



Très actif dans la lutte contre le phreaking, l'opérateur Open IP a ouvert un site dédié à l'information et aux parades contre le piratage.

Piratage : peu d'entreprises souhaitent témoigner

Par crainte de diffuser une mauvaise image, les entreprises victimes de piratage ne sont pas très enclines à faire part de leur expérience. Pourtant, les exemples commencent à être assez nombreux et concernent tout type d'entreprises (petites et grandes), dans divers secteurs d'activité (public comme privé). Même les établissements scolaires peuvent être concernés, puisqu'un lycée de Lannion s'est fait pirater pour 12 000 € en un week-end. « Pour notre part, nous en avons été de 3000 € de notre poche lorsque nous avons été victimes de piratage fin 2010 », explique Damien Cheminaud, responsable administratif de l'Espace Papeterie à

Limoges, « c'est France Telecom qui nous a alerté le lundi matin ». Après avoir porté plainte, l'entreprise a tout de même obtenu un dédommagement de 900 €. Lionel Fruh, PDG de Gerfran Bouteilles à Marmande, a lui aussi été informé par l'opérateur historique que son PBX avait été piraté, comme il le dit dans son témoignage publié sur le site www.SOS-piratage.com. Dans son cas, 3000 appels frauduleux avaient été passés à destination du Zimbabwe pour un total de 6500 €. La société avait dû payer. Depuis, elle a fait bloquer toutes les destinations téléphoniques avec lesquelles elle ne travaille pas. Un exemple à suivre !

tel-Lucent est aujourd'hui l'équipementier le plus attaqué, ce qui s'explique en partie par sa position de numéro 1 sur le marché, Cisco et Siemens suivent derrière, en revanche Aastra n'a eu à déplorer aucune attaque alors qu'il dispose d'une part de marché conséquente ».

Les pirates à l'abri, les opérateurs en première ligne

L'appât du gain constitue sans conteste la première motivation des pirates puisque les capacités de communication détournées peuvent être revendues à des opérateurs et qu'une partie du trafic piraté est directement routée vers des numéros surtaxés dans des pays étrangers. Cette motivation première est renforcée par le fait que la manœuvre ne présente pas de grandes difficultés techniques et, surtout, pas de gros risque juridique, puisque la quasi-totalité des pirates opèrent depuis l'étranger et ne peuvent être poursuivis. « Nous ne pouvons pas aller chercher les pirates à l'étranger », confirme Anne Souvira, commissaire divisionnaire de la BEFTI (Brigade d'Enquête et Fraudes aux Technologies de l'Information), « par conséquent, nos alternatives à la répression sont l'information et la sensibilisation au fait qu'il est indispensable de mettre en place une politique de sécurité adaptée sur les systèmes téléphoniques ». La BEFTI reconnaît recevoir beaucoup de plaintes sur le sujet, mais la résolution de ces dossiers réclame un gros investissement technique et beaucoup de temps. Toutefois, la brigade spécialisée confirme que les responsabilités peuvent être multiples sur ce type d'affaires. « Les opérateurs ont aussi un rôle à jouer, ils ont d'ailleurs vraiment intérêt à ce que ce fléau se

résolve car ce sont tout de même eux qui payent le plus souvent les factures du trafic piraté », explique Anne Souvira, « j'ai d'ailleurs rencontré récemment Bouygues Télécom, qui a décidé de revoir ses contrats afin de les rendre plus explicites, une manière de se couvrir ».

S'il est un opérateur qui a vraiment pris le sujet à bras le corps, c'est bien Open IP. En effet, ce dernier s'est lancé dans une démarche d'information tous azimuts vis-à-vis de ses clients. Open IP a même mis en ligne un site dédié au sujet (www.sos-piratage.com) afin de prévenir et surtout de conseiller les entreprises sur la conduite à tenir. Pourquoi un tel activisme ? Tout simplement parce que l'opérateur a été victime de piratage en 2008. A l'époque, en un seul week-end, 18 000 appels frauduleux ont été passés à son insu pour un préjudice s'élevant à 65 000 €. « Mais il faut clairement dire que les tentatives de piratage sont continues », explique Laurent Silvestri, PDG, « sur nos 1 800 entreprises clientes, 150 ont déjà été attaquées et nous les avons protégées ». En effet, depuis sa mésaventure, Open IP réalise des tests de sécurité quotidiennement sur son réseau.

La sensibilisation, première protection

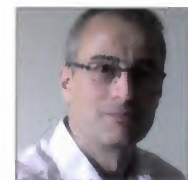
« Il existe deux types principaux de phreaking », explique Laurent Silvestri, « le premier mode de piratage consiste à entrer dans un système téléphonique par la messagerie vocale, le second consiste à traverser le firewall protégeant une solution de ToIP ». Et il est incontestable que le premier piratage est aujourd'hui à la portée de tout le monde. En effet, pour se connecter à la messagerie vocale d'un poste, il suffit d'en composer le numéro et de taper les 4 chiffres du code confidentiel qui, malheureusement, ne sont que très rarement personnalisés par les entreprises (ainsi les codes 0000 et 1234 permettent très souvent à n'importe qui d'accéder aux fonctionnalités de la messagerie). Fort de cette facilité, les pirates activent le renvoi d'appel vers des numéros surtaxés à l'étranger (serveur de jeux et serveurs de services pornographiques dans la grande majorité des cas). L'accès à distance aux fonctionnalités des postes téléphoniques permet aussi aux pirates de surnuméroter et ainsi d'appeler les destinations de leur souhait.

