



Sécurité de la Téléphonie d'Entreprise

Risques et recommandations

TABLE DES MATIERES

1.	INTRODUCTION	3
2.	LES PRINCIPES FONDAMENTAUX	4
2.1.	LA SÉCURITÉ DE L'ARCHITECTURE TÉLÉPHONIQUE	4
2.2.	LA SÉCURITÉ DES AUTOCOMMUTATEURS (SERVEURS DE TÉLÉPHONIE)	5
3.	LE DÉNI DE SERVICE TÉLÉPHONIQUE, OU TDoS (TELEPHONY DENIAL OF SERVICE)	5
3.1.	PROBLÉMATIQUES ET ENJEUX	5
3.1.1.	<i>TDoS PAR SATURATION DES CANAUX DE COMMUNICATION DES LIENS OPÉRATEURS</i>	5
3.1.2.	<i>TDoS PAR ABUS DE PROTOCOLE, OU « FUZZING »</i>	6
3.2.	SE PROTÉGER CONTRE LES ATTAQUES PAR DÉNI DE SERVICE TÉLÉPHONIQUE (TDoS)	6
3.2.1.	<i>LES ATTAQUES PAR SATURATION DES CANAUX DE COMMUNICATIONS DES LIENS OPÉRATEURS</i>	6
3.2.2.	<i>LES ATTAQUES PAR ABUS PROTOCOLAIRE, OU « FUZZING »</i>	6
4.	LA PÉNÉTRATION DES SYSTÈMES D'INFORMATION	7
4.1.	PROBLÉMATIQUES ET ENJEUX	7
4.1.1.	<i>LA PROBLÉMATIQUE DES MODEMS EN ÉCOUTE</i>	7
4.1.2.	<i>LA PROBLÉMATIQUE DES MODEMS SORTANTS</i>	7
4.2.	SE PROTÉGER CONTRE LES TENTATIVES DE PÉNÉTRATION DU SYSTÈME D'INFORMATION PAR LE BIAIS DU SYSTÈME TÉLÉPHONIQUE	8
4.2.1.	<i>CONTRÔLER L'ACTIVITÉ DES MODEMS DE TÉLÉMAINTENANCE</i>	8
4.2.2.	<i>CONTRÔLER L'ACTIVITÉ DES AUTRES MODEMS DE L'ENTREPRISE</i>	8
5.	L'ATTEINTE À LA CONFIDENTIALITÉ	9
5.1.	PROBLÉMATIQUES ET ENJEUX	9
5.1.1.	<i>L'ÉCOUTE DES COMMUNICATIONS</i>	9
5.1.2.	<i>LES POSTES PIÉGÉS</i>	9
5.2.	ASSURER LA CONFIDENTIALITÉ ET EMPÊCHER L'ESPIONNAGE PAR LE BIAIS DU SYSTÈME TÉLÉPHONIQUE	10
5.2.1.	<i>LES FONCTIONS DANGEREUSES DE L'AUTOCOMMUTATEUR</i>	10
5.2.2.	<i>LE CONTRÔLE DE L'ACCÈS ET LA PROTECTION DU RÉSEAU DE ToIP</i>	10
5.2.3.	<i>LE CHIFFREMENT DES COMMUNICATIONS</i>	10
6.	LA FRAUDE TÉLÉPHONIQUE	10
6.1.	PROBLÉMATIQUES ET ENJEUX	10
6.1.1.	<i>LES RENVOIS VERS L'EXTÉRIEUR ET LE PIRATAGE DE LA MESSAGERIE VOCALE</i>	11
6.1.2.	<i>LES FONCTIONS POTENTIELLEMENT COÛTEUSES</i>	11
6.1.3.	<i>LES SERVEURS VoIP ACCESSIBLES DEPUIS L'INTERNET</i>	11
6.2.	SE PROTÉGER CONTRE LA FRAUDE TÉLÉPHONIQUE	11
7.	CONCLUSION	13
	MÉMENTO DES RISQUES À PRÉVENIR	13

1. INTRODUCTION

Les enjeux de la sécurité des systèmes et des réseaux téléphoniques ne sont pas encore bien identifiés par les entreprises. Peu de sources d'informations sont disponibles tant concernant l'appréciation des risques que les propositions de mesure techniques et organisationnelles. De plus, dans la plupart des cas, les politiques de sécurité des systèmes d'information ne prennent pas directement en compte la téléphonie, ou les moyens de communication voix.

