Sécurité des services télécoms

La présente fiche concerne plus particulièrement la façon de se protéger contre l'usage incontrôlé des services de communication électronique professionnels et fait mention des risques de fraudes associés.

1 Le contexte

Les services de communication électronique vont du simple service téléphonique aux services délivrés via Internet les plus sophistiqués (Cloud). Les menaces sont de différentes natures selon les services et le terminal. Leurs modalités sont bien distinctes et les contre-mesures doivent par conséquent être appropriées.

2 Les risques

Les risques qui engendrent une surfacturation ne sont pas nécessairement les plus graves :

2.1 Risques financiers

Ces risques sont ceux soit d'une augmentation des frais facturés par l'opérateur, soit d'une attaque de type ransomware consistant à paralyser les communications électroniques jusqu'au versement d'une rançon.

2.2 Risques concernant la sécurité

Notamment :

- Usurpation d'identité
- Attaques virales du système (virus, vers, chevaux de Troie …)
- Destruction ou altération des données
- Altération de fichiers (annuaire, boites vocales)
- Spam sur les messageries vocales
- Recomposition des messages vocaux
- Modification des données de programmation
- Déni de service (DOS)

2.3 Risques concernant la confidentialité

Notamment :

- Interception et enregistrement des conversations
- Écoute téléphonique
- Écoute des boites vocales
- Écoute des conversations dans les bureaux

2.4 Risques juridiques

Aux yeux de la loi, l'entreprise est considérée comme responsable de la sécurité de ses systèmes d'information et de ses fichiers : elle doit « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ». L'entreprise doit tout mettre en œuvre pour éviter le détournement de données à caractère personnel comme celles que peut contenir un annuaire par exemple. En cas de faille de sécurité, celle-ci doit être notifiée aux autorités. Le risque juridique à ne pas le faire est une condamnation civile mais peut aussi être une condamnation pénale.

En outre, l'intrusion dans un système informatique peut provoquer des communications de type harcèlement ou plus généralement répréhensibles dont la responsabilité serait alors imputable au titulaire de l'installation.

Il est à noter que le règlement européen connu sous le nom de **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679) qui doit prendre effet le 25 mai 2018 prévoit de lourdes sanctions (jusqu'à 20 millions d'€ et 4% du CA) pour les entreprises qui faute d'avoir pris les mesures appropriées auraient compromis les données personnelles.

3 Application aux services téléphoniques

- Communications téléphoniques à l'insu de l'utilisateur vers des numéros hors forfait ;
- Altération de fichiers (annuaire, boites vocales) ;
- Recomposition du message d'accueil de la messagerie vocale ;
- Écoute des boites vocales ;
- Spam sur les messageries vocales ou les SMS ;
- Écoute téléphonique.

3.1 Sans intrusion :

L'application la plus fréquente, qui ne résulte généralement pas d'une intrusion, consiste à inciter par divers moyens (par ex. appel depuis un numéro surtaxé prématurément interrompu) l'utilisateur à passer des communications vers des numéros surtaxés dont le fraudeur encaisse la partie surtaxée. Toutefois, ces communications peuvent aussi être le résultat de complicités internes donnant accès à des tiers par transfert d'un poste de l'installation vers l'extérieur ou établissement de communications de longue durée de numéros surtaxés depuis un poste interne.

3.2 Avec intrusion :

Les installations téléphoniques actuelles sont des équipements informatiques plus ou moins complexes allant d'une simple box à des autocommutateurs (PABX ou IPBX) incluant de multiples services et, comme tels, peuvent faire l'objet de piratages propres

à ce type de systèmes (Phreaking). La plus classique de ces intrusions s'effectue en utilisant à l'insu du titulaire ses identifiants et mots de passe d'accès à l'administration du système, à l'espace client ou à l'accès distant à la messagerie vocale. Ces identifiants et mots de passe peuvent être obtenus par des complicités internes, parce qu'ils n'ont pas été convenablement protégés ou plus simplement parce que les valeurs par défaut n'ont pas été modifiées.

4 Application à l'informatique

L'objet n'est pas ici de se substituer aux spécialistes de la cybercriminalité mais de rappeler les principales modalités d'attaque et leurs conséquences. Dans ce domaine, l'essentiel des conséquences est le résultat :

1. d'introduction de virus par des pièces jointes corrompues de mails ou de fichiers contenus dans un PC portable, un smartphone ou une clé USB, visant à corrompre les fichiers locaux ou à mettre le réseau local hors service (éventuellement avec demande de rançon pour y mettre fin) ;
2. d'attaques plus sophistiquées par des portes dérobées dans le même but ;
3. d'attaques de type déni de service consistant à lancer un flot de requête vers les accès informatiques en vue de les saturer ;
4. de vol de données afin de dérober des secrets de fabrication ou des données concurrentielles (fichiers clients, propositions commerciales, etc. Contrairement aux précédents, la caractéristique de ces délits est la discrétion.

5 Quelles dispositions pour éviter les attaques de ce type

- Modifiez régulièrement les mots de passe d'accès à l'administration du système, à l'espace client ou à l'accès distant aux messageries vocales. Dans ce cadre appliquez les recommandations de la CNIL là où c'est pertinent.
- Sécurisez l'accès à votre système téléphonique en l'isolant dans un local dédié et protégé.
- Demandez à votre installateur de faire les mises à jour régulières de vos équipements (À prévoir dans le contrat). En effet, ces mises à jour bloquent les failles de sécurité au fur et à mesure qu’elles sont découvertes par le constructeur.
- Pour les PABX IP, faites mettre en place les outils permettant de bloquer les piratages classiques (firewall sur le port SIP 5060, etc.).
- Interdisez les appels vers les numéros surtaxés ou les destinations internationales n'ayant aucun lien avec l'activité de l'entreprise. Les appels les plus détournés étant souvent en direction de Taiwan, Somalie, Cuba, Iles Caïmans, Estonie, Corée du Nord, Azerbaïdjan, Slovénie, Afghanistan, Global Satellite, Globalstar, Égypte, Nigeria, Togo, Sri Lanka, Bénin, Éthiopie, si vous

n’avez pas besoin d’appeler vers ces destinations, supprimez ou demandez à votre installateur de supprimer l’accès à celles-ci.
- N'activez que des options nécessaires au poste de l'utilisateur (en particulier : messagerie vocale, accès à distance, renvoi d'appel).
- Demandez à votre opérateur de téléphonie fixe de mettre en place une alerte quotidienne en cas de surconsommation, en particulier vers les destinations internationales.

Votre installateur ou votre opérateur diffuse régulièrement des informations sur la sécurité des systèmes : lisez-les attentivement, elles peuvent vous aider à leur demander de mettre en place des protections complémentaires :

- Grâce à des logiciels de protection adaptés, les appels peuvent être enregistrés et les appels non-autorisés décryptés.
- Définir des niveaux de sécurité minimaux afin de rejeter automatiquement les mots de passe qui n’ont pas le niveau minimal de **robustesse**[1] requis.
- Fixer un nombre limité de tentatives d’identification par mot de passe. Un moyen supplémentaire de contrer les tentatives de connexion à répétition des hackers. Une fois le nombre limite atteint, les adresses de connexion sont bloquées.
- Définir un nombre limité d’appels simultanés de façon à éviter un grand nombre d’appels sortants.