# Tribune libre

## Nouvelle révélation sur les écoutes de la NSA

## Votre entreprise est-elle bien protégée contre le piratage ?

WikiLeaks, en collaboration avec «Libération» et «Mediapart» révèlent comment la NSA s'est penchée, dès 2002, sur les intérêts commerciaux français. Une nouvelle révélation qui devrait amener les entreprises à réfléchir sur la protection des données.

La digitalisation des entreprises et l'accès illimité aux outils numériques offrent des possibilités sans limites au développement des entreprises mais également au développement des cyberattaques (hacking).
Quelles solutions techniques existent pour garantir la sécurité des données d'une entreprise ?
Comment combiner mobilité et sécurité informatique / télécom ? Existe-il des solutions pour empêcher les écoutes téléphoniques ?

**Surveiller vos portes d'entrées et vos back-doors !**
Il est toujours bon de rappeler les évidences. La base de la sécurité reste la porte d'entrée. Tout réseau se sécurise par le firewall (parefeu). Il faut être parfaitement équipé. Ensuite, pour ne pas se faire hacker de l'intérieur, il faut avoir de bons antivirus et antispams.
Passé ce niveau, il est souvent très utile de séparer les données (réseau Data) des communications téléphoniques IP (réseau Voix IP). Cette technique empêche de créer des failles dans le système informatique. La séparation des réseaux Voix / Data peut se faire virtuellement (VLAN) ou physiquement (câblage séparé).
Pour les travailleurs nomades, il est impératif de créer vos propres réseaux externes privés (WAN) qui permettront de tout contrôler (réseaux avec gestion de la qualité de service type MPLS ou équivalent). Ces solutions permettent de cloisonner, surveiller et sécuriser l'ensemble des données Voix / Data. Un réseau MPLS est un réseau privé (sur plusieurs sites distants) avec une seule porte d'entrée sécurisée. Il est plus facile de sécuriser une fois pour tous les sites, plutôt que de multiplier les portes d'entrées… Pour les utilisateurs nomades hors du réseau externe privé (WAN), un réseau privé crypté (VPN) demande une authentification via une application, pour accéder au réseau de l'entreprise. Ce réseau est crypté et la clé est un mot de passe très évolué.

**Sortez des grands standards !**
Pour nos solutions de téléphonie d'entreprise par exemple, nous choisissons des ports IP ou des protocoles différents de ceux visés par les hackers (qui utilisent les port(e)s les plus répandues). Ces ports IP sont beaucoup moins populaires et font l'objet de beaucoup moins d'attaques de la part des hackers… Simple mais efficace.
L'utilisation d'applications propriétaires (installées sur l'ordinateur) et non pas en pages web (Saas-Cloud), permet aussi de se prémunir du détournement de l'information malveillant.

**Le Softphone, le téléphone de demain !**
Des logiciels ou applis mobiles appelés « Softphone IP » permettent de se prémunir simplement de l'écoute et du piratage ! Depuis n'importe où et avec un simple accès internet (Wifi, 3G, 4G), vous avez l'équivalent de votre téléphone de bureau sur PC, Mac, smartphone, tablette… Non seulement les appels sont à la charge de votre entreprise, mais en plus les communications n'empruntent pas les réseaux mobiles opérateurs mais la Data VOIP. La voix peut alors être cryptée donc inécoutable. Chaque softphone a son protocole de transmission de la voix. Ce qui complique encore plus le piratage.
Vous avez donc des solutions pour communiquer avec les membres de la direction, avec les collaborateurs restés aux bureaux ou avec les partenaires et clients stratégiques en utilisant vos lignes fixes, avec votre mobile !

Profitez de cet été pour vous mettre à jour et rendre étanches vos réseaux informatiques (Data) et téléphonies (VoIP), vis à vis de l'internet publique.
Et si vous ne dormez toujours pas sur vos deux oreilles, demandez des solutions avec sécurité préventive et envois de notifications lors de tentatives de piratages informatiques ou lors d'une consommation téléphonique anormalement élevée.

**Alain Denis, Président d'Alliance Telecom**