Les attaques visant la téléphonie prennent de l'ampleur avec l'arrivée de la téléphonie sur IP (ToIP). Désormais, au sein d'un réseau informatique, la voix et la signalisation des communications sont considérées comme des données et transitent par le LAN, le WAN voire dans certains cas Internet. Si la ToIP est considérée comme de la donnée et se comporte comme telle, elle possède également des contraintes particulières de qualité de service et de disponibilité.

Comme toute nouvelle technologie, la téléphonie sur IP introduit de nouveaux risques et de nouvelles menaces. Héritant à la fois des propriétés de la téléphonie traditionnelle et des réseaux de données, la téléphonie sur IP est donc susceptible de connaître les problématiques sécuritaires de ces deux mondes. Ainsi, les possibilités d'attaques aux impacts potentiellement critiques se retrouvent aussi bien en téléphonie classique qu'en téléphonie sur IP : l'espionnage, la fraude, la pénétration des systèmes d'information, et les dénis de service.

La sécurité de la téléphonie doit s'inscrire dans le cadre de la politique de sécurité globale et doit être capable de traiter les problématiques en terme de :

- **Disponibilité** : le service de téléphonie a de fortes exigences en matière de disponibilité et de qualité du service. Le maintien du service de téléphonie en condition opérationnelle est un facteur fondamental qui contribue à la sécurité des biens et des personnes. En effet, il est impératif de pouvoir passer des appels d'urgence à tout moment. Un éventuel dysfonctionnement est également associé à une perte de revenus, d'opportunités, et d'efficacité.

- **Intégrité** : la téléphonie de l'entreprise repose sur des équipements dont la configuration, souvent complexe, constitue une source de risque majeur. Un changement (malveillant, ou non) de la programmation du système téléphonique peut occasionner de nombreux désagréments :

- l'octroi de droits avancés d'utilisation parfois dangereux ou illégaux,
- l'altération des tables de numérotation, ou de routage, de l'autocommutateur,
- le détournement d'appels, l'usurpation de numéros,
- la surfacturation abusive pour l'entreprise
- l'indisponibilité totale ou partielle du service de téléphonie.

- **Confidentialité** : il est fréquent que la communication d'informations confidentielles ou stratégiques entre dirigeants ou décideurs ait lieu par téléphone. Un accès malveillant à ces informations, traitées par le système téléphonique, peut mettre en péril la santé de l'entreprise. Les moyens d'interception d'informations sont nombreux :

- écoute ou enregistrement des communications, interception ou vol d'appels,
- capture des flux de téléphonie,
- accès aux annuaires et aux contacts de l'entreprise,
- accès aux boîtes de messagerie vocale et à leur contenu.

- **Imputabilité (authentification et traçabilité des opérations)** : véritable opérateur interne de télécommunications, l'entreprise est responsable de l'usage qui est fait de son système téléphonique. En cas de nécessité, l'entreprise est tenue de disposer de journaux (historique d'accès, historique des appels, ...) pouvant, le cas échéant, être mis à disposition de la justice.

Imaginons l'impact de l'absence de journaux d'accès ou de traçabilité des communications lors :

- de surfacturation abusive pour l'entreprise (fraude téléphonique),
- d'accès au système de télémaintenance donnant lieu à des modifications abusives de la configuration de l'autocommutateur permettant la mise en place d'écoutes, de déni de service, ...
- d'utilisation illicite du système de téléphonie à des fins malveillantes (terrorisme) mettant en cause la responsabilité de l'entreprise.

En effet, une entreprise dont le système téléphonique serait piraté et servirait de rebond pour nuire à un tiers peut être tenue pénalement et/ou civilement responsable. Les risques sont non seulement d'ordres financiers, mais aussi très conséquents sur l'image de la société. La sécurité n'étant malheureusement pas infaillible, la société devra démontrer qu'elle a fait de son mieux pour mettre en place des moyens de sécurisation afin d'éviter ce genre de situation.

2. LES PRINCIPES FONDAMENTAUX

2.1.LA SÉCURITÉ DE L'ARCHITECTURE TÉLÉPHONIQUE

La téléphonie doit, avant toute chose, être prise en compte au même titre que l'informatique dans la politique de sécurité du système d'information de l'entreprise.

