

Quand les téléphones IP se positionnent comme un risque pour la sécurité : Les terminaux VoIP pris entre deux feux

Depuis quelque temps, des rumeurs, notamment dans les médias américains, font état de graves failles de sécurité sur certains téléphones IP. Ces allégations ont donné lieu à de nombreuses discussions sur le niveau de sécurité des terminaux IP. Luca Livraga, chef d'équipe de l'assistance technique internationale chez Snom Technology GmbH, le pionnier de la VoIP, explique ce qui est important dans la sécurisation des terminaux IP.

Ils ne sont pas seulement utilisés pour l'espionnage, mais ils constituent aussi des proies faciles pour les cybercriminels : Les téléphones IP font régulièrement l'objet de l'attention des médias en raison de leurs failles de sécurité. Récemment, les médias américains ont fait état d'allégations à l'encontre de certaines marques détenant une part de marché élevée. Cela alimente le préjugé selon lequel tous les terminaux IP ne sont pas sûrs. Bien sûr, en termes de sécurité offerte, on ne peut pas mettre tous les téléphones IP dans le même sac. Les mécanismes de protection intégrés diffèrent considérablement d'une marque à l'autre, ce qui n'est pas seulement lié à la mise en œuvre technique.

Chaque pays a ses coutumes

Les directives de protection des données applicables en Europe sont actuellement les plus strictes au monde. Certaines pratiques qui se sont imposées ailleurs sont considérées comme de graves atteintes à la sécurité en Europe. Il s'agit par

exemple de la vente de données d'utilisation à des tiers et de l'accès automatique aux données et informations pour les agences gouvernementales. Les fabricants et les gouvernements européens sont intransigeants sur la réglementation européenne : personne n'est autorisé à écouter ne serait-ce qu'un seul téléphone ou à accéder aux données d'utilisation sans ordonnance judiciaire préalable ou approbation par divers comités. Cela vaut également pour les gouvernements. Avec SRAPS, Snom ajoute un obstacle supplémentaire. Le serveur SRAPS est situé en Allemagne, un État qui s'appuie actuellement des lois les plus strictes en matière de protection des données.

« Par exemple, la seule information qui est transmise avec certitude par les téléphones Snom, ce sont les données convenues au niveau mondial pour tracer un appel reçu par le service d'appel d'urgence, par exemple lorsqu'une personne cherchant de l'aide est incapable de communiquer sa position. Ici, l'adresse IP du téléphone ne peut être retracée qu'à son emplacement (adresse, si nécessaire étage) au moyen de protocoles standardisés pour la fourniture de services d'urgence par des organismes légitimes », explique Livraga.

Par conséquent, l'idée de transmettre des extraits ou des conversations, entières, à des tiers tels que des commerçants en ligne est totalement impossible. Même l'accès à distance aux téléphones par un service clientèle ou des revendeurs de confiance à des fins de maintenance est soumis à la protection des données. Le commerçant est légalement tenu de rendre anonyme toute information personnelle de l'utilisateur. Snom veille même à ce que toutes les données personnelles des téléphones envoyés en réparation soient supprimées, afin d'éviter tout abus éventuel. De même, le suivi des données de connexion d'un ou plusieurs appels à des fins de dépannage via le micrologiciel des téléphones n'a lieu qu'avec l'accord de l'autre partie – et les données techniques enregistrées n'ont aucune valeur pour quiconque, à l'exception les

responsables de l'assistance. Les interfaces permettant de stocker les données d'utilisation sur le PC de l'utilisateur ou de les transmettre intégralement à des tiers ne sont pas disponibles sur les téléphones Snom.

Le téléphone IP : Quel est son niveau de sécurité ?

Outre le niveau minimal de sécurité défini par la loi, certains fabricants installent plusieurs mécanismes de sécurité dans les téléphones. Livraga nous présente deux exemples pour expliquer ce qui est important lorsqu'il s'agit de protéger une conversation et d'échanger des informations entre le téléphone et le standard.

Certificats et identification du téléphone

Le transfert des paramètres du central téléphonique vers le téléphone s'effectue via https et nécessite par défaut l'échange de certificats. Chaque appareil Snom possède un certificat unique associé à l'adresse MAC. Le central téléphonique vérifie l'exactitude et la validité du certificat avant d'autoriser la connexion. « Cela pourrait être comparé à une procédure d'identification par présentation de l'identifiant personnel du téléphone », explique Livraga. Ensuite, le téléphone Snom vérifie lui aussi le certificat du serveur pour s'assurer qu'il est bien connecté au bon PABX. Cette procédure, appelée authentification silencieuse, permet d'éviter les cyber-attaques les plus fréquentes. D'autres mécanismes empêchent également que le certificat soit reconnu comme valide, même si l'adresse MAC est manipulée. La seule solution est donc le vol du téléphone. Cependant, « il s'agit d'une étape complexe, et c'est exactement là que réside le concept de sécurité informatique : compliquer le processus de manière à le rendre désavantageux. Snom a néanmoins prévu la possibilité que le téléphone perde toutes ses données dès qu'il est déconnecté de l'alimentation électrique, de sorte que cette tentative est également inutile. », ajoute Livraga.

Port RTP aléatoire et flux de données crypté

Il s'agit du premier niveau de sécurité. Une autre mesure de sécurité contre l'enregistrement des appels téléphoniques est la « randomisation » des ports d'entrée et de sortie pour le flux de données RTP (donc pour l'appel téléphonique) et son chiffrement (SRTP). Le central et le téléphone communiquent entre eux via des certificats, mais le téléphone décide indépendamment, lors de chaque appel, du port utilisé. Cette opération se déroule automatiquement et oblige les attaquants potentiels à effectuer une série d'analyses pour identifier le port utilisé pour l'appel en cours. C'est là que les Firewalls entrent en jeu : ces derniers détectent rapidement des analyses anormales et qu'une tentative d'attaque est en cours.

Sécurité : l'utilisateur est également sollicité

« Tant que l'utilisateur respecte les directives concernant l'utilisation de https et des mots de passe sécurisés, ainsi que les mises à jour, il sera protégé. Mais dans ce contexte, il est également important de choisir un système téléphonique qui a les mêmes priorités », confirme Livraga. « Sinon, ce serait comme verrouiller la voiture en laissant le capot ouvert ! Pour cette raison, il est important de s'adresser à des professionnels certifiés. »

