Christophe Leroy (Telindus) : « Le piratage téléphonique est appelé à se développer »

« Les entreprises n'ont pas encore pris en compte la sécurité de leurs solutions de VoIP/ToIP et des smartphones, car elles n'ont pas conscience des risques que cela pose pour leur système d'information. » Et pourtant, selon **Christophe Leroy**, directeur du Security Research Center de la SSII Telindus (filiale de Belgacom depuis 2006), la menace « phreaking » est bien réelle.

Le responsable rapporte ainsi la mésaventure d'un client de 150 employés qui dépensait 20.000 euros par mois en factures téléphoniques d'appels pirates vers l'étranger. Souvent, ces entreprises demandent à leur opérateur de passer l'éponge, ce que ces derniers font généralement de mauvaise grâce.

« Un grand groupe de téléphonie réfléchit avec nous comment accompagner leurs clients victimes, souligne le dirigeant. *Il chiffre le phénomène à 7 millions d'euros par an pour lui. »* Rien que sur l'Île-de-France, Christophe Leroy estime à plusieurs millions d'euros les conséquences annuelles des attaques des réseaux téléphoniques des organisations.

Apparu dans les années 60, le phreaking (ou piratage téléphonique) a pris une nouvelle ampleur ces dernières années avec les réseaux informatiques. Avec divers objectifs de la part des attaquants qui vont du détournement d'appel depuis les boîtes vocales aux tentatives de pénétration du SI en passant par l'espionnage pur et simple des communications. Avec des conséquences potentiellement considérables pour l'entreprise.

Le piratage téléphonique est très démocratisé

« Aujourd'hui, le piratage téléphonique est très démocratisé car, en récupérant des informations confidentielles, la délinquance y voit une source de chantage. Donc de revenus, estime le directeur. *Il y a aussi les hacktivistes qui cherchent à récupérer de l'information, même illégalement. Donc la pratique est appelée à se développer. »*

Les méthodes d'attaques par Internet restent classiques. Les attaquants scannent les plages de ports réseau d'une entreprise, déterminent la présence d'une plate-forme de gestion des appels (call manager) et tentent d'y pénétrer en piratant le compte du gestionnaire principal, souvent par simple saisie du mot de passe testé en série ou en s'appuyant sur une faille système du PABX. Souvent, l'opération est automatisée, effectuée par des robots.

« Dans 80 % des cas, les vulnérabilités sont énormes et simples à corriger. Toute la problématique de mise à jour, de l'infrastructure dédiée, et de la gestion du call manager est en cause. » Une problématique assez proche dans la méthodologie de celle des réseaux informatiques traditionnels mais *« avec des attaques un peu spécifiques »*.

Des missions d’attaque

La problématique avec les smartphones est un peu différente. Elle peut passer par l’installation d’applications compromettantes ou l’ouverture de pièces jointes. Mais aussi par des accès physiques par l’intermédiaire d’un téléphone perdu ou volé configuré avec un accès au SI de l’entreprise. *« Et l’on ne pense pas au fax, modem, photocopieur aujourd’hui installés sur le réseau téléphonique avec les risques d’interception inhérents. »*

Pour répondre à cette problématique de piratage des lignes de communication, le Security Research Center de Telindus a notamment développé… des outils d’attaque. *« Ils sont utilisés dans le cadre de nos missions et pour notre R&D »*, précise Christophe Leroy. Missions qui visent à tester la fiabilité d’un réseau de téléphonie et à en dénicher les failles afin de définir les mesures à prendre pour les combler.

« Composé d’une dizaine de personnes, le Security Research Center est dédié à tout ce qui a trait à l’intrusion, y compris en ToIP/VoIP. Des missions totalement indépendantes des services de Telindus, » insiste le responsable qui se montrera néanmoins discret sur les solutions d’intrusion en question. *« La question de la sécurité doit être abordée de manière globale et la VoIP/ToIP, à ce titre, ne doit pas rester périphérique mais intégrer la problématique IT »*, conclut-il.