BOSCH
Tecnologia per la vita

Mantenere sicuri i dati video

I dati di videosorveglianza sono sempre più interconnessi sulle reti locali e mondiali. Un numero in costante crescita di componenti distribuiti (telecamere) invia dati ai server via Internet, dove sono in agguato hacker e criminali informatici.

I rischi

Anche un solo punto debole in una configurazione di sorveglianza può potenzialmente mettere a rischio un intero sistema. Ad esempio, hacker esperti possono sferrare attacchi man-in-the-middle, dirottando le comunicazioni tra una telecamera e un sistema di gestione video (VMS). Una volta guadagnato l'accesso, sono in grado di iniettare un video alternativo per occultare attività illecite oppure manipolare le riprese dal vivo della telecamera per rimuovere in maniera selettiva determinati dettagli o persone dalla scena.

Coprire ogni angolo

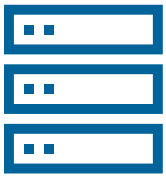
Bosch soddisfa gli standard più elevati con un approccio in quattro fasi che prende in considerazione l'intera infrastruttura di videosorveglianza. Stabiliamo innanzitutto un rapporto di fiducia assegnando una chiave di autenticazione a ogni componente della rete. Proteggiamo i dati dagli hacker crittografandoli a livello hardware, utilizzando una chiave di crittografia memorizzata in maniera sicura in un esclusivo modulo TPM (Trusted Platform Module) integrato. Forniamo modi semplici per gestire i diritti di accesso degli utenti assicurando che solo gli utenti autorizzati abbiano accesso ai dati. E infine supportiamo l'impostazione di un'infrastruttura a chiave pubblica. Bosch assicura il massimo livello di protezione.

Dal momento che i dati video sono spesso di elevata criticità e sensibilità, Bosch adotta un approccio di sistema per ottimizzare la protezione dei dati, integrando sicurezza fisica e sicurezza informatica. L'approccio di sistema di Bosch è fondamentale per assicurare la conformità agli standard più elevati di protezione dei dati end-to-end.

Bosch copre tutti i più importanti elementi dell'infrastruttura di videosorveglianza:

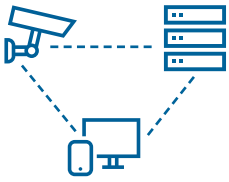
Come proteggiamo le telecamere

- Sono supportati collegamenti sicuri (HTTPS)
- Applicazione password alla configurazione iniziale
- Esecuzione software di terze parti “disabilitata”
- Aggiornamenti firmware solo attraverso file con firma del produttore
- Operazioni di crittografia, per l'autenticazione e la crittografia, eseguite solo all'interno dell'esclusivo modulo TPM (Trusted Platform Module) integrato



Come proteggiamo i dispositivi di base

- Operazioni di crittografia, per l'autenticazione e la crittografia, eseguite solo all'interno dell'esclusivo modulo TPM (Trusted Platform Module) integrato
- Supporto di Microsoft Active Directory per la gestione sicura dei diritti di accesso degli utenti
- Solo autenticazione accessi Digest
- Aggiornamenti regolari con patch di protezione



Come proteggiamo le comunicazioni di rete

- Porte non sicure disattivate per impostazione predefinita
- Applicazione password alla configurazione iniziale
- Autenticazione di rete con protocollo 802.1x
- Supporto di Advanced Encryption Standard (chiavi di autenticazione fino a 256 bit per la crittografia)

Come supportiamo le infrastrutture a chiave pubblica

- Certificati univoci con firma Bosch caricati in fabbrica su tutte le telecamere
- Esclusivo modulo TPM (Trusted Platform Module) integrato per operazioni di crittografia a elevata protezione
- Autorità di certificazione (Escrypt) interna
- Supporto di certificati specifici del cliente
- Supporto di soluzioni di infrastruttura a chiave pubblica di terze parti

Per ulteriori informazioni, scaricare:
Guida alla sicurezza dei dati
Nota tecnica sull'autenticazione di rete
VS-EH-it-06_F01U561102_02