- Il est recommandé de disposer d'une architecture résiliente. L'autonomie des sites et des accès opérateurs est un point crucial pour la continuité du service en cas de panne des systèmes centraux.
- Il est recommandé de mettre en place des éléments permettant de garantir la haute disponibilité du service de téléphonie. La sécurisation physique, logique, et la redondance des serveurs de téléphonie, de l'énergie et de la climatisation sont autant de critères à ne pas négliger.
- Il est recommandé de contrôler l'administration des équipements télécoms. Les accès doivent être délimités en fonction du niveau d'habilitation et/ou du champ d'action de l'administrateur. De plus, les accès et les actions effectuées doivent être consignés dans des journaux de bords.
- Il est recommandé de mettre en place des protections adaptées. Il est important de s'assurer plus particulièrement de la pertinence des configurations des serveurs de téléphonie et de la licéité du trafic télécom sur les liens opérateurs. Les différentes protections doivent permettre :
 - o la détection de postes ou équipements téléphoniques pirates,
 - o la surveillance de l'ensemble des liaisons opérateurs,
 - o la traçabilité des appels et la détection du type d'appel (voix/données),
 - o la mise en œuvre de règles de sécurité permettant la détection d'activités anormales et l'émission d'alertes.
- Il est recommandé de 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).

2.2.LA SÉCURITÉ DES AUTOCOMMUTATEURS (SERVEURS DE TÉLÉPHONIE)

L'ensemble des droits d'un système téléphonique constitue une liste particulièrement longue, accessible à travers des interfaces souvent complexes. Une modification intempestive des droits peut rester inconnue pendant une durée indéterminée.

- D'une manière générale, il est recommandé de limiter les droits des utilisateurs en respectant le principe du « moindre privilège ».

Les modifications des configurations des équipements constitutifs de la téléphonie sont potentiellement dangereuses et peuvent impacter l'intégrité, la confidentialité et la disponibilité du système téléphonique.

- Il est recommandé d'effectuer régulièrement des inspections et audits des configurations des autocommutateurs afin de relever les risques présents.
- Il est recommandé de suivre les modifications portant sur les configurations des autocommutateurs et de les valider.
- 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).
- Il est conseillé de disposer d'une base de connaissance de vulnérabilités et de menaces de l'équipement concerné afin d'appréhender les risques et leurs impacts, et de faciliter la prise de décision.

3. LE DÉNI DE SERVICE TÉLÉPHONIQUE, OU TDoS (TELEPHONY DENIAL OF SERVICE)

3.1.PROBLÉMATIQUES ET ENJEUX

3.1.1. TDoS PAR SATURATION DES CANAUX DE COMMUNICATION DES LIENS OPÉRATEURS

Les attaques de déni de service téléphonique visent à empêcher de recevoir ou d'émettre des appels et éventuellement à saturer les boîtes vocales des utilisateurs : tous les téléphones de l'entreprise sonnent sans interruption. Lorsque vous décrochez, vous n'entendez qu'un bruit de fond ou une musique d'attente. Lorsque vous raccrochez, votre téléphone se remet à sonner quelques secondes plus tard. Les utilisateurs, exaspérés, finissent par laisser leur combiné décroché ou par débrancher leur ligne.

Toutes vos lignes sont occupées, vos correspondants externes ne peuvent plus vous joindre, vous ne pouvez plus émettre d'appels. Même les services d'urgences peuvent être impactés. Et cette attaque peut durer des heures.

Pour saturer la capacité d'une infrastructure téléphonique à recevoir des appels, il suffit d'utiliser autant de canaux de communications que ceux dont dispose l'entité ciblée, et d'utiliser des robots d'appels (logiciels ou matériels) pour appeler en boucle les numéros de celle-ci. Ce principe vaut tant en téléphonie traditionnelle qu'en VoIP.

Pour l'attaquant, les appels sont souvent gratuits. Les services de téléphonie par Internet sont un moyen

particulièrement efficace pour lancer ces attaques de déni de service téléphoniques, grâce à l'utilisation de comptes piratés de téléphonie par Internet. Un petit programme suffit pour automatiser les appels.

