Conseils importants pour les clients : Assurer la conformité avec les lois et règlements de l'UE en matière de protection des données.

En tant que fournisseur de systèmes d'alarme numérique qui mettent en œuvre PD CLC/TS 50134-9:2018 et SS 91100:2014 (« Alarme sociale numérique - Protocole Internet d'alarme sociale (SCAIP) - Spécification »), nous nous engageons à aider nos clients à se conformer à la législation européenne en vigueur, en particulier à l'acte délégué de la Directive relative aux Équipements Radioélectriques (« Radio Equipment Directive »).

Nos systèmes d'alarme sociale sont conçus pour utiliser le protocole SCAIP (Protocole Internet pour Alarme de Soins Sociaux) et sont basés sur les normes SS 91100:2014 et PD CLC/TS 50134-9:2018. Ces normes spécifient l'utilisation d'un format XML pour les codes d'alarme et d'information, transportés sur un réseau de communication IP tel que l'internet. Le protocole s'appuie sur le protocole d'initiation de session (SIP) pour la gestion des sessions.

Pour garantir la conformité avec la législation de l'UE, en particulier en ce qui concerne la protection des données personnelles et de la vie privée dans les communications électroniques, il est essentiel que tous les messages d'alarme et les communications vocales ou multimédias associées soient transmis sur un canal sécurisé.

Bien que nos produits puissent être configurés pour transmettre des messages d'alarme en « clair » afin de s'adapter aux infrastructures existantes des centres de réception des alarmes qui peuvent ne pas mettre en œuvre actuellement la sécurité de la couche de transport (TLS), cette méthode de communication n'est généralement pas considérée comme sûre pour les informations sensibles.

La norme PD CLC/TS 50134-9:2018 stipule explicitement que l'unité locale et le contrôleur et le centre de réception des alarmes doivent prendre en charge le chiffrement, et que l'unité locale et le contrôleur ne doivent pas transmettre d'informations personnelles ou sensibles sur une connexion non sécurisée sans chiffrement. Il stipule en outre que les données personnelles et sensibles ne peuvent être transmises que par le biais d'un protocole SIP sécurisé (SIPS). Cela inclut la prise en charge du SIP sécurisé sur des connexions non sécurisées et, pour les communications vocales, l'utilisation du protocole de transport sécurisé en temps réel (SRTP) avec un cryptage AES-128 au minimum.

Par conséquent, pour se conformer aux exigences de la législation européenne concernant la protection des données et la sécurité des communications électroniques, les clients doivent s'assurer de l'un des points suivants pour leurs déploiements de systèmes d'alarme sociale :

Utiliser Secure SIP (SIPS) avec TLS 1.2 ou supérieur : Il s'agit de la méthode privilégiée pour sécuriser les messages d'alarme et les communications vocales/multimédia sur les réseaux IP. Nos produits prennent en charge cette fonctionnalité. Le centre de réception des alarmes doit présenter un certificat ITU X509 valide, et l'unité locale doit vérifier l'identité du certificat du serveur à l'aide d'un certificat local de l'autorité de certification racine (Root CA Certificate).

Transmettre les messages d'alarme et la voix sur un canal sécurisé distinct (par exemple, un réseau privé virtuel (VPN)) : Si le cryptage SIP TLS direct n'est pas possible en raison des limitations de l'infrastructure du centre de réception des alarmes existante, un tunnel sécurisé tel qu'un VPN doit être établi pour crypter toutes les communications entre l'expéditeur de l'alarme (unité locale et contrôleur) et le récepteur de l'alarme (centre de réception des alarmes).

L'absence de mesures de sécurité adéquates pour la transmission des messages d'alarme et des communications vocales peut entraîner une non-conformité avec les réglementations de l'UE en matière de protection des données et de communications électroniques. **Il incombe au client de configurer et d'exploiter le système de manière à garantir cette conformité.** Nous vous conseillons vivement de consulter vos équipes juridiques et de sécurité informatique pour vous assurer que votre déploiement répond à toutes les exigences réglementaires applicables.