1) Qui sont les pirates ?

2) Les principales attaques

3) Les conséquences du piratage

4) Comment se protéger ?

5) Les règles de bonne conduite

6) Comment faire en cas de piratage ?

1) Qui sont les pirates ?

Les pirates sont particulièrement compétents et très organisés. Une simple connexion Internet leur suffit. Ils semblent venir majoritairement d'Europe de l'Est et d'Asie mais, à ce jour, personne n'a encore réussi à les localiser.

L'action des pirates consiste à s'introduire frauduleusement dans les installations téléphoniques des entreprises afin de s'en servir de passerelle pour émettre des appels internationaux. Ces appels sont ensuite détournés et revendus à des opérateurs Télécoms (peu scrupuleux) du monde entier qui les achètent à des tarifs particulièrement attractifs.

Comment les pirates Télécoms s'enrichissent-ils ?

Il existe plus de 5000 opérateurs Télécoms dans le monde. Les opérateurs Télécoms achètent et revendent à leurs clients des appels téléphoniques vers toutes les destinations nationales et internationales. Les opérateurs transitent des milliards de minutes chaque année. Les opérateurs achètent selon des tables de routages particulièrement pointues, permettant de transiter les appels de leurs clients au meilleur coût.

Il existe des centaines de sociétés spécialisées dans le revente de tarifs Télécoms. Ces sociétés sont surnommées des Carriers. Les plus importants carriers exploitent des liaisons dédiées entre les pays, tel que les liaisons transatlantiques. D'autres, plus petits, se contentent de faire du troc de minutes. Ceux-ci sont les clients privilégiés des pirates Télécoms.

Les pirates détournent les appels des installations téléphoniques de plusieurs centaines d'entreprises pour revendre le trafic Télécom à des carriers.

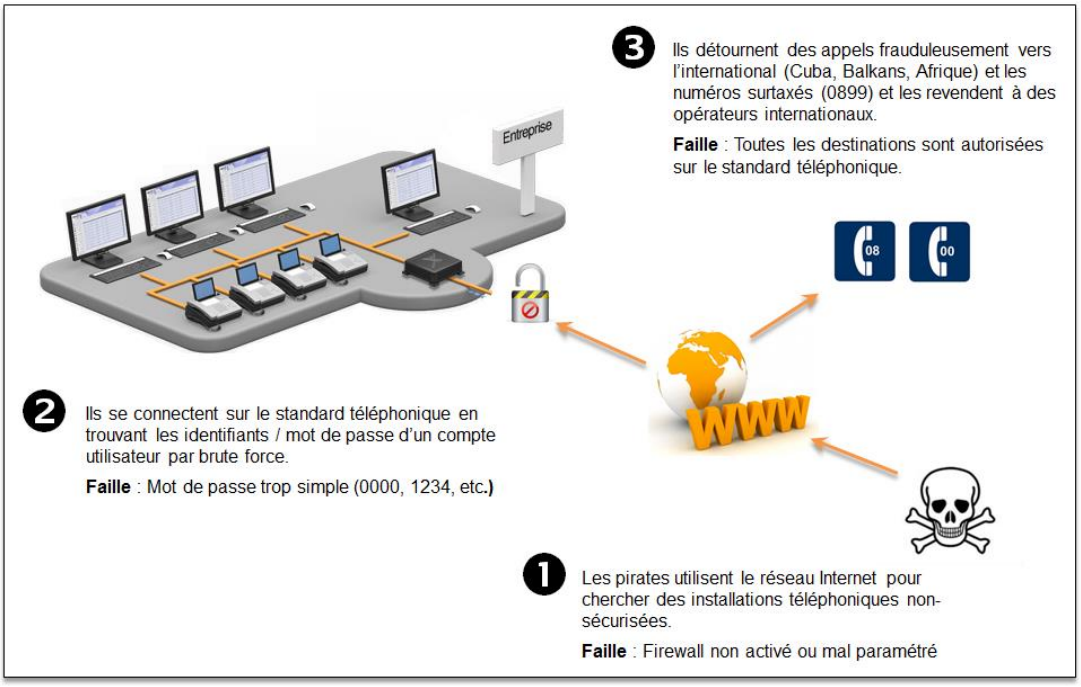
Les carriers les revendent ainsi aux opérateurs qui les revendent à leurs clients.

2) Les principales attaques

Il existe trois failles majeures utilisées par les pirates Télécoms **:**

A- Le piratage sur réseau IP

La nouvelle génération de standards téléphoniques (Téléphonie IP) est totalement intégrée au réseau informatique de l'entreprise. Cependant, un pare-feu informatique (Firewall) mal configuré, ne protège pas le standard téléphonique. Les pirates peuvent ainsi s'introduire sur le réseau téléphonique de l'entreprise et utiliser l'installation comme passerelle d'appels vers l'international.