La portée d'une telle attaque peut aussi s'étendre au système de messagerie unifiée. La forte sollicitation en plus de l'espace de stockage nécessaire à l'enregistrement des messages vocaux peut le rendre temporairement indisponible ou bien le paralyser totalement. L'entreprise ne peut alors plus communiquer ni par téléphone, ni par courrier électronique.

3.1.2. TDoS PAR ABUS DE PROTOCOLE, OU « FUZZING »

Le « fuzzing » est une méthode permettant de tester les logiciels afin de mettre en évidence des dysfonctionnements potentiels. L'une des méthodes couramment utilisées chez les éditeurs de logiciels consiste à envoyer des informations incorrectes à un serveur pour voir comment ce dernier réagit. En cas de comportement anormal du serveur, les développeurs corrigent le problème.

Cette méthode peut être détournée par des personnes malintentionnées pour rechercher et trouver des faiblesses dans un système ToIP. Cette attaque, si elle aboutit, peut permettre d'obtenir des droits d'administration sur le serveur de téléphonie, d'allonger les temps de réponses, ou de mettre le système hors service.

3.2. SE PROTÉGER CONTRE LES ATTAQUES PAR DÉNI DE SERVICE TÉLÉPHONIQUE (TDoS)

3.2.1. LES ATTAQUES PAR SATURATION DES CANAUX DE COMMUNICATIONS DES LIENS OPÉRATEURS

- Il est nécessaire de disposer d'équipements de type « firewall » permettant d'exercer un filtrage dynamique des communications téléphoniques (réseau classique TDM ou VoIP). Ces équipements doivent être en mesure de détecter les communications rendues dangereuses par leurs nombres ou leurs fréquences et permettre de les stopper en amont de l'autocommutateur selon des seuils définis par la politique de sécurité (nombre de communications simultanées pour un même appelant ou nombre d'appels sur une durée spécifiée).
- Il est recommandé de mettre en place des liens opérateurs dédiés aux appels entrants et d'autres dédiés aux appels sortants. Ainsi, lors d'une attaque depuis l'extérieur, seules les communications entrantes seront perturbées.

3.2.2. LES ATTAQUES PAR ABUS PROTOCOLAIRE, OU « FUZZING »

- Il est nécessaire de s'équiper d'équipements de type « firewall » permettant d'exercer un filtrage applicatif des protocoles de téléphonie utilisés (niveau 7 du modèle OSI). L'analyse du contenu (au-delà de l'entête), ou « Deep Packet Inspection », des datagrammes permet d'identifier les paquets malformés et de les filtrer, de détecter les paquets hors-contextes et ainsi d'éviter les intrusions ou les sabotages.

4. LA PÉNÉTRATION DES SYSTÈMES D'INFORMATION

4.1. PROBLÉMATIQUES ET ENJEUX

Les deux mondes de l'informatique et des télécommunications se côtoient et s'interconnectent depuis des années. L'autocommutateur est connecté d'un côté sur le réseau télécom public et d'un autre sur le réseau informatique. Nombre d'autocommutateurs disposent d'une fonction de télémaintenance. Le risque d'un accès externe à ces équipements est à évaluer en fonction des connexions dont ils disposent avec les autres systèmes sur le réseau.

4.1.1. LA PROBLÉMATIQUE DES MODEMS EN ÉCOUTE

Les autocommutateurs et certains équipements (copieurs, fax, ...) disposent soit de modems externes, soit de modems internes (intégrés à une des cartes électroniques) destinés à la télémaintenance. Le niveau de sécurité des solutions d'accès en télémaintenance est très variable. Aussi, il n'est pas inhabituel de trouver des modems opérationnels et non répertoriés au sein de l'entreprise.

En utilisant des outils spécifiques (basés sur des batteries de modems) permettant d'effectuer la reconnaissance des équipements se cachant derrière les numéros de téléphone, un attaquant peut facilement détecter la présence de modems en écoute dans une entreprise. L'outil appelle automatiquement et successivement les numéros de l'entreprise à la recherche de points d'entrée (pratique appelée « wardialing »). Les outils utilisés permettent la détection du type d'équipement distant qui répond à l'appel : simple téléphone, fax, modems. Il ne reste ensuite plus qu'à lancer une attaque de type « brute-force » sur les équipements potentiellement intéressants. Les premiers mots de passe essayés sont, bien évidemment, les mots de passe « constructeurs », ou « par défaut ». De plus, des listes de mots de passe d'entreprises circulent au marché noir. En effet, la divulgation de ces informations sensibles se monnaie fréquemment.

