ Espionnage

Il s'agit de la surveillance des communications et du vol d'informations :

- Ecoute illégale et enregistrement des conversations.
- Piégeage des postes en vue de les utiliser comme des microphones distants.
- Ecoute des messages sur les boîtes vocales à mots de passe faibles.
- Fuites d'informations sensibles et stratégiques pour l'entreprise.

Impacts : identification des contacts (clients, partenaires, fournisseurs, …), vols de brevets et de technologies, stratégies d'entreprise divulguées, divulgation publique d'informations confidentielles, atteinte au respect de la vie privée.

A noter :
Le cas des Softphones : il n'est pas facile de cloisonner les réseaux voix et données sur les postes équipés de Softphones, ce qui entraîne une perméabilité entre les réseaux, mais aussi la possibilité de lancer des attaques sur le réseau Voix depuis un poste de travail doté d'un Softphone, ou encore la propagation de programmes malveillants entre les réseaux.

Ce que dit la loi

Les autocommutateurs manipulent une correspondance entre des numéros de téléphone et des postes téléphoniques associés à des personnes. De ce fait, il s'agit d'un système effectuant un traitement automatisé de données nominatives ce qui, conformément à la loi n° 78-17 du 6 janvier 1978 dite « Loi informatique et libertés », nécessite une déclaration auprès de la CNIL.

La loi du 5 janvier 88 punit l'intrusion et le maintien volontaire dans un système (Nouveau Code Pénal, art. 323-1, al. 1er), comme l'altération de son fonctionnement (Nouveau Code Pénal, art. 323-2).

Si les peines sont sévères pour les pirates (prison et amende), il n'en demeure pas moins qu'il est très difficile d'obtenir des condamnations, la plupart des attaques provenant de l'étranger.

Ce que dit la loi

Dés lors, face à cette difficulté, l'entreprise doit compter plus sur les précautions qu'elle doit elle-même mettre en œuvre que sur la réponse pénale.

Ces précautions doivent être prises dés la rédaction des contrats signés avec l'ensemble des acteurs intervenant sur le système télécoms, et dans la souscription d'un contrat d'assurance couvrant le risque de fraude.

Si l'entreprise piratée est en premier lieu la victime, il lui est possible de se retourner contre des tiers : opérateur, installateur, éditeur ou constructeur, et tenter de démontrer qu'ils sont en faute. Aussi, les limites de responsabilité de chaque acteur doivent être le plus précisément possible définies dans les contrats et autres documents officiels.

Face à ce type de risque avéré, l'entreprise doit également s'assurer pour les dommages couvrant les pertes directes et certaines pertes indirectes (intérêts débiteurs et créditeurs, pénalités contractuelles, frais de reconstitution d'informations, frais supplémentaires d'exploitation, frais de procédure, etc.) subies suite à des fraudes (détournements de leurs fonds, biens ou marchandises leur appartenant) ou à des malveillances informatiques, quels que soient leurs auteurs.

Les moyens pour se protéger

La téléphonie doit faire partie de la politique de sécurité du système d'information de l'entreprise. Le dirigeant d'entreprise doit donc disposer d'une politique de sécurité « voix » et l'appliquer.
Il existe des solutions faciles à mettre en place pour sécuriser l'architecture téléphonique et les autocommutateurs. Nous les avons synthétisés en 10 points clés:

1/ Contrôler l'administration et l'utilisation des équipements télécoms

- En attribuant des droits avec des niveaux d'accès différents en fonction du niveau d'habilitation du ou des administrateurs. Ainsi qu'en restreignant les droits à l'utilisation de certaines fonctions sensible, par exemple en interdisant ou limitant l'utilisation des transferts et renvois vers l'extérieur (aboutement réseau), aussi bien pour les postes que pour la messagerie vocale.
- En définissant et appliquant une politique et des processus de gestion des mots de passe. Dès l'installation d'un nouvel équipement, il est conseillé de réinitialiser les mots de passe par défaut, y compris les mots de passe constructeur. Il est aussi recommandé de modifier régulièrement les mots de passe, d'éviter les mots de passe trop simples.
- De plus, il est important de tracer les événements, afin de pouvoir détecter les intrusions et retrouver l'historique. Ainsi, chaque accès (y compris les connexions distantes, pour la télémaintenance par exemple) et chaque action effectuée doivent être consignés dans des journaux de bord.

Les moyens pour se protéger

2/ Sélectionner des partenaires de confiance

pouvant aider l'entreprise dans sa démarche de sécurisation de l'infrastructure téléphonique (habilitation des sociétés et certification des produits). Il est en outre conseillé que le partenaire dispose de connaissances sur les vulnérabilités et les menaces encourues par les équipements télécoms, afin d'appréhender les risques et leurs impacts, et donc de bien conseiller l'entreprise dans sa prise de décision.