B- Le piratage des messageries vocales

La plupart du temps, les utilisateurs en sein des entreprises ne personnalisent pas le code d'accès de leurs messageries vocales. Certains standards téléphoniques donnent ensuite la possibilité d'émettre des appels. Cette faille est utilisée par les pirates pour transformer le téléphone de l'utilisateur en passerelle pour émettre vers des numéros surtaxés, des numéros de serveurs de jeux ou des numéros de recharge de compte (type Paypal).

1- Programmation de renvoi par l'utilisateur

- Sur la messagerie vocale
- Sur le Serveur Vocal Interactif
- Sur un poste (programmation à distance de ses renvois, follow-me)
- Sur un accès utilisateur distant = DISA

- Se faire passer pour l'utilisateur

- Mot de passe simple (0000, 1111, 1234, etc.) ou mot de passe par défaut du constructeur: parfois trouvé sur le web, ou les documentations techniques produit

2- Autres méthodes avec complicité interne

- Transfert d'appel vers l'extérieur
- Conférences avec participants externes
- … mais peu utilisé : risque de licenciement pour faute grave, etc

Exemple de méthodologie des pirates :

- **La faille par les messageries vocales**

- Permettant d'être renvoyé avant ou après dépôt de message
- Permettant une configuration à distance

- **Procédure des pirates**

- Appeler des n° d'une entreprise

- Si on tombe sur celui de la messagerie vocale, navigation dans les menus (consultation, configuration), saisie du mot de passe, configuration du n° de renvoi

- Appel vers l'utilisateur, renvoyé vers messagerie, qui, elle–même, renvoie vers un destinataire… lointain!

- Pour ne pas être repéré tout de suite, désactiver le renvoi après usage

C- Le piratage de l'interface Administrateur

Votre standard téléphonique possède une interface d'administration qui peut être piratée si les identifiants ne sont pas personnalisés de manière complexe. Les risques sont les suivants:

- Autorisation des renvois vers l'extérieur
- Programmation des renvois

- Utilisateur
- Messagerie
- SVI

- Gestion des mots de passe (reset)
- Gestion des journaux de trace

Exemple de méthodologie des pirates :

1- Accès à l'administration d'un PABX

- Trouver l'adresse IP
- Suivre la documentation d'administration
- Tenter les mots de passe constructeur par défaut

2- Modification de la configuration

- Configurer les renvois

3- Après utilisation

- Restaurer la configuration
- Supprimer les journaux de traces

4- Prévoir la suite

- Explorer la configuration
- Eventuellement ouvrir d'autres accès à l'administration

3) Les conséquences du piratage

Les entreprises subissent des conséquences financières énormes. Plusieurs piratages sont recensés chaque jour en France et plusieurs dizaines de millions d'euros piratés chaque année.

Le piratage Télécom représente des fraudes de plusieurs dizaines de milliers d'euros à plusieurs centaines de milliers d'euros chacune. Le cas recensé le plus important en France est de 600,000 euros.

La plupart du temps, le piratage a lieu durant des périodes ou l'entreprise est fermée, notamment durant les weekends, les fêtes, les jours fériés. L'entreprise piratée ne peut donc pas être prévenue immédiatement, puisqu'elle est fermée. Il suffit de quelques heures de piratage pour subir des préjudices de plusieurs dizaines de milliers d'euros.

On peut citer par exemple le cas d'une PME francilienne, fermée entre Noël et le jour de l'an. Des pirates ont très facilement pénétré le système d'information, en utilisant la messagerie. Bilan : 70,000 euros perdus.

Les principales destinations piratées à ce jour sont les suivantes: Taiwan, Somalie, Cuba, Iles Caimans, Estonie, Corée du Nord, Azerbaibjan, Slovénie, Afganistan, Global Satellite, Globastar, Egypte, Nigeria, Togo, Sri Lanka, Benin, Ethiopie.

Les différents types de menaces

Au-delà de la fraude financière, le piratage Télécoms rend totalement vulnérable votre entreprise. Vous trouverez ci-dessous un récapitulatif des risques encourus.

La Fraude
- Usurpation d'identité
- Téléphoner en imputant la taxe à un autre
- Aboutements d'appels vers des numéros surtaxés
- Falsification de la taxation
- Utilisation abusive des ressources

La Rupture de confidentialité
- Interception et enregistrement des conversations
- Ecoute téléphonique
- Ecoute des boites vocales

La Rupture d'intégrité
- Intrusion sur le système téléphonique
- Attaques virales du système (virus, vers, chevaux de Troie …)
- Destruction ou altération des données
- Altération de fichiers (annuaire, boites vocales)
- V-Bombing, spam sur les messageries vocales
- Recomposition des messages vocaux
- Modification des données de programmation
- Déni de service (DOS)
- Dégradation physique des équipements

4) Comment se protéger ?

