

# Le téléphone, cible des pirates !

novembre 2009 par Emmanuelle Lamandé

*Le téléphone a su s'imposer au fil des ans comme une « évidence » dans notre quotidien. La disponibilité a toujours représenté un facteur clé de cet outil, qui permet avant tout d'assurer la sécurité des biens et des personnes. Pourtant, les systèmes de téléphonie ont bien changé depuis leur création. Les PABX sont aujourd'hui de véritables systèmes informatiques, avec toutes les problématiques que cela suppose pour les entreprises. Les vulnérabilités de la ToIP viennent s'ajouter à celles de la téléphonie TDM, attirant toujours plus d'« âmes » malveillantes. Quelles sont ces vulnérabilités ? Existe-t-il des moyens de s'en prémunir ? Le CLUSIF ouvre le débat.*

Pour Benoît Le Mintier, Directeur des Opérations Ercom, 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 QoS. En effet, la téléphonie reste avant tout un outil permettant d'assurer la sécurité des biens et des personnes. Avec la ToIP, la DSI ne fournit plus seulement des services informatiques. Elle devient aussi opérateur interne de télécoms. Il est donc nécessaire de redéfinir, au niveau organisationnel, les responsabilités de chacun. Enfin, au niveau fonctionnel, il s'agit de déterminer de quelle manière le poste de travail doit être pensé ?

Frédéric Dur, Consultant CheckPhone, déplore le manque d'attention portée sur la sécurité des PABX, d'autant que les enjeux sont importants pour l'entreprise, notamment dans la relation de confiance qu'elle entretient avec ses clients. Les PABX sont aujourd'hui de véritables systèmes informatiques (connectivité IP, système d'exploitation, ...), ce qui engendre de nouvelles failles et attirent les « âmes » malveillantes.

Qui attaque une infrastructure télécoms ? Au sein de l'entreprise, il peut s'agir de bidouilleurs curieux, de stagiaires, d'employés mécontents ou encore d'espions. De l'extérieur, ce peut être la résultante d'un pirate isolé ou de hackers professionnels agissant pour le compte de tiers (groupe mafieux, concurrent, état, ...). Ces attaques peuvent avoir différents objectifs : l'espionnage de l'entreprise, l'appât du gain, la volonté de nuire (atteinte à la disponibilité par exemple), la vengeance, ...

Comment hacker ? De nombreux sites Internet fournissent des informations permettant de pirater les systèmes de téléphonie. Il peut s'agir de méthodes et d'outils de piratage, d'informations sur les entreprises à pirater, des listes de vulnérabilités des systèmes, ... Au travers d'un PABX, on peut, en effet, pirater ou détruire des informations, écouter ou enregistrer une conversation, provoquer des arrêts de services, pénétrer dans le SI, ... Les conséquences de telles attaques peuvent s'avérer plus que dommageables pour une entreprise. Outre les impacts financiers pour l'entreprise, c'est la responsabilité pénale du dirigeant qui est en cause, ce dernier étant responsable du système de téléphonie qu'il offre à ses employés. Les peines peuvent d'ailleurs aller jusqu'à 5 ans d'emprisonnement et 300.000 euros d'amende.

## Ecoute illégale, phreaking, DoS ... autant de risques qui pèsent sur la téléphonie

Les risques existaient déjà dans les systèmes de téléphonie traditionnels. On se souviendra en 2002 du piratage du standard téléphonique de la Cité des Congrès de Nantes. Le préjudice de cette attaque s'élevait à près de 70.000 euros (source : La Tribune 02/2002). Cependant, depuis l'arrivée de la ToIP, les attaques se généralisent. Début 2009, une entreprise australienne reçoit une facture téléphonique salée (11.000 appels pirates en 46 heures), un préjudice estimé à plus de 120.000 dollars (Source : The West 01/2009).