Une fois un modem identifié et son mot de passe acquis, il ne reste plus qu'à s'y connecter pour avoir un accès à tout ou partie du système d'information de l'entreprise. Cet accès peut permettre la prise de contrôle de l'autocommutateur, sa reprogrammation, son sabotage, l'accès à ses journaux et aux informations sensibles qu'il contient, ou alors servir de rebond vers d'autres équipements sensibles (serveurs de données, ...) de l'entreprise.

4.1.2. LA PROBLÉMATIQUE DES MODEMS SORTANTS

Il n'est pas rare de trouver encore des modems utilisés comme mode d'accès à certains services dans les entreprises. De même, nos ordinateurs portables disposent toujours de modems analogiques permettant une connexion à l'Internet lors de déplacement.

Ce mode d'accès est aussi parfois utilisé par le personnel de l'entreprise pour contourner la politique de sécurité du système d'information afin d'accéder librement à l'Internet, en déjouant les protections souvent contraignantes (firewalls, serveurs proxys, solutions de filtrage d'accès aux URL) mises en place sur l'accès Internet de l'entreprise.

En effet, il suffit de s'emparer de la prise téléphonique, analogique, d'un fax pour se raccorder sur le réseau public et initialiser une connexion vers un Fournisseur d'Accès Internet. Dès lors, tout l'Internet est à portée de l'utilisateur, sans restriction, mais aussi sans protection.

Pour exemple, nous nous souvenons qu'il y a seulement quelques années, un ordinateur connecté à l'Internet

sans protection, ou patches de sécurité, à jour se faisait infecter en seulement dix minutes. Les menaces étant aujourd'hui plus nombreuses, le risque de compromission de cet ordinateur directement connecté à l'Internet est toujours très élevé (virus, logiciel espion, cheval de Troie, ...).

Pire encore, l'utilisateur de l'ordinateur a « oublié » de se débrancher du réseau local de l'entreprise lors de sa connexion à l'Internet avec son modem : le système d'information est alors potentiellement accessible depuis l'extérieur.

4.2. SE PROTÉGER CONTRE LES TENTATIVES DE PÉNÉTRATION DU SYSTÈME D'INFORMATION PAR LE BIAIS DU SYSTÈME TÉLÉPHONIQUE

- Il est recommandé de ne pas interconnecter l'ensemble du système téléphonique au réseau informatique, sauf si ce dernier est spécifique à son administration et son exploitation.
- L'interconnexion entre des VLAN du réseau de données et des VLAN du réseau voix ne doit être autorisée que sur des interconnexions identifiées, maîtrisées et protégées.
- Il est recommandé de disposer de moyens de détection d'attaques de type « wardialing ». Pour se protéger de cette attaque consistant à appeler successivement tous les numéros d'une entreprise dans le but de rechercher des points d'entrée (serveur de boîtes vocales, modem, fax, etc.), il est nécessaire de surveiller l'activité sur les liens opérateurs.

4.2.1. CONTRÔLER L'ACTIVITÉ DES MODEMS DE TÉLÉMAINTENANCE

- Il est recommandé de ne pas activer en permanence la liaison de télémaintenance des serveurs et, lorsque cela est possible, de débrancher physiquement le modem d'accès (dorénavant les modems sont le plus souvent intégrés au cœur de l'autocommutateur).
- Il est déconseillé d'utiliser un modem simple, sans mécanismes d'authentification, pour l'administration distante des autocommutateurs. Il est recommandé d'utiliser les mécanismes de sécurisation suivants :
 - o modem utilisant des moyens de chiffrement,
 - o modem acceptant exclusivement des méthodes d'authentification forte,
 - o modem assurant un rappel automatique d'un numéro prédéfini (call-back),
- Il est recommandé, dans le cas où toute ou partie de la télémaintenance est réalisée par des prestataires externes, d'imposer des règles très strictes de gestion des moyens d'identification et d'authentification, ainsi que de contrôle du personnel en charge de la prestation. Ces règles doivent inclure l'accès nominatif des comptes d'administration, la mise en place de moyens techniques spécifiques de traçabilité et la tenue d'un carnet de bord des actions d'administration réalisées.
- Il est recommandé, pour l'administration à distance des autocommutateurs à travers un réseau public, de faire attribuer un numéro de téléphone SDA ne faisant pas partie de la ou des principales plages de numéros SDA gérés par l'autocommutateur, de le faire inscrire sur liste rouge et de veiller à ce qu'il ne soit référencé dans aucun document public.
- Il est recommandé de mettre en place des moyens de détection et d'alerte lorsqu'un appel a lieu sur les modems de télémaintenance afin de vérifier le bien fondé de cette communication.

