BOSCH

Innovación para tu vida

Proteja los datos de vídeo

Los datos de seguridad mediante vídeo están cada vez más conectados a las redes locales y mundiales. Así, un número creciente de componentes periféricos (cámaras) envían sus datos a componentes principales (servidores) a través de Internet, donde merodean intrusos digitales y hackers.

Los riesgos

Un solo enlace débil en la configuración de seguridad mediante vídeo puede poner en peligro la totalidad del sistema. Por ejemplo, los hackers experimentados pueden perpetrar los llamados ataques de intermediarios y secuestrar las comunicaciones entre una cámara y un sistema de gestión de vídeo (VMS). Una vez que los hackers obtienen acceso, pueden infiltrar un vídeo alternativo para ocultar su actividad ilícita, o bien manipular las grabaciones en directo de la cámara para eliminar de forma selectiva detalles o personas concretos de la escena.

Cobertura de todos los ángulos

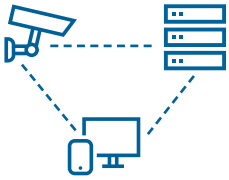
Logramos los más altos niveles con nuestro enfoque de cuatro pasos, que tiene en cuenta toda la infraestructura del sistema de seguridad mediante vídeo. Creamos confianza asignando una clave de autenticación a cada componente de la red. Protegemos los datos de los hackers cifrándolos en el nivel de hardware, con una clave criptográfica que se almacena protegida en un módulo de plataforma de confianza (TPM) integrado exclusivo. Ofrecemos formas fáciles de gestionar los derechos de acceso de los usuarios para garantizar que solo personal autorizado tenga acceso a sus datos. Y, por último, le ayudamos a configurar una infraestructura de clave pública (PKI). Así, con Bosch, no puede estar más seguro.

Como los datos de vídeo suelen ser muy delicados y confidenciales, Bosch dirige un enfoque sistemático que aumenta al máximo la seguridad de los datos teniendo en cuenta al mismo tiempo la seguridad física y la ciberseguridad. El enfoque del sistema de Bosch es la clave para conseguir los niveles más altos en la seguridad de los datos de principio a fin.

Bosch cubre todos los elementos principales de una infraestructura de seguridad mediante vídeo:

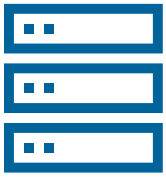
Cómo protegemos nuestras cámaras

- Se admiten conexiones seguras (HTTPS)
- Aplicación de contraseñas durante la configuración inicial
- Ejecución de software de terceros “deshabilitada”
- Actualizaciones de firmware solo con los archivos firmados por el fabricante
- Las operaciones criptográficas, para autenticación y codificación, se ejecutan solo dentro del módulo de plataforma de confianza (TPM) integrado



Cómo protegemos la comunicación en la red

- Los puertos no seguros están desactivados de manera predeterminada
- Aplicación de contraseñas durante la configuración inicial
- Autenticación en la red con el protocolo 802.1x
- Compatibilidad con el estándar de codificación avanzada (de hasta 256 bits para la codificación)



Cómo protegemos nuestros dispositivos esenciales

- Las operaciones criptográficas, para autenticación y codificación, se ejecutan solo dentro del módulo de plataforma de confianza (TPM) integrado
- Compatibilidad con Microsoft Active Directory para la gestión segura de los derechos de acceso de los usuarios
- Acceso a Digest Authentication solamente
- Actualizaciones periódicas con parches de seguridad

Cómo apoyamos las infraestructuras de claves públicas (PKI)

- Certificados exclusivos firmados por Bosch cargados en fábrica en todas las cámaras
- Módulo de plataforma de confianza (TPM) integrado exclusivo para operaciones criptográficas altamente seguras
- Autoridad certificadora propia (Escrypt)
- Compatibilidad con los certificados específicos del cliente
- Compatibilidad con soluciones de PKI de terceros

Para obtener más información, descargue los siguientes documentos de nuestra empresa:
Guía de seguridad de los datos
Nota técnica sobre autenticación en la red
VS-EH-es-06_F01U561099_02