La Chambre Monégasque des NT

Parution du Guide des Bonnes Pratiques : "Comment se prémunir des fraudes téléphoniques (phreaking) ?"

Chaque année, une dizaine d'entreprises monégasques sont victimes de fraudes téléphoniques, qui leur ont coûté cher, parfois jusqu'à des dizaines de milliers d'euros. Cette pratique frauduleuse appelée "phreaking" est techniquement simple : le pirate s'introduit sur le réseau interne de l'entreprise, via des connections internet ou des lignes téléphoniques, pour émettre des appels vers des numéros surtaxés ou certains numéros étrangers. Son but est de récupérer une partie du coût de la communication que l'entreprise doit payer, généralement sans espoir de retrouver les coupables.

Cette fraude est beaucoup moins connue des entreprises, et parfois moins stratégique, que le piratage informatique. Aussi, elles s'en protègent moins, ce qui facilite l'action des pirates.

Pour sensibiliser les entreprises, principales victimes de ces attaques en recrudescence, la Chambre Monégasque des Nouvelles Technologie a édité un Guide des Bonnes Pratiques. Rédigé par des représentants des installateurs de réseau téléphonique en collaboration avec l'opérateur de télécommunications de la Principauté, il passe en revue tout ce qu'il faut savoir pour réduire les risques de fraudes, et le cas échéant en diminuer l'impact financier.

Pour mieux en saisir les enjeux, le MBN a interrogé deux rédacteurs du Guide : Jean-Louis Oustrières, Responsable du Projet, Vice-président de la Chambre, et Administrateur de MES-I2S-C2S, et Martin Péronnet, Conseiller au Bureau Syndical de la Chambre, et Directeur Général de Monaco Telecom.

MBN/ ***En quoi consiste la fraude dite "PABX"* ?***

Jean-Louis Oustrières : Les hackers s'introduisent dans l'installation téléphonique et vont programmer les téléphones pour appeler soit des destinations exotiques, soit des numéros surtaxés. L'attaque en elle-même se fait soit par une prise en main du réseau IP de l'entreprise, auquel est raccordé le réseau téléphonique, soit par la prise de contrôle du serveur téléphonique, notamment en profitant de mots de passe non sécurisés. Le pirate bénéficie de la réversion des coûts par l'opérateur étranger final.

MBN/ ***Ces attaques sont-elles fréquentes ?***

J.-L.O. : On a vu en 2016 une recrudescence de ces attaques, notamment une multiplication des attaques à petits montants. Pour passer inaperçues, celles-ci se font plutôt la nuit ou le week-end, et ciblent les PME qui ont des relations à l'international. Le problème est que la sensibilisation au risque de piratage du réseau informatique s'est traduite par une mise de côté du risque présenté par le réseau téléphonique.

MBN/ ***Comment peut-on s'en protéger ?***

J.-L.O. : Il y a deux choses à faire absolument : configurer le PABX avec un mot de passe solide (ne surtout pas laisser celui d'origine) et le mettre à jour en appliquant les updates fournis par les fabricants, voire en changeant son système téléphonique s'il est trop ancien. Il faut donc bien vérifier son contrat d'entretien auprès de l'installateur. On peut aussi augmenter son niveau de protection en limitant les droits des postes, par exemple que seuls certains soient autorisés à passer des appels internationaux, ou seulement à certaines heures.

MBN/ ***Quels sont les moyens mis en place par Monaco Telecom ?***

Martin Péronnet : En préventif, nous ne pouvons rien faire car nous ne contrôlons pas les accès aux systèmes d'information des entreprises. En curatif, nous avons par contre mis en place des processus de lutte contre la fraude, qui analysent en temps réels les "anomalies" (par quantité et destination) dans les comportements d'appels de nos abonnés. Lors de suspicion de fraude, nous prévenons les clients, ou coupons les flux en cas de non réponse de leur part. Cette détection et ces règles de gestion permettent de limiter considérablement les impacts, mais ils ne les annulent pas puisque la faille de sécurité se trouve au niveau de l'installation téléphonique des entreprises.

MBN/ ***Que prévoit la loi pour protéger les victimes ? Est-il possible de s'assurer ?***

M. P. : Ce type d'attaques peut constituer des infractions d'accès et de maintien frauduleux dans un système d'information, ou d'altération frauduleuse de données informatiques selon le cas, sanctionnées pénalement à Monaco. La récente Loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la Criminalité Technologique renforce en effet la caractérisation du délit en le sanctionnant d'une peine de prison ou d'une amende. Il reste indispensable de porter plainte, afin de permettre l'ouverture d'une enquête et d'activer la police d'assurance éventuellement souscrite pour couvrir les frais liés à cette attaque. Il est toutefois souvent difficile de remonter aux auteurs, qui agissent en général de pays étrangers et de façon masquée. Obtenir réparation est donc délicat. Concernant l'assurance, de nouveaux contrats peuvent viser plus spécifiquement les conséquences des attaques cyber, celles liées aux fraudes PABX. Mais, elles prévoient également que l'entreprise fasse un minimum pour se protéger, et il peut être plus compliqué d'obtenir un dédommagement si elle a laissé par exemple des mots de passe usine sur un PABX, ou n'a pas effectué d'audit régulier de son système. ■

Pour en savoir plus, le guide complet est téléchargeable sur le site web www.chambre-nt.mc

*PABX (Private Automatic Branch Exchange) : Il s'agit d'un commutateur téléphonique privé utilisé dans les entreprises. Les utilisateurs d'un réseau téléphonique basé sur un PABX partagent un nombre de lignes externes pour effectuer des appels vers l'extérieur de la société.