Téléphonie IP : la face cachée de la cybercriminalité

Stanislas de Goriainoff, Directeur Technique (CTO) de Sewan

Les entreprises de toutes tailles, et particulièrement les TPE et PME, sont de plus en plus fréquemment la cible de cyberattaques en tout genre. Parmi elles : défiguration de sites Internet, compromission de comptes de messagerie et réseaux sociaux, vol de données sensibles, à caractère personnel, ou encore rançongiciels. Mais dans cet inventaire à la Prévert, on oublie encore trop souvent de citer les malveillances touchant à la téléphonie IP. Insidieuses et récurrentes, mais plus discrètes en ce qu'elles n'impactent pas directement l'image de l'entreprise, elles peuvent néanmoins être très coûteuses pour leurs victimes. Il convient donc de considérer pleinement ce risque et de s'en protéger dès à présent, autant que faire se peut.

Des cyberattaques en évolution constante…

Dans le domaine de la téléphonie IP comme dans d'autres, les cyberattaques évoluent constamment, le plus souvent au rythme des changements réglementaires et des modèles tarifaires. Le hack le plus classique consiste ainsi à réaliser un transfert d'appel vers un numéro surtaxé. Ce fut le cas pour les téléphones satellites dans un premier temps, puis pour les numéros internationaux. Or, dès lors que les opérateurs bloquent ces cibles spécifiques, les hackers ne mettent pas longtemps pour se déporter sur un autre service. Ainsi depuis plus d'un an maintenant, les attaques en la matière se concentrent principalement sur les numéros payants en « 08 », aussi appelés numéros SVA (Service à Valeur Ajoutée). Ouvrant un numéro SVA en ligne depuis un site français puis le clôturant rapidement, après avoir néanmoins généré un revenu conséquent, ces pirates sont malheureusement difficilement traçables. Cette technique préférant les numéros tarifés à l'appel plutôt qu'à la minute, qui sont eux modérés par les opérateurs au-delà d'un certain seul, s'avère très lucrative au regard du volume d'appels générés: les entreprises victimes peuvent ainsi voir leur facture téléphonique mensuelle gonfler de 3000€ à 5000€ supplémentaires ! Et il leur est alors bien difficile de se retourner contre leur opérateur ou de s'adresser à leur assurance, en ce que ces appels ont effectivement été passés. La responsabilité de s'être fait hacker leur équipement par négligence leur incombe, pouvant alors entraîner d'importantes difficultés de trésorerie…

Mais comment une telle négligence peut être si courante ? Sur les installations professionnelles type IPBX, les petits équipements comme les lignes téléphoniques sont par nature peu sécurisés, le plus souvent à l'aide de mots de passe génériques connus des constructeurs et que les installateurs ne pensent pas toujours à changer. Le cas échéant, une attaque par force brute (visant à tester les différentes combinaisons possibles) aboutit alors rapidement à l'obtention d'une clé d'accès. Par ailleurs, une entreprise peut être exposée en cas d'erreur de manipulation lors des opérations de maintenance à distance. En supprimant une brique de sécurité et en rendant un poste visible pour s'en faciliter l'accès, l'agent de maintenance fait ainsi naître une faille dans laquelle s'engouffrent facilement les acteurs malveillants. Il est donc essentiel pour les entreprises d'appliquer au plus vite des bonnes pratiques de sécurité en la matière, ce pour se prémunir d'attaques potentielles aujourd'hui… mais aussi demain ! Car une chose est sûre : ces attaques seront sans cesse renouvelées à l'avenir. La future cible de ces cybercriminels pourrait en effet être les SMS surtaxés, à l'instar de ceux utilisés par les émissions TV, à moins qu'un nouveau service payant pense légitimement son business model autour de la téléphonie d'ici là, et ne se fasse rapidement détourner…

… contre lesquelles il convient de se prémunir !

De nos jours, il ne viendrait à l'idée de personne de donner un accès direct à un poste informatique. Ce dernier est toujours à minima protégé par un processus de modification des adresses IP et des ports sources et de destination, appelé NAT (Network Address Translation), et au mieux par un *firewall*. Or, ces logiques ne semblent pas être encore pleinement entrées dans les mœurs des entreprises - notamment des TPE et PME - en matière de téléphonie IP. Pourtant, il convient d'appliquer dans ce domaine aussi les règles de bonnes pratiques et de sécurité que l'on adopterait pour l'informatique bureautique. La clé de sécurité réside ici dans le fait de bien comprendre l'usage de ses collaborateurs utilisateurs en amont, de sorte à appliquer le plus efficacement possible la règle du moindre privilège. Autrement dit, sans certitude quant au besoin avéré d'un service, il est préférable de l'interdire. Reprenons l'exemple des annuaires SVA : si les numéros en « 0890 », correspondant à la voyance et aux jeux, doivent être bloqués de base, ils convient en sus de mettre en place une règle la plus restrictive possible au démarrage, quitte à ouvrir ensuite le champ des possibles à certains numéros au cas par cas si nécessaire. Côté opérateurs, il est par ailleurs essentiel d'instaurer un mécanisme d'analyse préventive ou prédictive, de sorte à connaître les flux de départ et d'arrivée des diverses communications, notamment lorsqu'un grand nombre d'appels arrivent sur un même numéro depuis la même source. Enfin, si l'aspect réglementaire est strict concernant les numéros SVA, ces derniers pouvant être acquis uniquement par des sociétés françaises, c'est leur achat via internet qui permet aujourd'hui cette fraude de masse. Il convient alors à l'État de jouer son rôle régalien en faisant rigoureusement appliquer cette réglementation.

De tous temps, la téléphonie a été la cible de cybercriminels (on se souvient encore de l'exemple des *blue box* dans les années 1980). Elle le sera encore à l'avenir, via des moyens sans cesse repensés, d'autant plus que son usage est devenu un indispensable, ancré au cœur de nos modes de vie et de travail. Quoi qu'il en soit, ce sujet ne peut plus être invisibilisé. Opérateurs télécoms, distributeurs, intégrateurs, installateurs, fournisseurs d'accès, il en est de notre responsabilité commune, ce pour la bonne santé de notre tissu économique français !

Une tribune publiée en exclusivité par le JDN.