4.2.2. CONTRÔLER L'ACTIVITÉ DES AUTRES MODEMS DE L'ENTREPRISE

- Il est recommandé de recenser les modems légitimes de l'entreprise et de consigner les informations d'usage du modem (son utilité, nom de la ou les personnes l'utilisant, son emplacement physique) dans un document d'exploitation.

- Il est recommandé de mettre en place des moyens d'identification des communications modems illicites (identification de porteuses) afin de détecter la présence de modems inconnus et actifs.
- Il est recommandé de pouvoir être alerté lors de l'établissement de communications modems afin de pouvoir, le cas échéant, réagir rapidement.
- Il est nécessaire de disposer des moyens de protection en temps réel contre les communications de type modem provenant de numéros non référencés aussi bien à l'intérieur qu'à l'extérieur de la société. Par exemple, un poste de travail, s'il se connecte à l'Internet par l'intermédiaire d'un FAI, via le RTC, alors qu'il est connecté sur le réseau de données, ouvre un accès vers le système d'information (création de porte dérobée, ou « backdoor » permettant d'outrepasser les protections habituelles du réseau de données). A l'inverse, toute communication modem entrante depuis un numéro inconnu et vers un poste, non référencé comme pouvant effectuer des communications modem, doit être surveillée. En effet, un tiers pourrait tenter d'accéder au système d'information par ce biais. Ces comportements doivent pouvoir être identifiés et automatiquement stoppés.

5. L'ATTEINTE À LA CONFIDENTIALITÉ

5.1. PROBLÉMATIQUES ET ENJEUX

5.1.1. L'ÉCOUTE DES COMMUNICATIONS

Il s'agit d'intercepter, d'écouter, et même d'enregistrer des conversations à l'insu des interlocuteurs.

En téléphonie traditionnelle, certaines fonctionnalités sensibles de l'autocommutateur comme l'« entrée en tiers » ou l'« écoute discrète » permettent l'écoute de conversations. De même, la fonction d'enregistrement peut être utilisée afin de recevoir la conversation au format audio directement dans sa boîte e-mail, ce qui permet ensuite de la manipuler aisément ou encore de la publier sur Internet.

En ToIP, des attaques du monde informatique permettent à une personne malintentionnée d'intercepter une conversation et de l'enregistrer. Les captures de flux ou bien les attaques de type « Man-In-The-Middle » peuvent alors être utilisées pour réaliser des écoutes, des enregistrements et même des dénis de service. Les « outils » nécessaires à ce type d'attaques sont librement accessibles sur l'Internet.

La messagerie vocale n'est pas en reste puisqu'elle permet d'écouter ses messages, même depuis l'extérieur, avec, dans la plupart des cas, un mot de passe n'excédant pas 4 chiffres qui est très rarement modifié. Il n'est pas très difficile de retrouver le mot de passe d'un compte, souvent laissé par défaut. De plus, il existe des outils spécifiques permettant de tester rapidement et automatiquement les seules 10 000 possibilités.

5.1.2. LES POSTES PIÉGÉS

Il est possible d'utiliser certaines fonctions d'un autocommutateur afin de « piéger » temporairement des postes téléphoniques. Ces postes téléphoniques pourront, lorsqu'on les appelle, décrocher automatiquement et silencieusement, sans sonnerie aucune. Si ces manipulations nécessitent un minimum de préparation, l'utilisation qui peut en être faite dans les bureaux de direction, dans les salles de réunion et lors de comités stratégiques permet à un tiers de prendre connaissance de diverses informations, en toute discrétion.

Inutile alors de solliciter une société pour rechercher d'éventuels micros cachés lorsque celui utilisé est

légitimement posé, bien en vue, sur le bureau.

