

Risques s curitaires pour Les terminaux VoIP

S curit 

Post  par : JPilo

Publi e le : 2/2/2022 15:00:00

Depuis quelque temps, des rumeurs, notamment dans les m dias am ricains, font  tat de graves failles de s curit  sur certains t l phones IP. Ces all gations ont donn  lieu   de nombreuses discussions sur le niveau de s curit  des terminaux IP.

Luca Livraga, chef d' quipe de l'assistance technique internationale chez Snom Technology GmbH, le pionnier de la VoIP, explique ce qui est important dans la s curisation des terminaux IP.

Ils ne sont pas seulement utilis s pour l'espionnage, mais ils constituent aussi des proies faciles pour les cybercriminels : Les t l phones IP font r guli rement l'objet de l'attention des m dias en raison de leurs failles de s curit . R cemment, les m dias am ricains ont fait  tat d'all gations   l'encontre de certaines marques d tenant une part de march   lev e.

Cela alimente le pr jug  selon lequel tous les terminaux IP ne sont pas s rs. Bien s r, en termes de s curit  offerte, on ne peut pas mettre tous les t l phones IP dans le m me sac. Les m canismes de protection int gr s diff rent consid rablement d'une marque   l'autre, ce qui n'est pas seulement li    la mise en  uvre technique.

Chaque pays a ses coutumes

Les directives de protection des donn es applicables en Europe sont actuellement les plus strictes au monde. Certaines pratiques qui se sont impos es ailleurs sont consid r es comme de graves atteintes   la s curit  en Europe. Il s'agit par exemple de la vente de donn es d'utilisation   des tiers et de l'acc s automatique aux donn es et informations pour les agences gouvernementales.

Les fabricants et les gouvernements europ ens sont intransigeants sur la r glementation europ enne : personne n'est autoris     couter ne serait-ce qu'un seul t l phone ou   acc der aux donn es d'utilisation sans ordonnance judiciaire pr alable ou approbation par divers comit s. Cela vaut  galement pour les gouvernements. Avec SRAPS, Snom ajoute un obstacle suppl mentaire. Le serveur SRAPS est situ  en Allemagne, un  tat qui s ppuie actuellement des lois les plus strictes en mati re de protection des donn es.

  Par exemple, la seule information qui est transmise avec certitude par les t l phones Snom, ce sont les donn es convenues au niveau mondial pour tracer un appel re  u 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 t l phone ne peut  tre retrac e qu'  son emplacement (adresse, si n cessaire  tage) au moyen de protocoles standardis s pour la fourniture de services d'urgence par des organismes l gitimes  , explique Livraga.

Par cons quent, l'id e de transmettre des extraits ou des conversations, enti res,   des tiers tels que des commer ants en ligne est totalement impossible. M me l'acc s   distance aux t l phones par un service client le ou des revendeurs de confiance   des fins de maintenance est soumis   la protection des donn es.

Le commer ant est  galement tenu de rendre anonyme toute information personnelle de

l'utilisateur. Snom veille m  me    ce que toutes les donn  es personnelles des t  l  phones envoy  s en r  paration soient supprim  es, afin d'  viter tout abus   ventuel.

De m  me, le suivi des donn  es de connexion d'un ou plusieurs appels    des fins de d  pannage via le micrologiciel des t  l  phones n'a lieu qu'avec l'accord de l'autre partie - et les donn  es techniques enregistr  es n'ont aucune valeur pour quiconque,    l'exception les responsables de l'assistance. Les interfaces permettant de stocker les donn  es d'utilisation sur le PC de l'utilisateur ou de les transmettre int  gralement    des tiers ne sont pas disponibles sur les t  l  phones Snom.

Le t  l  phone IP : Quel est son niveau de s  curit   ?

Outre le niveau minimal de s  curit   d  fini par la loi, certains fabricants installent plusieurs m  canismes de s  curit   dans les t  l  phones. Livraga nous pr  sente deux exemples pour expliquer ce qui est important lorsqu'il s'agit de prot  ger une conversation et d'  changer des informations entre le t  l  phone et le standard.

Certificats et identification du t  l  phone

Le transfert des param  tres du central t  l  phonique vers le t  l  phone s'effectue via https et n  cessite par d  faut l'  change de certificats. Chaque appareil Snom poss  de un certificat unique associ      l'adresse MAC. Le central t  l  phonique v  rifie l'exactitude et la validit   du certificat avant d'autoriser la connexion.

   Cela pourrait   tre compar      une proc  dure d'identification par pr  sentation de l'identifiant personnel du t  l  phone   , explique Livraga. Ensuite, le t  l  phone Snom v  rifie lui aussi le certificat du serveur pour s'assurer qu'il est bien connect   au bon PABX.

Cette proc  dure, appel  e authentification silencieuse, permet d'  viter les cyber-attaques les plus fr  quentes. D'autres m  canismes emp  chent   galement que le certificat soit reconnu comme valide, m  me si l'adresse MAC est manipul  e. La seule solution est donc le vol du t  l  phone.

Cependant,    il s  agit d  une   tape complexe, et c'est exactement l   que r  side le concept de s  curit   informatique : compliquer le processus de mani  re    le rendre d  savantageux. Snom a n  anmoins pr  vu la possibilit   que le t  l  phone perde toutes ses donn  es d  s qu'il est d  connect   de l'alimentation   lectrique, de sorte que cette tentative est   galement inutile.   , ajoute Livraga.

Port RTP al  atoire et flux de donn  es crypt  

Il s'agit du premier niveau de s  curit  . Une autre mesure de s  curit   contre l'enregistrement des appels t  l  phoniques est la   randomisation    des ports d'entr  e et de sortie pour le flux de donn  es RTP (donc pour l'appel t  l  phonique) et son chiffrement (SRTP).

Le central et le t  l  phone communiquent entre eux via des certificats, mais le t  l  phone d  cide ind  pendamment, lors de chaque appel, du port utilis  . Cette op  ration se d  roule automatiquement et oblige les attaquants potentiels    effectuer une s  rie d'analyses pour identifier le port utilis   pour l'appel en cours. C'est l   que les Firewalls entrent en jeu : ces derniers d  tectent rapidement des analyses anormales et qu'une tentative d'attaque est en cours.

S  curit   : l'utilisateur est   galement sollicit  

« 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. »