Les synthèses du CLUSIF

PABX IP et la Sécurité

Synthèse de la conférence thématique du CLUSIF du 25 avril 2013 à Paris

Olivier Guérin du Clusif annonce que des nouveaux groupes de travail sont en cours de création : « Sécurité SCADA » (dans le cadre de travaux communs avec l'ANSSI) et un autre sur les vulnérabilités.

Lazaro Pejsachowicz, Président du Clusif, rappelle que le Clusif a déjà publié un premier document sur la sécurité de la téléphonie il y a huit ans puis un second, plus récent et centré sur l'IP. Or même si on assiste à une sophistication des attaques, les modèles anciens sont toujours d'actualité.

Panorama de la fraude : le point du Ministère de l'intérieur. Ampleur de la menace. Anne Souvira, Commissaire divisionnaire, Chef de la BEFTI (Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information) de préfecture de police.

Outre sa mission d'enquête sur les délits informatiques, la BEFTI (qui couvre Paris et la petite couronne) sensibilise les agents publics et les entreprises.

La fraude est favorisée quand l'organisation n'a pas mesuré les risques juridiques, financiers et techniques et qu'elle n'a pas investi dans la sécurité et formé ses salariés.

L'entreprise doit par exemple veiller aux compétences de son installateur : s'il utilise des mots de passe visibles sur internet c'est qu'il ne gère pas suffisamment la sécurité. Elle doit veiller également à son honnêteté. L'entreprise doit également s'attacher au fonctionnement de son matériel : s'il ne logue pas les entrées et les sorties, il empêche de retrouver la trace des attaques. Elle doit imposer certaines procédures de bon sens : les ports de télégestion doivent être fermés quand on ne s'en sert pas.

Deux modes opératoires principaux caractérisent les fraudes au PABX.

- Le mode technique
  - piratage par l'utilisation des fonctions du répondeur, de l'assistant personnel en activant les renvois d'appels
  - piratage de la console de télégestion.
- Les escroqueries tant grâce à la robotisation des appels en renvoi vers des numéros surtaxés (encaissant des micro-paiements) que par des appels à destination des pays lointains, dont le coût est supporté par le titulaire de l'autocommutateur, etc.

Quand une plainte est déposée, les enquêteurs de la BEFTI cherchent quel est le type de contrat et quel contrôle est prévu sur l'installation. Ils peuvent ensuite auditionner l'installateur. De manière générale, le travail des enquêteurs est facilité si la révélation de la fraude est rapide et si toutes les sauvegardes ont été faites (journalisation des appels poste par poste par exemple).

Si les pirates agissent depuis l'étranger, ils sont difficilement identifiables et, même s'ils le sont, dans la plupart des cas, la BEFTI ne pourra pas procéder à leur arrestation. La répression n'étant pas toujours possible, la

sécurité du réseau téléphonique passe donc bien, avant tout, par la prévention.

En résumé, il est essentiel d'intégrer la sécurité du PABX ou IPBX à la politique de sécurité générale de l'entreprise et de l'intégrer dans un plan de continuité d'activité.

Panorama des risques liés aux solutions téléphoniques et introduction aux mesures de réduction. Marc Lefebvre, Consultant sécurité, Orange.

Concernant les risques sur la téléphonie, les attaquants et leurs motivations sont :

- Le personnel interne (jeu, volonté de nuire, espionnage).
- Le personnel externe (espionnage économique, commerce frauduleux).
- Les évènements externes (incendie, pannes).

Un exemple d'attaque est l'utilisation du système téléphonique comme plate forme pour faire du rebond vers des numéros surtaxés.

La téléphonie sur IP hérite des principales vulnérabilités de la téléphonie numérique : écoutes des conversations, dénis de service, usurpation d'identité, fraudes financières etc. Mais sur cet écosystème « hyperconnecté », de nouveaux risques apparaissent, notamment avec les smartphones et leurs nombreuses applications et le développement du BYOD (*Bring your own device*). Un exemple édifiant, celui du TDos (*Telephony Denial of Service*) qui permet l'envoi massif d'appels sur un téléphone pour en bloquer l'accès.

Pour réduire ces risques, un certain nombre de mesures peuvent être mises en place :

- Renforcement de la sécurité des équipements (contrôles d'accès).
- Cloisonnement entre les flux de données et les flux voix, implémentation de systèmes de sécurité.
- Mise en place d'une gouvernance SSI pour la Voix (audits, mots de passe, mises à jour, etc.).

Concernant la sécurité en mode Cloud (mode centrex IP), il est nécessaire de contrôler l'existence des mesures de sécurité adéquates (chiffrement des données en repos et en transfert, cloisonnement des serveurs téléphoniques, authentification pour les accès internet, protection contre les TDoS, etc.).

En conclusion, la PSSI d'entreprise doit impérativement intégrer la téléphonie sur IP.

Les scénarios d'exploitation, Joffrey Czarny, Chercheur en sécurité informatique, EADS.