3/ Sensibiliser le personnel de l'entreprise.

En effet, responsabiliser les administrateurs et les utilisateurs sont deux facteurs clés pour mener à bien une politique de sécurité globale dans l'entreprise. L'installateur ou l'exploitant peuvent ainsi informer l'entreprise des risques encourus, notamment liés à la configuration du système ; par exemple, sensibiliser l'entreprise si les renvois vers l'extérieur sont autorisés par configuration, ou si des mots de passe par défaut sont laissés inchangés sur le système installé.
En matière de sensibilisation à la sécurité, il faut également se méfier des nouveaux usages liés aux réseaux sociaux. En effet, la socialisation du web tend à pousser chacun à diffuser à la communauté ses expériences, y compris les architectures et projets mis en place. Or, diffuser des informations quant à son architecture télécom peut donner à d'éventuels pirates des informations leur permettant d'orienter leurs recherches, et donc d'augmenter le risque d'intrusion pour l'entreprise.

4/ Sécuriser le local abritant l'IPBX et les serveurs

5/ Sécuriser les systèmes :

- Sécuriser les réseaux de l'entreprise :
  - En les cloisonnant : mise en place de pare-feu ou ALG (Application Layer Gateway) adapté, VPN (Virtual Private Network) ou NAT (Translation d'adresse) pour commu-niquer avec l'extérieur, éventuellement mise en place d'une DMZ pour les serveurs, etc.
  - En séparant les flux téléphonie des flux data, par l'utilisation de VLAN
  - En mettant en oeuvre les bonnes pratiques de configuration des switchs : Filtrage des adresses mac, fiiltrage des offres DHCP, éventuellement authentification des équipements (802.1X), etc.
- Sécuriser les systèmes d'exploitation et les applications télécom :
  - En n'installant que les packages nécessaires dans le système d'exploitation
  - En installant régulièrement les patchs de sécurité, afin de s'assurer de posséder tous les correctifs de sécurité,
  - En arrêtant tous les services inutiles sur l'OS
  - En mettant en œuvre des anti-virus
- Sécuriser l'accès aux terminaux et au service, par des fonctions de login, verrouillage, authentification (tel SIP Digest)
- Eventuellement, sécuriser les communications elles-mêmes, par du chiffrement de la voix et de la signalisation

6/ Installer une solution d'analyse et d'observation du trafic

et de contrôle de la facturation, plus vulgairement connue sous le terme de « solution de taxation ». Elle va permettre d'analyser précisément et régulièrement le trafic téléphonique pour déterminer si des consommations sont anormales. Elle permet en outre de garder une traçabilité des évènements, et fonctionne généralement dans des environnements multi-sites et hétérogènes (PABX ou IPBX de constructeurs différents) :

- Postes
- Détection de modems « pirates »
- Date et heure des appels
- Numéros composés / numéros appelants

- Durée de conversation
- Destination des appels
- Coûts
- Nombre de communications
- Analyse de la charge sur les différents liens inter-sites
- Etc

Certains logiciels d'analyse du trafic sont plus complets que d'autres : ils offrent la possibilité de remonter des alarmes dès que certains seuils sont dépassés, ou de couper les lignes sur lesquelles un crédit préalablement affecté vient à s'épuiser. Ils permettent également d'archiver régulièrement les configurations des IPBX, et de journaliser automatiquement les actions menées par les utilisateurs des outils de sécurisation (nom, adresse IP, date de l'action, nature de l'action).

7/ Protéger le réseau téléphonique en mettant en place des moyens d'analyse de trafic (VoIP : interne/externe, et ISDN : T0/T2/E1), en utilisant des IDS/IPS spécialisés Voix permettant la détection d'anomalies et la protection contre les intrusions, en surveillant le réseau Voix, en temps réel, et en émettant des alertes de sécurité lors de détection d'anomalies.

8/ Mettre en place une architecture résiliente permettant de garantir la haute disponibilité du service de téléphonie, par exemple la redondance des serveurs de téléphonie ainsi que des fonctions d'autonomie des sites et des accès opérateurs assurant la continuité du service en cas de panne des systèmes centraux.

9/ Effectuer régulièrement des audits des configurations des autocommutateurs (manuellement ou à l'aide d'outils automatiques spécialisés). En complément, il est recommandé de disposer de moyens de contrôle et de détection des modifications de configuration afin d'être alerté si des modifications de configuration mettant en péril la sécurité du système téléphonique surviennent (erreurs de manipulation, ou modifications malveillantes).

Dans tous les cas, il convient de se tourner vers des professionnels des télécoms (constructeurs, intégrateurs téléphoniques et éditeurs de logiciels adaptés). Ces derniers peuvent vous conseiller sur la meilleure manière de protéger votre installation téléphonique.