5.2. ASSURER LA CONFIDENTIALITÉ ET EMPÊCHER L'ESPIONNAGE PAR LE BIAIS DU SYSTÈME TÉLÉPHONIQUE

5.2.1. LES FONCTIONS DANGEREUSES DE L'AUTOCOMMUTEUR

- Il est recommandé d'interdire les fonctionnalités à risques telles que l'entrée en tiers (discrète ou non), l'écoute bébé (« baby-phone »), l'interphonie, la substitution, etc. Celles-ci ne doivent être activées que lors de circonstances exceptionnelles ou si le besoin est dûment motivé. L'activation des fonctionnalités à risques, au su ou à l'insu des administrateurs télécoms, devra être détectée par des moyens de sécurisation ou d'audit automatisé.
- Il est recommandé de mettre en place des audits réguliers de la configuration de l'autocommutateur vérifiant l'attribution de ces fonctionnalités à risques.

5.2.2. LE CONTRÔLE DE L'ACCÈS ET LA PROTECTION DU RÉSEAU DE ToIP

- Il est nécessaire de disposer de moyens de sécurisation des réseaux permettant de protéger contre les attaques classiques d'interception et d'usurpation sur les réseaux IP (ARP poisoning, DNS spoofing, DHCP spoofing ...).
- Il est nécessaire de disposer de moyens permettant d'être alerté lors de la connexion d'un équipement inconnu sur le réseau.
- Il est conseillé, lorsque cela est possible, de s'équiper de moyens de contrôle d'accès au réseau de ToIP (NAC).
- Il est recommandé de sensibiliser les utilisateurs aux risques de l'utilisation de mots de passe faibles et de les contraindre à changer le mot de passe par défaut de leur compte de messagerie vocale.

5.2.3. LE CHIFFREMENT DES COMMUNICATIONS

- Il est recommandé de chiffrer les flux des communications internes et intersites de l'entreprise.
- Il est également recommandé de chiffrer les flux de signalisation.

6. LA FRAUDE TÉLÉPHONIQUE

6.1. PROBLÉMATIQUES ET ENJEUX

La fraude téléphonique consiste à utiliser le système téléphonique d'une entreprise pour effectuer des appels non autorisés et à grande échelle. Ces abus sont généralement rendus possibles grâce à la détection d'une mauvaise configuration des serveurs de téléphonie depuis l'intérieur ou l'extérieur de l'entreprise par des personnes malveillantes.

6.1.1. LES RENVOIS VERS L'EXTÉRIEUR ET LE PIRATAGE DE LA MESSAGERIE VOCALE

Une des techniques les plus utilisées consiste à activer les fonctions de renvoi d'appels pour forcer une entreprise à appeler un serveur surtaxé qui, afin de compliquer les investigations, est généralement placé à l'étranger. Une fois le renvoi vers le numéro surtaxé en place, il suffit de lancer une campagne d'appels vers le poste renvoyé. Tous les appels seront réacheminés, au frais de l'entreprise, vers le serveur surtaxé. L'attaquant, généralement propriétaire du serveur surtaxé, ou son complice, gagne une somme d'argent proportionnelle au trafic généré. Afin de ne pas être détectées, ces attaques se déroulent le plus souvent le weekend et la nuit. Pour exemple, le coût de ces attaques pour une entreprise peut varier de quelques milliers à plusieurs centaines de milliers d'euros en un week-end. Plus l'entreprise dispose de canaux de communication, plus rapidement le fraudeur gagne de l'argent. Sachant que les appels vers certains numéros sont facturés à des tarifs importants dès la mise en relation, la compromission d'une seule ligne téléphonique qui appelle ce numéro des dizaines de fois par minute suffira à alourdir considérablement la facture.

Il n'est pas nécessaire de disposer d'une complicité en interne pour configurer les renvois vers la destination surtaxée. En effet, les fonctionnalités des messageries vocales permettent souvent de configurer un renvoi de son poste vers un autre numéro, à distance. Il suffit alors de « trouver » une boîte vocale disposant d'un mot de passe faible (0000, 1234, etc.) pour pouvoir configurer le renvoi.