Il n'est pas beaucoup plus difficile de passer au travers d'un firewall censé protéger une installation de ToIP. En effet, sur ce type de configurations, des postes sont connectés en RJ45 sur la plate-forme de communication et sont authentifiés à l'aide d'identifiants traditionnels (login et password). « Mais de plus en plus de PC sont égale-



LAURENT SILVESTRI, PDG D'OPEN IP

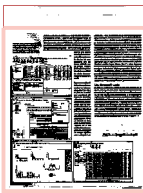
« Les tentatives de piratage sont continues, sur nos 1 800 entreprises clientes, 150 ont déjà été attaquées et nous les avons protégées (...) Il existe deux types principaux de phreaking, le premier mode de consiste à entrer dans un système téléphonique par la messagerie vocale, le second consiste à traverser le firewall protégeant une solution de ToIP ».



STÉPHANE VALETTE, DIRECTEUR GÉNÉRAL DE CHECKPHONE

« [Le firewall ETSS] permet d'envoyer des alertes ou de couper les flux automatiquement en cas de comportement d'appel suspect, par conséquent toutes les tentatives de piratage sont déjouées ».





Définir une politique de sécurité poste par poste, auditer l'existant, créer ensuite des rapports, une politique efficace de lutte contre le piratage, passe à la fois par des outils et par des procédures, une bonne combinaison des deux permettant d'atteindre une certaine efficacité.

ment connectés à ces installations pour éviter les coûts de câblage », explique Laurent Silvestri, « et comme les PC ont accès à Internet, les pirates peuvent entrer sur le réseau, trouver le login/password d'un téléphone, tester des adresses IP à l'aide d'un automate et trouver celle qui répond au port 5060 (port utilisé par le SIP, ndr), ensuite ils peuvent faire absolument ce qu'ils veulent ». Ils vont alors le plus souvent chercher à faire transiter des milliers de communications vers différentes destinations.

Une capacité de trafic qui sera alors revendue à des opérateurs. En effet, les très petits opérateurs sont des clients privilégiés pour les pirates télécoms (d'ailleurs, il arrive que certains d'entre eux achètent des minutes de communication piratées sans le savoir).

Dans ce contexte, Open IP n'a donc cessé de communiquer sur les bonnes pratiques qu'il faut mettre en place sur le marché pour se prémunir des risques de phreaking. « Premièrement, les équipementiers doivent transmettre toutes les informations nécessaires aux installateurs-intégrateurs (faibles de sécurité et mesures à prendre), dans un deuxième temps les intégrateurs doivent fermer les firewalls de leurs clients et informer les entreprises sur le fait qu'elles doivent personnaliser les identifiants et les changer régulièrement », récapitule Lau-

rent Silvestri, « mais les opérateurs doivent aussi mettre à disposition de leurs clients des outils permettant de fixer des limites d'utilisation et de consommation ». En effet, le principal objectif à poursuivre n'est pas de chercher la solution miracle qui permettrait de bloquer complètement les pirates dans leurs tentatives de rentrer dans les plates-formes téléphoniques car, malheureusement, il semble qu'ils auront toujours la possibilité de trouver un moyen pour parvenir à leurs fins (notamment avec l'usage d'automates qui permettent de trouver les codes). Mais il s'agit bien de limiter les conséquences des éventuels piratages. « Ainsi, en limitant les capacités d'appels des entreprises, qui n'ont à priori aucune raison de passer des appels vers des pays avec lesquels elles ne travaillent pas, on réduit de manière considérable les préjudices financiers », explique Laurent Silvestri. Open IP a mis en place cette limitation des capacités d'appel au bénéfice de ses propres clients, en restreignant les destinations téléphoniques possibles. En plus, l'opérateur teste régulièrement la sécurité de leurs installations et analyse leurs comportements de communication afin de détecter d'éventuelles répétitions d'appels vers des destinations surprenantes. « Au cours de ce premier trimestre 2012, nous allons également proposer à nos clients de fixer des paliers de limites de consommation », ajoute Laurent Silvestri.

Un firewall voix

Parallèlement, certains acteurs ont mis sur le marché des gateways, ou des firewalls voix, destinés à assurer la protection des plates-formes de communication. Ce type de solutions représente un petit investissement pour les PME, mais peut certainement apporter un niveau de sécurité supplémentaire. Checkphone, notamment, vient de lancer un firewall voix, baptisé ETSS (Expert Telecom Security System), spécialement adapté pour lutter contre le piratage téléphonique. « Il s'agit d'un boîtier à placer entre le lien opérateur et le PBX du client, tout le trafic voix passe alors par le firewall qui applique les politiques de sécurité adoptées par l'entreprise », explique Stéphane Valette, directeur général, « ce type de solutions permet d'envoyer des alertes ou de couper les flux automatiquement en cas de comportement d'appel suspect, par conséquent toutes les tentatives de piratage sont déjouées ». Du moins faut-il l'espérer !