Grandes entreprises / PME : avantages et inconvénients

Les **grandes entreprises et grands groupes** disposent généralement de moyens financiers et de ressources humaines dédiées et formées à la gestion de l'informatique et de la téléphonie de l'entreprise. Il leur est donc normalement facile de mettre en place une politique de sécurité. Seul bémol : l'efficacité de cette dernière est souvent altérée par les comportements à risques des employés. Et plus l'effectif de l'entreprise est important, plus le plan de sensibilisation des employés est difficile à mettre en place et à aboutir.

Les moyens pour se protéger

Les **TPE et PME** quant à elles, disposent d'un effectif plus modeste qui leur permet de sensibiliser plus rapidement et efficacement leur personnel aux problèmes de sécurité.

En revanche, la personne en charge de l'informatique et de la téléphonie cumule souvent cette fonction avec d'autres fonctions, son attention est plus souvent focalisée sur l'exécution des ses taches quotidiennes plutôt que sur la politique de sécurité de l'entreprise, et ses connaissances en matière de sécurité des systèmes d'information sont souvent limitées. Résultat : le système de téléphonie de l'entreprise n'est pas ou mal sécurisé, et encore trop peu de TPE/PME font appel à des prestataires extérieurs spécialisés.

Dans tous les cas, la **volonté du ou des dirigeants** de se prémunir contre des attaques de leur système de téléphonie sera prépondérante aux avantages et aux inconvénients liés à la taille de l'entreprise et à l'affectation des moyens dont elle dispose.

Conclusion

La disponibilité de la téléphonie est un impératif, tout comme son intégrité, sa confidentialité et son imputabilité (authentification et traçabilité des opérations).

Le maintien du service de téléphonie en condition opérationnelle est un facteur fondamental pour les entreprises, mais à l'heure actuelle, trop peu d'entre elles ont fait le pas pour se prémunir contre les risques de piratage.

Peut-être parce qu'il s'agit justement (seulement ?) de risque.

Désormais, les risques associés à la téléphonie peuvent avoir des conséquences sur le système d'information de l'entreprise.

Il convient donc d'apporter des réponses pertinentes en matière de sécurité aux nouvelles menaces qui pèsent sur la téléphonie et qui sont liées à l'évolution des technologies et des usages.

Or, comme nous l'avons vu, des solutions simples et efficaces existent déjà pour lutter contre ces attaques.

Mais trop souvent, les chefs d'entreprise ne se décident à investir dans une solution de sécurité qu'après avoir subi une attaque majeure, ayant occasionné de graves dégâts pour leur entreprise. N'hésitons donc pas à continuer à les sensibiliser sur le sujet.

A propos d'Aastra

Situé à Concord (Ontario, Canada), Aastra (TSX : AAH) est un groupe international, acteur majeur du marché des communications d'entreprises. La société développe et commercialise des solutions ouvertes de téléphonie sur IP, de communications unifiées et de travail collaboratif, destinées tant aux PME qu'aux grandes entreprises.

Aastra compte 50 millions d'utilisateurs dans le monde et dispose d'une présence directe et indirecte dans plus de 100 pays.
Aastra permet aux entreprises de communiquer et de collaborer plus efficacement en proposant à ses clients une gamme complète de solutions de communications - terminaux, systèmes et applications - basées sur les standards du marché tels que SIP, LDAP, XML, etc.

www.aastra.fr

@Aastra_France

Aastra Handbooks

Aastra édite tout au long de l'année des Handbooks.

Certains présentent les résultats de sondages/enquêtes effectués auprès d'utilisateurs et traitant de sujets tels que :

- La Collaboration Vidéo sur IP
- Les Communications collaboratives unifiées
- Etes-vous un collaborateur 2.0 ?
- Nouveaux usages, nouveaux médias

D'autres sont des livres blancs abordant des sujets d'actualités comme :

- XML et SIP, ou comment enrichir fonctionnellement le terminal SIP
- Les obligations légales pour les personnes offrant un accès à l'Internet au public
- Comment optimiser les relations entre Consultants, Intégrateurs (S.S.T.R.) et Equipementiers ?
- Les outils du marketing :
  du bon usage du mailing, de l'e-mailing… aux réseaux sociaux.

Site de téléchargements :
www.support.aastra.fr/handbooks

A propos de Cogis Networks

La société COGIS développe des solutions logicielles pour les télécoms depuis près de 25 ans et met son savoir-faire au service des PME/PMI, Grands Comptes, et Collectivités dans tous les domaines d'activité: Industrie, Services, Santé.

