BOSCH

Des technologies pour la vie

Assurez la sécurité des données vidéo

Les données issues de la sécurité vidéo sont de plus en plus connectées aux réseaux locaux et internationaux. Un nombre croissant de composants périphériques (caméras) envoie leurs données aux composants principaux (serveurs) via Internet, où des intrus numériques et des pirates informatiques sont à l'affût.

Les risques

Une seule faiblesse au niveau de la liaison dans la configuration de la sécurité vidéo peut suffire à compromettre tout le système. Par exemple, des pirates informatiques habiles peuvent mettre en place des attaques de type « man-in-the-middle », en interceptant les communications entre une caméra et le système de gestion vidéo (VMS). Une fois que les pirates informatiques ont accès aux communications, ils peuvent injecter un flux vidéo secondaire pour masquer leur activité illicite, ou pour manipuler l'enregistrement vidéo en temps réel afin de supprimer de manière sélective certains détails ou certaines personnes de la scène.

Couvrir tous les angles

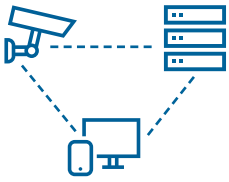
Nous parvenons à une sécurité optimale grâce à une approche en quatre étapes qui prend en compte l'ensemble de l'infrastructure de la sécurité vidéo. Nous instaurons la confiance en affectant une clé d'authentification à chaque composant du réseau. Nous sécurisons les données vis-à-vis des pirates informatiques en chiffrant celles-ci au niveau matériel à l'aide d'une clé de chiffrement stockée en toute sécurité dans un module TPM (Trusted Platform Module) intégré et unique. Nous offrons des moyens simples de gérer les droits d'accès utilisateur afin que vous puissiez vous assurer que seules les personnes autorisées ont accès à vos données. Enfin, nous pouvons prendre en charge la configuration d'une infrastructure de clés publiques (PKI). Avec Bosch, vos données bénéficient d'une sécurité optimale.

Les données vidéo étant souvent extrêmement stratégiques et sensibles, Bosch utilise une approche systématique pour optimiser la sécurité des données en prenant en compte la sécurité physique et la cybersécurité de manière simultanée. L'approche de Bosch permet de parvenir aux meilleurs résultats en matière de sécurité des données de bout en bout.

Bosch prend en charge tous les principaux éléments de l'infrastructure de sécurité vidéo :

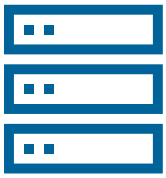
Sécurisation de nos caméras

- Les connexions sécurisées sont prises en charge (HTTPS)
- Application d'un mot de passe lors de la configuration initiale
- « Désactivation » de l'exécution de logiciels tiers
- Actualisation du firmware via des fichiers signés par le fabricant uniquement
- Les opérations liées à l'authentification et au chiffrement sont exécutées uniquement à l'intérieur du module TPM intégré et unique



Sécurisation des communications réseau

- Les ports non sécurisés sont désactivés par défaut
- Application d'un mot de passe lors de la configuration initiale
- Authentification réseau à l'aide du protocole 802.1x
- Prise en charge de l'AES (clés jusqu'à 256 bits pour le chiffrement)



Sécurisation de nos périphériques principaux

- Les opérations liées à l'authentification et au chiffrement sont exécutées uniquement à l'intérieur du module TPM intégré et unique
- Prise en charge de Microsoft Active Directory pour une gestion sécurisée des droits d'accès utilisateur
- Authentification des accès Digest uniquement
- Mises à jour régulières à l'aide de correctifs de sécurité

Prise en charge des infrastructures de clés publiques (PKI)

- Certificats uniques signés par Bosch chargés en usine sur toutes les caméras
- Module TPM intégré unique pour des opérations de chiffrement hautement sécurisées
- Autorité de certification interne (Escrypt)
- Prise en charge des certificats spécifiques aux clients
- Prise en charge des solutions PKI tierces

Pour plus d'informations, téléchargez les documents suivants :
Guide sur la sécurité des données
Note technique sur l'authentification réseau
VS-EH-fr-06_F01U561100_02