FRAUDE TÉLÉPHONIQUE : DES RÈGLES ESSENTIELLES POUR PROTÉGER SON ENTREPRISE DE CETTE MENACE

Écrit par La rédaction (/web/actu-technologies/author/633-laredaction) jeudi, 03 novembre 2016 16:54
Taille de police

Actu Technologies (/web/actu-technologies)

Face à la multiplication des cas de piratage téléphonique qui touchent au quotidien les entreprises françaises, la Fédération EBEN vous propose de suivre les préconisations ci-dessous élaborées dans le cadre des ateliers entreprises de l'ARCEP. Il s'agit d'adopter les bons réflexes afin de protéger vos systèmes téléphoniques de ces attaques qui peuvent constituer de véritables menaces pour la survie de vos structures.

Savez-vous que le coût de ce type de fraude s'élève généralement à plusieurs milliers d'euros voir plusieurs dizaines de milliers, dans les cas les plus importants ? Il ne suffit que de quelques heures, souvent durant les weekends, mais pas toujours, pour qu'un pirate détourne une ou plusieurs lignes téléphoniques afin d'émettre un grand nombre d'appels par le biais de « systèmes automatisés » vers des numéros surtaxés situés hors de l'hexagone. Ce sont donc des centaines d'appels qui sont alors facturés aux victimes propriétaires de la ligne détournée.

L'ensemble des structures peut être concerné : entreprises (quelle que soit la taille), administrations, indépendants, organismes divers…

Les règles essentielles* pour sécuriser vos systèmes téléphoniques :

- Il vous incombe de modifier dès l'installation et de manière régulière **l'ensemble des mots de passe**. Ceux-ci doivent être complexes

- Nommez une personne au sein de votre entreprise formée aux procédures de changement des mots de passe ou une personne par service selon la taille de votre structure.

- Sécurisez et isolez votre serveur téléphonique dans un espace dédié et dont l'accès est restreint (fermé et accessible seulement aux personnes habilitées) comme vous le feriez pour vos serveurs informatiques.

- Les flux VOIX et les flux DATA doivent transiter par deux réseaux distincts.

- Votre intégrateur a un devoir de conseil et de mise en garde à votre égard, définissez donc avec lui une politique de gestion des communications dans votre entreprise avec une **définition des niveaux de service par utilisateur.**
Par exemple :
- boîte vocale simple avec enregistreur ou assistance personnelle ;
- choisissez le renvoi d'appel vers l'extérieur uniquement si cela est nécessaire pour l'utilisateur ;
- si votre activité ne nécessite pas d'appeler à l'étranger, optez plutôt pour un accès national.

- Les constructeurs mettent régulièrement à jour la politique de sécurisation de leurs produits, choisissez **un niveau de contrat qui intègre ces évolutions.**

- Sécurisez également vos systèmes pendant les heures ouvrables par des moyens complémentaires. Par exemple, installez un logiciel de scrutation des lignes et de gestion des VOIX qui vous permettra de surveiller en temps réel l'activité de vos systèmes (appels entrants, sortants et émis en interne).

- Questionnez votre opérateur pour savoir si votre contrat est éligible à une analyse de vos flux VOIX qui inclurait **la possibilité de couper, notamment en heures non ouvrables, les communications lors d'appels émis vers des destinations anormales** ou en rafale sur des numéros surtaxés.

- Vos partenaires (opérateur, intégrateur ou installateur) sont régulièrement amenés à vous informer ou vous alerter sur la sécurité de vos systèmes, restez vigilant quant à ces communications (courriers, mails…). N'hésitez pas aussi à leur poser vos questions.

* Cette liste est fournie à titre non exhaustif et est susceptible d'évoluer en fonction de la loi et de la jurisprudence

La rédaction (/web/actu-technologies/author/633-laredaction)