A l'heure actuelle, 5 risques majeurs pèsent sur la téléphonie d'entreprise :

- ▶ L'écoute illégale et donc l'atteinte à la confidentialité : ce peut être à travers l'utilisation abusive des fonctions d'écoute, un accès frauduleux au système de messagerie vocale, l'enregistrement de conversations ou du journal d'appels, ... avec pour conséquences des fuites d'informations sensibles et stratégiques pour l'entreprise, ou encore l'atteinte à la vie privée.
- ▶ La fraude téléphonique (phreaking) : utilisation abusive du service de téléphonie, revente de communications, renvois vers des numéros surtaxés, entraînant une surfacturation téléphonique importante, voire une saturation des canaux de communication.
- ▶ Le Déni de Service (DoS) : sabotage du PABX, re-routage du trafic, rebond automatique, interruption abusive d'appels, augmentation du temps de réponse des équipements téléphoniques. Ces attaques peuvent engendrer l'indisponibilité du service de téléphonie, des plaintes de clients et des pertes de chiffre d'affaires, de contrats commerciaux ou encore d'image.
- ▶ L'utilisation malveillante des modems : depuis l'extérieur, il peut s'agir de du piratage des modems de télémaintenance ou des modems internes. Depuis l'intérieur, ce peut être l'utilisation de lignes analogiques, dans le but d'outrepasser la politique de sécurité Internet par exemple. L'utilisation malveillante des modems peut permettre une interconnexion clandestine d'Internet avec le réseau de l'entreprise.
- ▶ Le cas des Softphones : difficulté à 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.

## **Dans 4 cas sur 5, le test d'intrusion permet un accès à la totalité du réseau depuis un téléphone**

A travers différents scénarios d'attaques, Loïc Castel, Ingénieur Tests d'intrusion, Telindus SCR, nous a démontré qu'il existe des attaques tout à fait réalisables, et ce pour tous types d'entreprises. Pour lui, les principaux risques pour l'entreprise ont trait à la disponibilité, la confidentialité, l'intégrité et l'impact financier. Pourtant, malgré ces risques, le constat des audits effectués par son entreprise est éloquent. 50% des clients n'ont pas changé le mot de passe par défaut du call server. Plus de 95% des clients n'ont pas installés de chiffrement. Et dans 4 cas sur 5, le test d'intrusion permet un accès à la totalité du réseau depuis un téléphone.

Quelles solutions existent face à ces risques ? Pour Frédéric Dur, il apparaît, tout d'abord, primordial de disposer d'une politique globale de sécurité « voix » et de l'appliquer. Il est nécessaire d'intégrer la téléphonie dans les Tableaux de Bords de Sécurité du Système d'information. Les équipements (PABX,...) doivent être protégés, à travers des audits réguliers d'analyse des configurations, une sécurisation et journalisation des accès aux modems de télémaintenance. Le réseau téléphonique doit également être protégé. Il faut mettre en place des moyens d'analyse de trafic et de détection d'anomalies, découvrir les modems « pirates » de l'entreprise, ... Enfin, il est nécessaire de garantir la traçabilité des événements, en journalisant les éléments de connexion.

La formation et la responsabilisation des administrateurs et des utilisateurs représentent, pour Loïc Castel, deux points clés dans un projet de VoIP, en parallèle de la politique de sécurité globale. Concernant le Call Server, il conseille d'en restreindre l'accès logique et physique, de définir et d'implémenter une politique d'accès. Au niveau des systèmes et de l'infrastructure, il recommande, entre autres, le chiffrement des communications et des signaux, la revue des vulnérabilités et l'application des patches. Enfin, pour les postes IP, il conseille l'autodéconnexion la nuit et l'ajout d'authentifiant afin d'empêcher la récupération d'informations.

## **La disponibilité de la téléphonie est un impératif**

Le CLUSIF prépare actuellement une synthèse concernant la « malveillance des outils de communication Voix », conclut Jean-Marc Grémy, Consultant Cabestan Consultants. Un document didactique, visant à réunir les professionnels du monde de la voix TDM et VoIP, qui devrait sortir avant la fin de l'année. Il souligne l'enjeu majeur de la disponibilité que le monde de la téléphonie a toujours été habitué à traiter, beaucoup plus que le monde informatique. Dans ce flot de convergence, la DSI doit prendre en compte ce nouvel impératif, car il est inenvisageable pour tout un chacun de ne pas réussir à joindre les secours en cas d'urgence, ou pire de voir les secours arriver au mauvais endroit et donc trop tard ... un scénario catastrophe pas si irréel que cela puisqu'il s'est déjà produit en France comme aux Etats-Unis.