Sécurité économique territoriale
Rhône-Alpes

MESSAGE D'ATTENTION
PIRATAGE DE SERVEUR TÉLÉPHONIQUE (Phreaking)

Fin août 2014, à l'issue d'un week-end, une entreprise implantée en région Rhône-Alpes constate que son serveur téléphonique a été piraté.

Plusieurs centaines d'appels ont été émis essentiellement à destination de l'Afrique. Le préjudice est estimé à environ 12 000 €uros hors taxes.

DE QUOI PARLE-T-ON ?

Si la protection du système informatique a été prise en compte par nombre d'entreprises, il en va tout autrement pour la téléphonie professionnelle, qui elle ne bénéficie bien souvent d'aucune attention particulière.

Le piratage de serveurs téléphoniques, communément appelé « *phreaking* », consiste en l'exploitation des failles des infrastructures téléphoniques dans un but malveillant. Dans la plupart des cas, il s'agit d'attaques des messageries vocales permettant l'activation des fonctions de renvoi d'appels vers des pays étrangers.

Le piratage du standard suite à la détection d'une brèche dans le pare-feu ou la prise de contrôle à distance de l'interface d'administration est également utilisé.

Toute entreprise, quelle que soit sa taille, son type d'organisation (*mono-site ou multi-sites*) **ou son modèle d'installation téléphonique, est concernée par ce type de fraude. Des dizaines, voire des centaines de milliers d'euros peuvent ainsi leur être indûment facturées et mettre en jeu leur pérennité.**

Très rémunérateur, ce marché est appelé à se développer surtout au préjudice des TPE / PME, moins bien équipées et peu informées pour y faire face.

A noter que ces appels ont généralement lieu le week-end, la nuit et/ou les jours fériés afin de ne pas éveiller trop rapidement les soupçons.

QUE FAIRE ?

Les conséquences de telles attaques pouvant avoir un impact catastrophique sur le fonctionnement de l'entreprise, il convient donc d'y apporter une attention particulière en amont. Ainsi, pour limiter les risques, il est conseillé de :

- **➥ *Contacter en premier lieu* l'installateur en vue de réaliser un *audit du système téléphonique* et prendre ensuite les mesures idoines en vue de le sécuriser ;**
- **➥ *Paramétrer les indicatifs internationaux* pour interdire les appels vers certaines destinations étrangères inutiles au fonctionnement quotidien de la société ;**
- **➥ *Verrouiller les lignes sortantes* durant les périodes d'inactivité de l'entreprise** (*nuits, week-ends, jours fériés, vacances, …*) **et *désactiver* les fonctions inutiles ;**
- **➥ *Mettre en place,* en collaboration avec l'opérateur de téléphonie, un système de prévention permettant de détecter en temps réel toute surconsommation d'appels vers l'étranger ;**
- **➥ *Faire changer périodiquement les clés sécurisées* d'accès au modem du serveur téléphonique et les *mots de passe* des comptes de messagerie vocale des salariés ;**
- **➥ *Déconnecter le modem de télé-maintenance*** (*si possible*) **et ne le remettre en fonction que sur demande de votre opérateur ou à minima *sécuriser l'accès à la maintenance* ;**
- **➥ *Sensibiliser régulièrement les salariés* notamment quant à la *diffusion d'informations* sur les réseaux sociaux concernant l'architecture télécom, lesquelles peuvent orienter les recherches d'éventuels pirates et augmenter ainsi le risque d'intrusion et leur rappeler l'importance du *secret des identifiants* de messagerie ;**
- **➥ Et bien sûr, *intégrer la téléphonie dans la politique de sécurité du système d'information* de l'entreprise.**

En cas de problème avéré ou de simple tentative :

***Déposer rapidement plainte* auprès du service de police ou de gendarmerie territorialement compétent.**

Lettre électronique N° 3 éditée par la région de gendarmerie de Rhône-Alpes – 36 bd de l'Ouest – 69580 Sathonay-Camp - ☎: 04.37.85.21.00
Rédaction : Cellule Intelligence Économique régionale