Les pirates sont très habiles pour profiter des failles techniques de votre infrastructure Internet & Télécoms. La plupart des pirates informatiques sont motivés par le challenge technique et la fierté qui auront à s'introduire sur une infrastructure particulièrement bien protégée. Les pirates Télécoms sont avant tout motivées par les gains financiers.

L'objectif de notre lutte contre le piratage est de faire en sorte que les gains financiers des pirates soient réduits. Si leur action est trop complexe et surtout non-productive, les pirates se démotiveront rapidement. Afin de se protéger contre le piratage, nous préconisons les différentes actions suivantes :

- Les entreprises doivent **restreindre leur capacité d'appels aux seules destinations nécessaires à leur activité**. Inutile d'autoriser les appels vers l'Afrique, les Balkans ou les 0899, si votre entreprise n'appelle jamais ces destinations.
- Les entreprises doivent se rapprocher de la société qui gère leur installation téléphonique pour **s'assurer de la sécurité mise en place contre le piratage**. Les entreprises peuvent notamment demander un audit de sécurité à la société qui gère leur installation téléphonique.
- Les entreprises doivent **désactiver les fonctionnalités représentant des menaces** en cas de mauvaise utilisation par leurs employés.
- Les entreprises doivent demander à leur opérateur en Télécommunications de **fixer des plafonds de consommations** mensuels.
- Les entreprises doivent s'assurer que **leur police d'assurance les couvre contre le piratage Télécom**

Sécurisation technique des flux de téléphonie sur IP

La sécurisation des flux de téléphonie sur IP s'effectue à travers un schéma conceptuel de sécurité qui comprend les dispositifs suivants :

- Cloisonnement par VLAN
- Protection par firewall
- Authentification forte
- IP VPN privé avec l'opérateur
- Attention aux configurations par défaut
- Supervision en temps réel du système
- Mise à jour de sécurité des équipements

a- Cloisonnement des flux IP de téléphonie par VLAN

L'ensemble des composants du système qui sont connectés au réseau IP constituant l'infrastructure du réseau ont la capacité de constitution de VLAN garantissant l'étanchéité des flux.Le système interdit tout appel en provenance d'un équipement ne faisant pas partie du VLAN dédié à la téléphonie lors de l'installation.

Il est possible de permettre au VLAN data de dialoguer avec le VLAN voix mais ceux-ci doit être explicités minutieusement (IP, port, protocole). L'administrateur de réseau du site dispose de la faculté de reconfigurer l'un ou l'autre de ces VLAN pendant la durée de vie du système.

b- Pare-feu spécifique

Il existe deux types de firewall (Stateless, Statefull) ; l'un étant uniquement basé sur des notions d'IP, de ports et de protocole ; l'autre allant jusqu'à analyser le contenu des trames protocolaires. Dans la configuration d'un firewall gérant une infrastructure téléphonique sur IP basé sur SIP, vous devez ouvrir certains ports SIP et RTP. Lors de cette ouverture de ports, les IP sources et destination doivent être systématiquement spécifiées.

c- Authentification forte

En Téléphonie sur IP, vous devez définir un certain nombre d'identifiants Login/Password (pour un trunk SIP ou pour des comptes utilisateurs).
Lors de la création de ces identifiants, vous devez faire en sorte qu'ils soient très complexes afin d'éviter qu'un éventuel pirate puisse les découvrir et attaquer votre installation :

- Login : Supérieur à 8 caractères alphanumériques
- Password : Supérieur à 12 caractères alphanumériques + caractères spéciaux

d- Attention aux configurations par défaut

La mise en place de configurations par défaut, très demandées par les administrateurs réseaux, est à double tranchant.

Dans le cadre d'une configuration par défaut, les équipements sont configurés plus rapidement. Cependant, une fonctionnalité non-utilisée est peut être malgré tout, activée par défaut. L'administrateur réseau ne pense alors pas à sécuriser cette fonctionnalité, ce qui peut bien sûr, créer d'énormes failles de sécurité.

e- Supervision en temps réel du système

Tout système qu'il soit informatique ou téléphonique (même si celui-ci est très bien sécurisé), peut comporter des failles de sécurité plus ou moins simples à exploiter. Il n'existe pas aujourd'hui de solution garantissant qu'il sera impossible de pirater l'installation. Dans ce cadre, il existe des systèmes permettant de surveiller votre réseau IP via un protocole nommé SNMP (Simple Network Management Protocol). Ce protocole est implémenté dans tous les équipements qui composent votre réseau. Des logiciels permettant la supervision sont disponibles à l'achat ou en Open Source.