6.1.2. LES FONCTIONS POTENTIELLEMENT COÛTEUSES

Dans certains cas, les fonctionnalités téléphoniques nécessaires au fonctionnement opérationnel de l'entreprise, peuvent présenter un risque potentiel de malveillance : par exemple, les fonctions de conférence et de transfert permettent la mise en relation (aboutements) d'interlocuteurs externes aux frais de l'entreprise. Autre exemple, la fonction DISA permet l'accès aux services de l'autocommutateur depuis l'extérieur. Un utilisateur disposant d'un accès sur ce service peut téléphoner aux frais de l'entreprise.

6.1.3. LES SERVEURS VOIP ACCESSIBLES DEPUIS L'INTERNET

Une pratique courante des fraudeurs consiste à scanner les adresses IP accessibles depuis l'Internet et à identifier les serveurs VoIP accessibles et mal protégés ou disposant de comptes utilisant des mots de passe faibles. Ces serveurs permettent alors de téléphoner gratuitement depuis l'Internet. L'affaire resterait anodine si le fraudeur gardait sa découverte pour sa propre utilisation. En effet, ceux-ci abusent du système et revendent à grande échelle les communications vers des destinations onéreuses ou génèrent de nombreux appels vers des numéros surtaxés, sur lesquels ils touchent une commission. Ces fraudes peuvent ainsi atteindre plusieurs millions d'euros en seulement quelques mois.

6.2. SE PROTÉGER CONTRE LA FRAUDE TÉLÉPHONIQUE

- D'une manière générale, il est recommandé de limiter les droits des utilisateurs en respectant le principe du « moindre privilège ». En particulier, il est nécessaire de surveiller les fonctions de renvoi vers un numéro externe, de DISA, et les aboutements de réseau.
- Il est recommandé de limiter, en respectant le principe du « moindre privilège », les destinations pouvant être appelées (numéros internationaux, surtaxés, ou services coûteux).
- Il est recommandé de mettre en place des moyens permettant la détection automatique et la protection contre les menaces suivantes :

- o usage abusif du téléphone par les utilisateurs légitimes ou par un personnel extérieur (entretien, maintenance, gardiennage, etc.),
 - o détournement de trafic à des fins malveillantes,
 - o génération automatique de trafic vers des numéros surtaxés (exemple : par un ver introduisant un « dialer »),
- Il est recommandé de disposer de moyens de détection d'attaques de type « wardialing » consistant à appeler successivement tous les numéros d'une entreprise dans le but de rechercher des points d'entrée (serveur de boîtes vocales permettant d'établir des appels aux frais de l'entreprise, depuis l'extérieur).
- Il est recommandé d'identifier les utilisateurs qui bénéficient d'un accès depuis l'extérieur à la messagerie vocale permettant la génération d'appels aux frais de l'entreprise et de consigner le tout dans un document d'exploitation.
- Il est recommandé de sensibiliser les utilisateurs aux risques de l'utilisation de mots de passe faibles et de les contraindre à changer le mot de passe par défaut de leur compte de messagerie vocale.

7. CONCLUSION

La maîtrise des technologies et usages en matière de sécurité des infrastructures téléphoniques devient, comme pour les systèmes informatiques, un enjeu stratégique face aux menaces toujours plus nombreuses, diversifiées et dangereuses que représentent la cybercriminalité organisée ou le terrorisme.

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.

MÉMENTO DES RISQUES À PRÉVENIR	
Déni de service téléphonique	<ul style="list-style-type: none">• Saturation de la capacité des liens opérateurs menant à l'impossibilité de passer ou de recevoir des appels.• Mise hors service du service de téléphonie au moyen d'une attaque protocolaire.
Intrusion sur le système d'information	<ul style="list-style-type: none">• Attaques de « wardialing » permettant d'identifier les périphériques accessibles depuis le réseau téléphonique (modem, fax, serveurs de messagerie vocale) et tentatives d'authentications par « brute-force ».• Modems non maîtrisés pouvant donner accès à tout, ou partie, du système d'information.• Accès aux modems de télémaintenance dans un but de sabotage ou de rebond vers d'autres systèmes.• Création de portes dérobées (backdoors).
Espionnage	<ul style="list-style-type: none">• Ecoute discrète 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.
Fraude téléphonique	<ul style="list-style-type: none">• Détournement de trafic et revente de communications.• Rebonds.• Renvois vers des numéros surtaxés.