VoIP et sécurité: c'est le moment de s'en préoccuper !

Le succès de la VoIP en entreprises (et chez les particuliers) n'est plus à prouver. En France, on compte désormais 3 millions d'abonnés, soit 250% de plus qu'il y a un an. 11% du trafic téléphonique concerne désormais la téléphonie sur Internet. Et selon Juniper Networks, le marché mondial de la VoIP représentera 18 milliards de dollars en 2010…

Au départ, cette technologie a été perçue par les entreprises comme un formidable réducteur de coûts. Mais aujourd'hui, se pose le problème de la sécurité de cette application. Car la VoIP est une application informatique en ligne comme une autre, elle est soumise à des vulnérabilités, à des risques d'intrusion, de fraudes. Intégrée au système d'information de l'entreprise, elle constitue donc un risque supplémentaire qu'il faut prendre en compte. Cette prise en compte est aujourd'hui une réalité. Car, l'interruption de la téléphonie suite à une attaque ou à une farude est parfaitement inenvisageable pour les entreprises. La question de la sécurité devient donc récurrente lors des appels d'offres. **Prise de conscience** Pour Joseph Saouma, responsable de l'offre VoIP pour l'opérateur Dynetcom, *« les responsables se posent des questions et les problématiques de sécurité deviennent un élément important dans le processus »*. *« De plus en plus de responsables s'inquiètent, c'est devenu un souci majeur »*, renchérit Pascal Debon, chairman de CheckPhone, spécialisé dans la sécurisation des applications téléphoniques pour entreprise. *« Les directions générales comprennent que la VoIP est une application classique qui exige des mesures de protection adéquates »*, ajoute-t-il. Une application qui est particulièrement faillible. *« La faiblesse du protocole et de la couche applicative est connue depuis longtemps »*, explique Gérard Péliks d'EADS Secure Networks. On peut aussi y ajouter la faiblesse des équipements filaires ou sans fil. Autant de vulnérabilités qui génèrent des risques importants. Des risques pas toujours connus des entreprises. *« Aux risques liés au monde IP comme les dénis de services distribués, l'altération des paquets IP et donc de l'intégrité des communications, l'usurpation d'identité et l'écoute des conversations, sans oublier les malwares (vers, virus, cheveux de Troie), il faut ajouter les risques liés aux protocoles comme le H323 ou le SIP »*, ajoute Gérard Péliks. *« Deux tendances de menaces sont aujourd'hui représentées »*, précise Pascal Debon de CheckPhone. *« La fraude externe est la menace la plus importante aujourd'hui: il s'agit de détourner et de facturer des capacités téléphoniques. Ensuite vient l'écoute, de plus en plus facile avec la VoIP. Suivront dans un futur proche: les attaques DDos qui pourront faire tomber les fonctions téléphoniques d'une entreprise via le bombardement de requêtes puis les virus ou les spams injectés dans le réseau, une menace que l'on a pas encore observé, mais qui devrait se développer rapidement »*. **Intrusions, fraudes et bientôt virus et spam** Les grandes entreprises seront les premières visées par ces menaces. Si elles n'adoptent pas une attitude proactive, les dégâts seront considérables, préviennent les spécialistes (qui on le sait aiment tirer sur la sonnette d'alarme) Alors comment se protéger ? Les solutions existent, elles sont nombreuses. Encore faut-il d'abord analyser la situation. *« L'entreprise doit avoir une démarche volontaire, elle doit connaître le terrain. C'est nouveau pour elle, car les télécoms étaient jusqu'à présent un domaine où le laisser-aller était la règle »*, affirme Joseph Saouma de Dynetcom. En effet, beaucoup d'entreprises s'apperçoiventb bien tard des faraudes par exemple. Pour Patrick Cardot, expert sécurité pour Cisco Systems, *« il faut se poser trois questions. Quelles menaces pèsent sur l'application et quel niveau de sécurité lui fournir ? Quelles sont les contre-mesures et sous quelles formes sont-elles*

disponibles ? Enfin, comment les mettre en place et les organiser ? » Un point de vue partagé par Arnaud Fayolle, responsable marketing PME pour Completel. *« La migration vers la VoIP est effectivement l'occasion pour les entreprises de s'interroger sur la problématique sécurité. L'important est d'identifier les menaces et les parades associés, en fonction de la criticité de l'application voix »*. **De l'importance de l'audit** Auditer et évaluer: tels sont les maîtres mots lorsqu'on se penche sur la question de la migration. *« la sécurité est à la fois un problème de technologie et de méthode, la sécurité, ça se définit »*, ajoute Pascal Debon de CheckPhone. Une fois les règles bien définies et la situation évaluée, les solutions sont plutôt nombreuses. Elles sécurisent, soit la couche infrastructure et/ou la couche logicielle. *« Il s'agit de chiffrer les transactions si la confidentialité des échanges est requise. Et de protéger ses bases d'information en filtrant les échanges et ne laisser passer que ceux qui correspondent à la politique de sécurité soigneusement mise eu point »*, explique Gérard Péliks (EADS). Pour Patrick Cardot (Cisco), *« La stratégie repose sur quatre piliers : la sécurisation des éléments actifs qui composent la solution, l'utilisation de l'infrastructure pour empêcher les malveillances, la protection des échanges protocolaires et des communications et la surveillance active »*. Mais d'ajouter: *« les solutions doivent être adaptées aux besoins réels »*. D'où encore une fois l'importance de l'audit. *« Ne pas négliger, ni à l'inverse dramatiser »*, souligne Arnaud Fayolle (Completel). **Le cas Skype**

De nombreuses entreprises, en particulier des PME, sont tentées d'utiliser des solutions grand-public comme Skype pour se jeter dans le bain de la VoIP. Une pratique à hauts risques, selon les experts et les opérateurs traditionnels. *« Skype représente un danger, si de grandes entreprises l'interdisent, ce n'est pas pour rien »*, affirme Pascal Debon, chairman de CheckPhone, spécialisé dans la sécurisation des applications téléphoniques pour entreprise. *« Il ne faut pas assimiler les solutions de VoIP entreprises à Skype. Son utilisation ouvre des brèches béantes dans la politique de sécurité »*, ajoute Arnaud Fayolle, responsable du marché PME pour Completel. En cause: une plate-forme propriétaire et l'utilisation du peer-to-peer dans l'application. Mais les opérateurs traditionnels ne grossissent-ils pas le trait ? Surtout au moment où Skype concentre ses efforts sur le marché de la PME (cf notre podcast audio). *« Je conteste les expertises des experts. Il suffit de lire les rapports sur cette question »*, tonne Jérôme Archambeaud, patron de la branche française de Skype. *« Toutes les informations sont cryptées de A à Z, lorsque la conversation transite sur le réseau IP, il est imposible d'y avoir accès. je pense que nous payons le prix de la mauvaise image du peer-to-peer. Par ailleurs, nous payons également la rançon du succès »*.