IT-expert magazine

Phreaking : quand les pirates s'attaquent aux lignes téléphoniques

0

10 Dec 2015 Phreaking, piratage, sécurité, telecom by Aurelie Magniez

En s'attaquant à leurs infrastructures téléphoniques et en exploitant ainsi de manière malveillante leurs commutateurs privés (PABX ou IPBX), les pirates utilisent l'abonnement téléphonique des entreprises, générant pour leurs victimes des surfacturations importantes, pouvant aller, suivant les hypothèses, jusqu'à menacer l'existence de la société elle-même.

Les PABX ou IPBX sont des dispositifs chargés d'assurer la commutation d'un réseau téléphonique privé. Ils permettent d'offrir un grand nombre de fonctionnalités comme une messagerie vocale, un standard téléphonique intégré, une redirection d'appels, ou un accès distant au poste.

Le développement technologique de la téléphonie s'appuie sur le développement et l'implémentation de composants identiques aux systèmes informatiques. Ainsi les équipements téléphoniques deviennent des systèmes informatiques à part entière, ce qui explique que les attaques perpétrées par les pirates se soient multipliées.

Les actes malveillants poursuivent des objectifs distincts selon les types d'attaques perpétrées : blocage des systèmes, écoute des conversations téléphoniques, destruction de données ou encore détournement de la ligne pour passer des appels téléphoniques à l'international.

Comme pour les systèmes informatiques, la téléphonie permet aujourd'hui aux pirates de commettre des attaques par déni de service et des usurpations d'identité. L'explosion des smartphones sur le marché a entrainé de nouveaux types de fraudes, comme le Telephony Denial of Service (TDos) qui permet l'envoi massif d'appels sur un téléphone pour en bloquer l'accès.

Les fraudes à la téléphonie représentent des pertes considérables pour les entreprises, qui victimes du détournement de leur ligne téléphonique se voient facturer des appels surtaxés ou internationaux. En outre, les conséquences occasionnées par la destruction de données peuvent s'avérer considérables.

http://www.it-expertise.com/phreaking-quand-les-pirates-sattaquent-aux-lignes-telephoniques/

Il est pourtant possible d'agir de manière préventive pour empêcher ces attaques en mettant en pratiques certaines mesures. Lorsque le mal est fait, l'entreprise victime de la fraude doit réagir et mettre en œuvre un plan d'action pour lutter contre la fraude.

Prévoir les attaques

L'entreprise doit veiller à mettre en place une politique de sécurité intégrant l'installation téléphonique, au même titre que son équipement informatique. Certaines mesures de sécurité peuvent facilement être mises en œuvre :

- le renforcement de la sécurité des équipements téléphoniques, notamment par la mise en place de contrôle d'accès et de mots de passe, qui doivent en outre être changés régulièrement ;
- le cloisonnement entre les flux de données et les flux de voix ;
- une authentification pour les accès internet ;
- la mise en place de pare-feu adaptés aux technologies téléphoniques ;
- une analyse du trafic ;
- le cryptage des informations sensibles et la mise en œuvre de mesures propres à assurer la confidentialité des données.

La détection des anomalies passe surtout par un contrôle de la facturation régulière.

L'entreprise peut également réduire les fonctionnalités de l'équipement téléphonique au strict nécessaire et notamment restreindre les appels internationaux.

Il est important de communiquer en interne afin de sensibiliser ses collaborateurs, notamment passer par la mise en place d'une charte rappelant les règles de vigilance et incitant notamment les collaborateurs à enregistrer un mot de passe et à sécuriser leur messagerie.

Il est également possible de mettre en œuvre un audit de la sécurité dans l'entreprise. L'objectif de l'audit est de faire un état des lieux de la sécurité dans l'entreprise et notamment de déterminer si le système informatique et téléphonique de l'entreprise est suffisamment protégé.

Ce type d'attaque peut engendrer des frais très importants. Des sociétés d'assurance proposent désormais de souscrire des assurances spécifiques aux équipements téléphoniques. Il est préconisé de souscrire une assurance, qui pourra prendre en charge les coûts entrainés par l'attaque.

Comment réagir en cas d'attaque ?

Avant d'intenter une procédure judiciaire, les moyens d'action vont dépendre du type d'atteinte portée aux équipements téléphoniques de la victime.

Il est d'abord possible d'agir au civil sur le fondement du manquement de l'opérateur de télécommunications et/ou de l'intégrateur à son devoir de conseil et de mise en garde. En effet, Il résulte d'une décision de la Cour d'appel de Versailles du 25 mars 2014 reprise par le Tribunal de commerce de Nanterre dans une décision du 5 février 2015 quela responsabilité du prestataire de PABX peut, dans certaines circonstances, être engagée s'il est établi un manquement du prestataire à son obligation d'information, notamment en ce que« la cliente n'avait aucune conscience des risques qu'elle courait » et que celle-ci rapporte la preuve « d'un comportement fautif (du prestataire) qui n'a pas sensibilisé (sa cliente) à ce problème ».