La supervision vous permet donc de visualiser toutes anomalies de comportement de votre réseau.

En soit, la supervision ne fait que vous avertir d'un comportement anormale, elle ne règlera pas de manière automatique les failles. Afin de faire en sorte qu'une réaction automatique est lieu lors d'une détection d'anomalie, vous devez implémenter un IDS (logiciel de détection d'intrusion). Il en existe de très performant en Open Source. L'objectif n'est pas d'avoir un système infaillible car cela est quasiment impossible. L'objectif est simplement de rendre l'attaque tellement compliquée et longue que l'attaquant ne souhaitera pas perdre son temps sur une installation très protégée, alors que d'autres, non protégées, sont disponibles.

f- Mise à jour de sécurité des équipements

Une bonne méthode afin de se prémunir des failles connues sur les équipements est de consulter régulièrement les publications des différents constructeurs ou éditeurs. En effet, quand une faille de sécurité est découverte, une mise à jour de sécurité est rapidement publiée. Dans la majorité des cas, une mise à jour de l'installation est alors nécessaire.

5) Les règles de bonne conduite

Les règles de bonne conduite préconisées par SOS Piratage

Afin de protéger les entreprises contre le piratage Télécom, SOS Piratage engage les acteurs du marché de la Téléphonie ainsi que les entreprises à respecter les différentes règles suivantes. Ces règles permettent d'endiguer le piratage en réduisant les failles dans les installations et en limitant les conséquences financières.

Nous vous engageons à les appliquer dans les meilleurs délais et à vérifier régulièrement qu'elles sont bien respectées par tous vos interlocuteurs.

Règles de bonne conduite préconisées aux entreprises utilisatrices

- Les utilisateurs doivent personnaliser leurs codes d'accès la messagerie en utilisant des mots de passes complexes
- Les entreprises doivent définir avec leur installateur-intégrateur les destinations qu'elles souhaitent pouvoir appeler et demander un paramétrage du PABX/IPBX en conséquence
- Les entreprises doivent, si possible, souscrire à une police d'assurance intégrant les risques de piratage, fraude, usurpation d'identité, etc.

6) Comment faire en cas de piratage ?

Lorsque vous constatez que le système de Télécommunications de l'entreprise a été victime d'une fraude téléphonique, les mesures suivantes doivent être mises en œuvre :

1- Prévenir immédiatement **Tims Systèmes**.

2 - Un technicien viendra vérifier votre équipement (identifiants, mots de passe, etc.) et interdira l'accès à l'international ainsi que l'accès à certaines fonctionnalités accessibles depuis l'extérieur (messagerie vocale, renvoi d'appel, etc.) aux postes téléphoniques des utilisateurs qui n'en ont pas besoin.

3 - Demander au technicien qu'il récupère, vous communique et surtout sauvegarde les logs (c'est-à-dire les enregistrements réalisés par le système) de toutes les communications entrantes et sortantes intervenues pendant la période au cours de laquelle a eu lieu la fraude, et vous communique l'état des programmations du système tel qu'il était lors des piratages.

4 - Pour préparer un dépôt de plainte, constituez un dossier dans lequel doit figurer :

- La marque et le type du système de télécommunications piraté (n'hésitez pas à joindre la documentation utilisateur qui vous a été remise lors de l'achat),
- Les logs (enregistrements) fournis par le technicien (Cf. ci-dessus),
- Si c'est le cas, la preuve de la fermeture de l'entreprise (documentation commerciale mentionnant les horaires par exemple) pendant la période et aux heures au cours desquelles les appels des pirates ont été émis.
- Les factures détaillées de votre opérateur Télécoms sur lesquelles figurent les appels piratés, leur durée, l'heure d'émission, etc.
- Déposer une plainte auprès des services de police compétents, en leur communiquant les informations figurant dans le dossier que vous avez constitué.
- Informer votre compagnie d'assurance du piratage, si vous disposez d'un contrat vous garantissant contre les fraudes et les malveillances.

5 – Avec **Tims Systèmes**, analyser le piratage et définir une politique de sécurité si celle-ci n'existe pas dans l'entreprise, ou s'avère défaillante (fonctionnalités définies poste par poste, gestion des identifiants/mots de passe, discrimination à l'international, audits de sécurité réguliers, etc.).

Pour plus s'informations contactez-nous :
commercial@tims.fr
04 72 52 11 11