Joffrey Czarny cite les menaces suivantes :

- L'écoute des communications téléphoniques :
  Les flux Voix non chiffrés permettent de faire de l'écoute. Or, aujourd'hui, l'infrastructure voix permet facilement le chiffrement et il est donc conseillé de l'installer.
- La manipulation des flux de signalisation (redirection d'appel avec SCCP et vol d'identifiant avec SIP).
- L'écoute des échanges téléphoniques externes : les passerelles VoIP ne sont pas de simples routeurs. Or très souvent les protocoles de signalisation sur les passerelles VoIP n'utilisent pas d'identifiants. Il faut noter d'ailleurs que les passerelles sont aussi sensibles que les IPBX.
- Le vol d'identité via le vol d'identifiant de connexion SIP, ou via l'usurpation d'adresse MAC. Ce type d'attaque est possible parce que, très souvent, l'intégrateur laisse aux téléphones leur identifiant par défaut. Enfin, dans l'interface de l'administration des téléphones, le code source laisse apparaître le mot de passe en clair. La politique de mots de passe sur les identifiants de connexion doit impérativement être appliquée sur les téléphones.
- L'abus des fonctionnalités d'un téléphone IP, comme la prise de contrôle du téléphone à distance via Extension Mobility.

La présentation de M. Czarny comportait des démonstrations d'attaque visibles en vidéo sur le web CLUSIF
http://clusif.fr/fr/production/videos/#video130425

Les mesures de sécurisation périmétriques, Stéphane Choquet, Managing Director, Checkphone.

Stéphane Choquet prévient qu'accéder au PABX est devenu simple et que la fraude téléphonique est une source de revenus notable pour les pirates.
Or souvent, personne ne s'aperçoit de rien avant la réception de la facture téléphonique ou avant que l'opérateur informe son client d'une explosion du nombre d'appels vers l'international.
En général, le pirate utilise internet pour se créer un compte à l'étranger, il loue des numéros payants à des sociétés spécialisées et récolte l'argent. Le paiement par Paypal ou Western Union rend impossible le traçage.
Le piratage a souvent lieu à partir du vendredi soir et pendant tout le week end, quand personne n'est dans l'entreprise. Mais parfois aussi à petite dose sur la durée.
L'impact financier d'un hacking de PBX déclenche généralement un jeu complexe entre les différentes parties : l'entreprise victime, l'opérateur télécom, les juristes, l'installateur et les autorités. La plupart des fraudes n'entraînent pas de procès mais une grande frustration et une perte de confiance entre ces différents acteurs.
Pour réduire ces risques, il est possible d'utiliser des mesures de sécurisation périmétriques complémentaires aux mesures mises en œuvre sur les infrastructures téléphoniques (IPX, passerelles, terminaux).
Ces mesures périmétriques consistent à utiliser des pare-feux adaptés aux technologies téléphoniques, et permettent ainsi de filtrer des menaces de la même façon qu'un pare-feu traditionnel sur une infrastructure données.

~ o ~

Les mesures de sécurisation des équipements, Pierre Alexandre Fuhrmann, AASTRA.

Pierre Alexandre Fuhrmann explique quelles sont les mesures de sécurisation mises en œuvre lors du développement d'un PABX et lors de son intégration.
L'éditeur travaille sur plusieurs niveaux :

- L'application téléphonique en elle-même.
- La gestion de la solution de téléphonie.
- L'intégration dans le système d'information.
- L'intégration dans l'infrastructure de communication IP.

Une approche globale, qui prend en compte l'ensemble de ces niveaux, est nécessaire dès la phase d'architecture des solutions.

Quelques exemples de mesures de sécurité à déployer dans le système :

- Messages vocaux chiffrés et non écoutables par l'administrateur.
- Mots de passe par défaut configurables par l'administrateur (et non pas 0000 pour tous).
- Traçabilité des communications : tickets d'appel répliquables avec stockage sécurisé.
- Insertion d'un message lors de l'installation du système téléphonique afin de sensibiliser l'intégrateur à la sécurité.
- Politique de mot de passe constructeur modifiable par l'intégrateur une seule fois.
- Suivi des évolutions des distributions Linux pour résoudre de manière continue les failles de sécurité.
- Paramétrage restrictif par défaut de certaines fonctions sensibles (renvois vers l'extérieur, DISA écoute discrète etc.).
- Fonction « anti bavards » qui coupe toute communication qui dépasse cinquante minutes.
- Segmentation des droits de configuration.

En résumé, la téléphonie sur IP peut être davantage sécurisée que la téléphonie numérique.

Questions et Réponses avec l'assistance.

Cette conférence comportait également un débat avec la salle, non retranscrit dans ce document mais disponible en vidéo, sur le site web du CLUSIF, à l'adresse suivante :
http://www.clusif.fr/fr/production/videos/#video130425.

Retrouvez les vidéos de cette conférence et les supports des interventions sur le web CLUSIF http://www.clusif.fr/fr/infos/event/#conf130425.