Dans ces deux jurisprudences, la condamnation du prestataire de PABX a été prononcée car celui-ci était expressément tenu de vérifier l'état de sécurisation téléphonique dans le contrat qui le liait à son client.

http://www.it-expertise.com/phreaking-quand-les-pirates-sattaquent-aux-lignes-telephoniques/

La Cour d'appel de Versailles relève ainsi que : *« Considérant cependant que le contenu des engagements et obligations de la société (prestataire) doit être interprété à la lumière des conditions générales annexées au contrat de maintenance, dont il résulte que le prestataire de maintenance a une mission générale d'assistance du client en matière de télécommunication pouvant intéresser l'exercice de son activité et qu'il est en outre tenu à une « visite préventive » par an »* et le Tribunal de commerce de Nanterre : *« Attendu qu'il appartenait à la société (prestataire), qui était tenue de procéder à un minimum d'une visite annuelle de l'installation dans le cadre d'une formule « Excellence », de vérifier l'état de sécurisation de l'installation téléphonique de sa cliente et de vérifier que celle-ci l'utilisait dans des conditions optimales de sécurité et d'efficacité »*.

Il convient ainsi de s'assurer, lors de la conclusion d'un contrat avec l'intégrateur, des prestations qui sont à sa charge notamment en matière de sécurité.

En l'absence de dispositions contractuelles spécifiques, la responsabilité contractuelle cède au profit de la responsabilité délictuelle de droit commun, et la Chambre commerciale de la Cour de cassation a alors précisé dans sa décision du 11 juillet 2006 que *« le devoir de conseil du prestataire a ses limites dans l'obligation du client de s'informer et de collaborer avec ce dernier »*.

Par ailleurs, les opérateurs de télécommunications sont tenus de mettre en place un dispositif de contrôle des consommations anormales et doivent alerter l'entreprise lorsqu'ils constatent une consommation excessive sur la ligne. Lorsqu'ils ne prévoient pas de système d'alertes des anomalies, les opérateurs de télécommunications sont susceptibles d'engager leur responsabilité.

Si la facture est anormalement élevée, l'entreprise peut demander un détail de la facturation à son opérateur de télécommunications qui est tenu de lui fournir. La liste des appels pourrait lui permettre de démontrer qu'elle n'est pas l'auteur des appels frauduleux.

Il faut également préciser qu'en cas de manquement de l'opérateur de télécommunications à ses obligations, la jurisprudence accepte seulement de prononcer la condamnation au versement de dommages et intérêts, qui peuvent couvrir le montant des factures ou être plus élevés en cas de démonstration d'un préjudice plus important, mais l'entreprise reste tenue de payer les factures, y compris pour les appels téléphoniques passés par des tiers.

Il est donc indispensable pour l'entreprise de mettre en place une politique de prévention.

L'entreprise peut également envisager d'engager une action pénale en déposant une plainte contre personne non dénommée devant le procureur de la République territorialement compétent. En effet, ce type d'attaques peut notamment constituer les infractions d'accès et de maintien dans un système de traitement automatisé de données. Le procureur de la République a trois mois à compter du dépôt de la plainte pour faire part de sa décision à la victime : il peut classer la plainte sans suite, ouvrir une enquête préliminaire, ou bien adresser la plainte à un juge d'instruction afin que celui-ci ouvre une procédure d'instruction.

Après le dépôt de plainte, il est indispensable d'anticiper la déperdition de preuves. L'entreprise doit alors conserver une copie du système en se mettant en relation avec un huissier territorialement compétent, qui pourra réaliser un constat dans les plus brefs délais. Cet huissier pourra être assisté par un expert informatique.

Il a été constaté que les entreprises restent discrètes sur ce type d'attaque pourtant de plus en plus répandues. Toutefois, il est important pour l'entreprise de communiquer en interne sur l'évènement et réagir très rapidement pour éviter toute diffusion d'information erronée ou inexacte.

http://www.it-expertise.com/phreaking-quand-les-pirates-sattaquent-aux-lignes-telephoniques/

En conclusion, face à l'augmentation des attaques de type phreaking, il devient impératif pour les entreprises de vérifier les stipulations du contrat les liant à leur opérateur de télécommunications et à leur intégrateur et de mettre en œuvre une politique de prévention efficace, comprenant une surveillance attentive du trafic pour détecter les attaques et les intrusions, un contrôle régulier de la facturation et l'audit du système informatique par des professionnels.

Virginie Bensoussan-Brulé
Directeur du département Pénal numérique

Alain Bensoussan-Avocats est un cabinet d'avocat entièrement dédié au droit des technologies avancées depuis 1978. Pour la 4e année consécutive depuis 2010, il a été distingué par ses pairs, « Best Lawyer » de l'année en « Droit des Technologies ».
Site : **http://www.alain-bensoussan.com/**

http://www.it-expertise.com/phreaking-quand-les-pirates-sattaquent-aux-lignes-telephoniques/