Protection contre les attaques robots

Vous recevez des appels d'un destinataire qui a pour nom "cisco" ou unknow@98.76.54.32 ou 100@votreIP ?

Malheureusement tout le monde est confronté au problème (Tandberg, Polycom, Huawei, Lifesize .....)
Ce sont des « robots » qui scannent toutes les adresses IP possible pour trouver des systèmes qui utilisent frauduleusement votre passerelle ISDN/RNIS ou PSTN pour passer des appels audio sur de longue distance, ce qui peut vous couter cher en communication.
Ce risque est présent seulement si votre système possède une adresse IP publique et si vous utilisez les protocoles SIP ou H323 et ISDN/RNIS et PSTN

Comment mieux se protéger :

Malheureusement, on ne maitrise pas tout ce qu'il se passe sur Internet. Nous ne pouvons être tenus pour responsable des perturbations provenant d'internet !
Après identification d'un système compatible, ils génèrent des appels audio en SIP ou H323 puis prennent le contrôle de votre système.

- Ils utilisent frauduleusement votre passerelle ISDN/RNIS ou PSTN pour passer des appels audio sur de longue distance, ce qui peut vous couter cher en communication.
- Cela est dérangeant, car le système de visioconférence n'arrête pas de sonner. - Changer les mots de passe par défaut des accès (admin, support, ssh ...,) en augmentant la sécurité de ceux-ci.
(Système 200/220 jusqu'à 16 caractères numériques de 0 à 9 et les caractères * ou # pour le password Admin)
(Système Icon 400/600/800 Alphanumérique + caractère spéciaux)

- Désactiver SSH (sauf au système utilisant l'UVC Manager)
- Désactiver le Telnet (sauf au système utilisant automate de contrôle)
- Désactiver la réponse automatique et réponse automatique en multi-voie dans le système
- Désactiver l'accès Web au possible (sauf pour les systèmes qui ont un contrat sérénité)
- Désactiver les appels SIP, si vous le pouvez, plus difficile pour H323 car on ne peut pas tout désactiver sinon, plus rien ne fonctionne (Ceci entraine qu'aucun appel en SIP ne sera pas pris en compte, il faudra l'activer au besoin)

- Si votre point de terminaison est configuré pour effectuer des appels audio (via PSTN, RTC ou IPBX), assurez-vous que le préfixe utilisé pour placer un appel ne soit pas simple ou trop évident (ex 00 ou 9 ...). Les robots d'attaque essaient de préfixes communs pour voir s'ils peuvent placer un appel téléphonique à un numéro surtaxé à l'étranger.

- Utiliser le bouton "ne pas déranger" dès que l'on ne se sert pas du système de visioconférence ou que l'on est en conférence et que l'on ne souhaite pas recevoir d'autres appels. (Mais il faut le réactiver au besoin).

S'il vous est possible de créer des listes d'accès sur le Firewall de manière à n'autoriser l'accès vers ce terminal que depuis des systèmes ou adresses bien définis.

La meilleure solution est de cacher vos paramètres derrière une infrastructure tel un serveur ClearSea ou Cloud. (C'est la solution la plus efficace !) Mais cette solution à des contraintes (parfois financière) pour le client, mais cela reste possible.