voip

Veille technique

La Voix sur IP, raccourcie de voix par le protocole internet, est aussi connue sous le terme de VoIP.

Elle se réfère à la diffusion du flux de la voix sur les réseaux Internet, au lieu des réseaux téléphoniques RTC traditionnels.Le protocole internet (IP) a été adapté à la gestion de la voix, en transformant et en transmettant l'information en paquet de données. La VoIP est à présent disponible sur de nombreux smartphones, ordinateurs et tablettes.

La VoIP facilite les tâches et fournit des services qui sont difficiles ou coûteux à mettre en place en utilisant le réseau traditionnel.

Comment ça fonctionne?

Pleins d'appels téléphoniques peuvent être transmis sur la même ligne téléphonique haut débit, de cette manière-là voIP peut faciliter à l'entreprise l'ajout des autres lignes téléphoniques sans avoir besoin de matérielle supplémentaire.

Ses fonctionnalités qui sont habituellement facturées par la plupart des sociétés télécoms, tels que le transfert d'appel, l'ID d'appelant ou la composition automatique, sont simples avec les fonctionnalités de la voIP.

D'autres avantages de la VoIP sont que les entreprises et les particuliers adoptent des systèmes téléphoniques aussi connus sous le nom de téléphone SIP ou softphone, qui utilisent la voix sur VoIP pour placer et transmettre des appels téléphonique sur un réseau IP avec internet.

Les soft phones et SIP c'est quoi?

La voIP convertit le signal audio d'un téléphone en un format digital qui peut être transmis par internet, et convertit aussi le format digital d'un appel entrant venant d'internet vers un signal audio standard.

Un téléphone logiciel SIP est une application qui utilise les hauts parleurs et le microphone de l'ordinateur pour permettre de passer ou recevoir des appels.

On peut toujours utiliser 3CX, Linphone, Ekinga etc... Sont l'exemple d'un téléphone gratuit phone système.

Nous en savons beaucoup sur la voip et maintenant nous demandons comment la sécuriser une fois qu'on l'a dans nos mains?

Côté sécurité?

Différentes protocoles pour sécuriser un voip nous avons :
-H.232 regroupe plusieurs protocoles qui concernent trois catégories distinctes qui sont la signalisation, la négociation de codecs et le transport de l'information.
c'est aussi un protocole de communication englobant un ensemble de normes utilisées pour l'envoi de données audio et vidéo sur internet afin que les utilisateurs et les petites entreprises l'utilisent sans devoir débourser de l'argent.
-IEE 802.1X un standard lié à la sécurité des réseaux informatiques, qui a un contrôle d'accès par port et s'appuyant sur un serveur d'authentification.
Il fournit également une couche de sécurité pour l'utilisation des réseaux câblés et sans fil, et s'applique à l'ensemble des éléments du réseau ou des équipements actifs et réseaux (commutateurs,etc...) ainsi que les terminaux dont les équipements voip.
-SIP-TLS (SIP over TLS) c'est la version sécurisée du protocole SIP, il assure la confidentialité des données échangées et se charge de se protéger contre la lecture ou l'analyse des échanges SIP sur le réseau.
Elle fait appel au protocole de sécurisation des échanges TLS (Transport Layer Security), qui est utilisé notamment par les banques et les sites de commerce électronique pour protéger les transactions de leurs clients.
-SRTP (Secure Real-Time Protocol) un protocole RTP (Real-Time Protocole) utilisé pour la transmission des données qui nécessite de fonctionner en temps réel avec les flux média audio ou vidéo.
C'est aussi une extension du protocole RTP qui utilise un algorithme AES (Advanced Encryption Standard) pour chiffrer et déchiffrer tous les messages entrant et sortant. Assure également la protection anti-replay en conservant un index des messages, utilisé pour vérifier les nouveaux messages.
-HTTPS connue pour les cas d'interface des terminaux, plus pour les interphones, avec des systèmes tiers comme le contrôle d'accès en particulier, les échanges de données et commandes de requêtes envoyées sont alors chiffrées et en même temps sécuriser l'accès à des locaux par exemple.
Il est donc capital de bien choisir ses serveurs VoIP, sans oublier les interphones SIP installés en extérieur, afin qu'ils prennent en compte l'ensemble des éléments et fonctionnalités de sécurité que nous avons évoqué.

Nous devons savoir que la sécurisation sans faille des transmissions audio vidéo sur le réseau.
Maintenant que nous avons parlé de la manière de sécuriser son serveur, je vais vous donner 4 conseils pour se prémunir des risques.
Comme tout outil numérique, la téléphonie IP peut se présenter avec des failles de sécurité.
Pour mieux s'en protéger, il est important de connaître ces risques et de mettre en place un plan d'action pour les contrer. C'est ce que nous allons voir dans les lignes en bas.

Une technologie qui doit faire face à des risques?

Comme avec la téléphonie traditionnelle, la voip fait face à des problématiques de sécurité. On peut en trouver plusieurs comme le phreaking, la manipulation des protocoles de signalisation, le ddos. Et d'autres qui sont propres à leur fonctionnement.

- Le déni de service (DoS)

  C'est une attaque visant à rendre indisponible un serveur en le submergeant de requête. Cette cyberattaque est généralement dirigée à l'encontre des serveurs web ou serveur de fichier. Et s'applique aussi sur les serveurs voip et le rend totalement inutilisable.

  Les cybercriminels mettent en place un processus automatique qui génère une multitude d'appels sur le serveur. La ligne téléphonique va être saturée et ne va laisser de place à aucun autre appel. Les clients, partenaires ou fournisseurs ne pourront plus vous joindre par téléphone et ce qui va qui va qu'on pourra plus passer d'appel.

  -Le phreaking

  Est une menace à ne pas prendre à la légère. Il s'agit d'une prise de contrôle des postes téléphoniques par un pirate. Le pirate ou < le phreaker> s'introduit dans le système de téléphonie d'une entreprise et multiplie les appels qui sont souvent surtaxés, ce qui va entraîner des frais trop élevés pour l'entreprise.

  Il a également des écoutes téléphoniques afin de voler des informations confidentielles et stratégiques.

  -Malwares et virus

Ces attaques exploitent les vulnérabilités d'un système voip afin d'en prendre le contrôle ou d'accéder à des informations sensibles.
Le voip peut être également victime de logiciels malveillants (virus, web shell....)
-Appels Spams (Le SPIT)
Les appels spam, appelés également SPIT (Spam over Internet Telephony), sont basés sur le même principe. C'est des appels téléphoniques non désirés qui viennent saturer la messagerie vocale et pénalise l'activité de l'entreprise et fait perdre du temps considérable aux victimes.
-Ecoute non autorisées
Une personne malveillante interceptant une conversation téléphonique non cryptée afin d'écouter son contenu et de récupérer de précieuses informations.
Cette attaque ne date pas d'hier et malheureusement, elle persiste encore aujourd'hui.
-L'altération d'appel
Comme son nom l'indique c'est une attaque qui consiste à altérer un appel téléphonique cours. Le pirate gâche la qualité de l'appel en injectant des paquets de bruit dans le flux de communication. Il modifie également le contenu des messages entre deux personnes sans qu'elles ne s'en aperçoivent.
-Le détournement d'appel
Avec le voip, les hackeurs modifient les paramètres de transfert d'appels afin de rediriger les appels ou d'un service. Toutes les communications destinées à une personne en particulier seront alors transférées et interceptées par le hackeur.

Conclusion

Avec cette veille technologique vous êtes maintenant prêt à vous lancer dans la création et la gestion d'un serveur Voip.