La solution VISUAL TAXE PRO, plus communément appelée VTPRO, est un logiciel d'analyse du trafic téléphonique et de contrôle de la facturation qui permet d'analyser précisément et régulièrement les communications téléphoniques. VTPRO permet aux PME/PMI et aux Grands Comptes de lutter efficacement contre le phreaking en déterminant si des consommations sont anormales.

Conscient des risques grandissants encourus par tout établissement face à la problématique de piratage téléphonique, COGIS a doté sa solution VTPRO d'une option de lutte contre le phreaking, qui intervient a un triple niveau :

D'une part, en cas de dépassement de seuils prédéfinis, VTPRO envoie immédiatement une alerte.

D'autre part, sur certains PBX, VTPRO coupe automatiquement les lignes sur lesquelles un crédit préalablement affecté vient à s'épuiser.

Enfin, VTPRO garde la traçabilité des évènements et journalise les actions menées par les utilisateurs.

Les avantages de VTPRO :

- Multi-plateformes : compatible Windows et Linux.
- 100% web : installation, paramétrage et exploitation à partir d'un simple navigateur internet.
- Fonctionnement sous les environnements hétérogènes et multi-sites.
- Gestion jusqu'à 50 000 postes.
- Virtualisable.

Les autres solutions COGIS :

- Liaison : standard téléphonique à reconnaissance naturelle de la parole.
- Tim Tam Tom : borne interactive d'information, d'accueil et d'orientation.
- Medialert : automate de gestion d'alerte, de diffusion d'informations et de relance de rdv (appels vocaux, sms, e-mail et fax)

Cogis, your telecoms@work !

Plus d'infos :
13 avenue Charles de Gaulle
94470 Boissy Saint Léger
Tel : 01 45 10 31 00
E-mail : commercial@cogis.com
www.cogis.com
@COGISNETWORKS

A propos de la Ficome

Fédération Interprofessionnelle de la Communication d'Entreprise

Née en novembre 1946*, la Fédération Interprofessionnelle de la Communication d'Entreprise est le syndicat professionnel des sociétés de services Télécoms et réseaux qui installent, intègrent et maintiennent les systèmes de communications électroniques destinés aux utilisateurs professionnels en France.
Elle a pour rôle de promouvoir l'équipement et l'usage des systèmes de communications dans les entreprises et de valoriser l'image de ses membres et de la profession au niveau national en favorisant l'innovation, l'emploi et la qualité du service rendu aux clients.

Elle propose à ses membres un dialogue constant et structuré avec l'ensemble de l'écosystème Télécoms en les réunissant lors d'événements et groupes de travail dédiés, pour échanger entre experts points de vue et retours d'expériences sur les produits, solutions et services, qui donnent lieu à la diffusion de livrables.

Les sociétés de services adhérentes bénéficient en outre d'un ensemble de prestations spécifiquement développés à leur attention (actions collectives, assistance juridique, assurance professionnelle, règles et usages de la profession, etc.).
Ses actions concernent les questions d'intérêt commun et sont réalisées dans respect des règles de concurrence entre les membres.

La Fédération est structurée autour de 3 collèges : Sociétés de Services Télécoms et Réseaux, membres associés - réunissant équipementiers, opérateurs et éditeurs IT - et bureaux d'études et sociétés de conseil.

La FICOME s'implique dans une démarche de promotion de la qualité des prestations délivrées par la profession à ses clients, par la gestion du fichier FINISTEL (Fichier National d'identification des installateurs-intégrateurs de solutions de télécommunication), au travers de la charte FICOME qui engage ses adhérents, et en étant un partenaire actif dans la gestion de la certification de services QUALIFCOM.

http://www.ficome.fr
http://www.qualifcom.fr

FICOME
69, rue Ampère 75017 PARIS
Tél. : 33 (0) 1 56 43 62 00
Fax : 33 (0) 1 45 62 02 22
www.ficome.fr
@ficome

CODE APE 9411Z - Numéro d'immatriculation 9220
Siret 784243479 00077 - N° TVA FR 08784243479

Membre fondateur de l'ETSA - European Telecommunication Services Association

(*) Sous le nom de Syndicat National des Installateurs du Téléphone

Piratage téléphonique : Comment lutter contre la malveillance ?

Des solutions simples et efficaces existent pour toutes les entreprises.

Ce Handbook traite du piratage téléphonique, de la typologie des principales attaques, de ce que dit la loi sur le sujet et des moyens pour se protéger.

Alexandra Thomas (Cogis Networks), en chef de projet, accompagnée de Bruno Husson (Aastra France) et Guy Tétu (Ficome) dressent ici un panorama du piratage téléphonique et de ses remèdes.

cogis networks
www.cogis.com

FICOME
www.ficome.fr

AASTRA
www.aastra.fr

Papier recyclé
Recycled paper
02-12