



Sécuriser la Téléphonie sur IP (TOIP)

Facilité de mise en œuvre : difficile
Facilité d'exploitation : difficile
Hauteur de l'investissement humain : forte

La Téléphonie sur IP a pour objectif de permettre la communication vocale à l'aide des réseaux informatiques.

2 solutions techniques sont actuellement proposées :

- Le prestataire Internet peut fournir un service externalisé de téléphonie sur IP (TOIP). Tout est hébergé et administré chez lui.
 - ou
 - L'autocom téléphonique de l'entreprise est remplacé par un autocom compatible avec la TOIP. Cela peut être un autocom standard, auquel est rajoutée une carte d'extension IP ou une nouvelle machine (PC ou Autocom).
- Remarque : Les différentes box proposées par les fournisseurs Internet rentrent dans cette catégorie.

On est exposé à des risques de sécurité très importants, lorsque l'on utilise cette technologie.

⚠ Il est en fait fortement déconseillé pour le moment d'installer ou d'utiliser une solution de téléphonie sur IP car elle n'a pas atteint un niveau de sécurité satisfaisant.

Les risques, qui pèsent sur cette technologie.

- La ligne téléphonique a plus de risques d'être engorgée et bloquée, qu'une ligne téléphonique standard.
- Le trafic téléphonique peut être perdu et la conversation peut devenir incompréhensible.
- Les appels d'inconnus peuvent être pris en charge et payés par l'entreprise.
- Le trafic téléphonique peut être détourné vers des serveurs surtaxés.
- Quelqu'un peut facilement se faire passer pour un employé ou le dirigeant de l'entreprise et leur nuire.
- Les boîtes vocales peuvent être encombrées de messages publicitaires de la même façon que les boîtes mail sont encombrées de spam.
- Les appels peuvent être bloqués, les boîtes vocales saturées ou les équipements (les téléphones par exemple) rendus inutilisables.
- Les conversations peuvent aussi être facilement interceptées ou enregistrées.
- Les vers et virus peuvent aussi toucher ce réseau téléphonique et se propager sur le réseau des données informatiques. Ce qui implique la compromission des postes de travail ou du serveur de données.
- Enfin, un attaquant peut infiltrer le réseau informatique de l'entreprise à partir du réseau téléphonique IP, qui est très mal protégé.



L'utilisation de la téléphonie sur IP (TOIP) demande en fait la mise en œuvre de règles très strictes de sécurité et ce quelque soit la solution technique adoptée.

Les règles, que l'entreprise doit suivre pour sécuriser la téléphonie sur IP.

- Le débit de l'accès Internet doit être bien dimensionné, de telle sorte, qu'il puisse prendre en charge le trafic des données et le trafic téléphonique, afin d'éviter les blocages et la mauvaise qualité des communications.
- Les communications doivent être cryptées lorsqu'elles empruntent le réseau public Internet, afin d'éviter l'espionnage. La mise en place et la gestion d'un VPN "réseau privé virtuel" est donc indispensable.
- Le VPN utilisé doit permettre la priorisation des flux téléphoniques sur tous les autres flux, afin de garantir la qualité des communications et d'éviter les blocages et les coupures.
 - Une solution de secours doit être disponible, afin d'assurer une continuité du service téléphonique (redondance des équipements critiques et de l'accès à Internet par exemple).
 - Un pare-feu, capable de reconnaître et contrôler aussi les protocoles de communication très fragiles utilisés par la VoIP (SIP et H.323), doit être installé, afin de protéger l'entreprise des intrusions extérieures.
 - Une solution de contrôle antiviral, antispyware (anti-espion) à jour doit être installée sur les équipements utilisés par la téléphonie sur IP (TOIP), afin d'éviter toute possible compromission du réseau téléphonique mais aussi du réseau des données informatique.
 - Le débit réseau minimum requis dans l'entreprise doit être de 100Mb/s.
 - Le trafic Voix IP (VOIP) doit être isolé du reste du réseau de l'entreprise. Cela implique, que le réseau est compartimenté en 2 sous réseaux distincts, appelés aussi vlans, un pour la voix et un pour les données.
 - Les postes téléphoniques IP doivent être contrôlés et authentifiés avant de pouvoir se connecter au réseau de l'entreprise, afin d'empêcher toute connexion illicite.
 - La mise à jour des firmwares, qui est le logiciel installé dans les équipements de téléphonie IP doit être automatisée.
 - L'utilisation de solutions de type softphone (logiciel téléphonique sur PC) doit être évitée, car elles ne sont pas très stables et demandent une protection renforcée des postes de travail contre les codes malveillants et l'usurpation d'identité.