Déclaration de Lydis en réaction à « Follow The Money » - clients
Le 16 septembre 2023, deux articles ont été publiés sur la plateforme journalistique néerlandais « Follow The Money » et dans le journal économique belge « De Tijd ». D'après ces articles, plusieurs organisations utiliseraient des équipements de communication fabriqués par l'entreprise chinoise Yealink, dans lesquels des failles de sécurité auraient été découvertes.

Par le biais de cette communication, nous tenons à vous faire part de notre point de vue de la question. En effet, ces articles n'ont pas été communiqués au préalable pour vérification, ni à Lydis, ni à Yealink, et contiennent des inexactitudes factuelles démontrables qui donnent au lecteur une impression trompeuse de Yealink et de ses équipements, ainsi que des systèmes de communication audio et vidéo via internet de manière générale.

Au mois d'août 2022, Lydis et Yealink ont été informés de problèmes concernant l'équipement de téléphonie de Yealink. Le matériel de visioconférence de Yealink (par exemple pour une utilisation avec l'application Teams) n'est pas concerné. En effet, cette application est entièrement sécurisée par Microsoft et n'est utilisable que si ces appareils satisfont à certaines exigences. Bien entendu, en tant que distributeur, nous aussi, nous nous efforçons de garantir une sécurité optimale aux utilisateurs de nos produits. Aussi, Lydis est très reconnaissant à la personne qui a signalé ces problèmes. Lydis n'était pas au courant de cette situation, mais après concertation avec Yealink, nous avons découvert qu'il y avait effectivement des problèmes.

L'article traite en grande partie de la question de l'outil de cryptage qui, selon les opérateurs téléphoniques, n'est pas utilisé pour crypter les fichiers de configuration (appelés documents « provisioning » dans l'article). Ces opérateurs mettent en œuvre leurs propres mesures de sécurité, afin d'assurer les mesures de sécurité du produit, pour garantir l'échange sécurisé des données entre leur plateforme et l'équipement du bureau de l'utilisateur.

Les détails concernant l'abonnement téléphonique de l'utilisateur individuel ne sont jamais en la possession du fabricant de l'appareil. Ces données sont la propriété de l'opérateur téléphonique auprès duquel l'utilisateur final procure un service de téléphonie, et l'appareil communique directement avec le serveur de l'opérateur téléphonique, sans l'intervention de Yealink.

Le port mentionné dans l'article, 5060, est essentiel au fonctionnement des téléphones et est utilisé comme port par défaut pour les communications VoIP. Pour l'envoi d'images, lorsque ce port est fermé, le téléphone ne peut pas fonctionner. L'utilisation de ce port n'est pas propre aux équipements Yealink ; le port est utilisé par tous les fabricants de l'industrie de la VoIP.

En principe, les problèmes liés à l'outil de cryptage et à l'accès au logiciel système (firmware) pourraient concerner certains clients. C'est pourquoi Yealink a mis au point une mise à jour du logiciel système des modèles très anciens, bien qu'il ne soit plus pris en charge depuis des années. Une modification a également été apportée à

l'outil de cryptage. Nous avons communiqué ouvertement à ce sujet en avril 2023. Un certain nombre de clients ont alors constaté, après analyse et après avoir réalisé des tests d'intrusion (pen tests), l'absence de risque supplémentaire pour eux. Nous tenons donc à vous signaler que la sécurité de vos données n'a jamais été mise en danger en raison de ces lacunes.

La plateforme Follow The Money et le journal De Tijd évoquent quelques questions et produits aujourd'hui considérés comme obsolètes, et donnent ainsi à tort l'impression que la sécurité des flux de données de certaines organisations néerlandaises et belges est menacée. C'est absolument faux.

En juin 2023, nous avons reçu en nos locaux la personne qui a signalé le problème ainsi qu'un journaliste de Follow The Money et leur avons tout expliqué en détail. Ainsi, il est très regrettable de constater qu'ils n'ont pas intégré nos explications et informations dans l'article.

La coopération entre Lydis et Yealink est vieille de plusieurs dizaines d'années, et tout comme les partenaires ayant réalisé les tests d'intrusion, nous ne voyons aucune raison de mettre en question la politique de sécurité de Yealink. Yealink prend la sécurité des systèmes très au sérieux et nous estimons que l'entreprise a réagi de manière appropriée dès que ces problèmes ont été révélés. Bien entendu, nous nous tenons à votre entière disposition pour répondre à toutes les questions que vous pourriez avoir.

Au nom de l'équipe Lydis,

Gijsbert Zijlstra
Directeur technique
gijsbert.zijlstra@lydis.com

La déclaration complète de Yealink est consultable ici, Yealink partage ici les informations factuelles sur toutes les mesures de sécurité concernant ses produits et de son organisation, telles que ISO 27001, GDPR, SOC2 Type1, SOC2 Type2, et SOC3, 802.1x, AES Encryption.