BOSCH
Technik fürs Leben

Schutz von Videodaten

Videosicherheitsdaten werden zunehmend in lokalen und globalen Netzwerken versendet: Eine ständig steigende Anzahl von dezentralen Komponenten (Kameras) schickt ihre Aufzeichnungsdaten über das Internet zu Kernkomponenten (Server) – und unterwegs lauern Datendiebe und Hacker.

Die Risiken

Eine einzige Schwachstelle bei einer Videosicherheitseinrichtung kann das gesamte System gefährden. Geübte Hacker können sich beispielsweise durch einen sogenannten Man-in-the-Middle-Angriff in die Kommunikation zwischen einer Kamera und dem Videomanagementsystem (VMS) einklinken. Hat der Hacker Zugriff, kann er zur Vertuschung illegaler Aktivitäten einen eigenen Videostream einspeisen oder Live-Bildmaterial manipulieren, um ausgewählte Details oder Personen aus einer Szene zu entfernen.

Umfassender Schutz

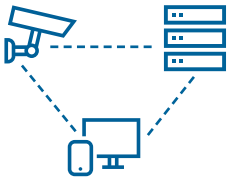
Mit einem vierstufigen Ansatz, der die gesamte Videosicherheitsinfrastruktur berücksichtigt, können wir höchste Standards erfüllen: Wir schaffen Vertrauen, indem wir jeder Komponente im Netzwerk einen Authentifizierungsschlüssel zuweisen. Wir schützen Daten vor Hackern, indem wir sie bereits auf Hardwareebene mit einem kryptografischen Schlüssel verschlüsseln, der sicher auf einem einzigartigen integrierten Trusted Platform Module (TPM) gespeichert ist. Wir ermöglichen die einfache Verwaltung von Benutzerzugriffsrechten, damit Sie gewährleisten können, dass nur autorisierte Personen Zugriff zu Ihren Daten haben. Darüber hinaus können wir Sie bei der Konfiguration einer Public-Key-Infrastruktur unterstützen. Mit Bosch sind Ihre Daten sicherer denn je.

Da bei der Videoüberwachung häufig äußerst kritische, sensible Daten produziert werden, geht Bosch den Datenschutz systematisch an und berücksichtigt sowohl die Netz- als auch physische Sicherheit. So können wir die höchsten Standards der Ende-zu-Ende-Verschlüsselung erfüllen und Ihre Daten schützen.

Bosch deckt alle wichtigen Komponenten der Videosicherheitsinfrastruktur ab:

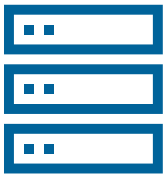
So schützen wir unsere Kameras

- Sichere Verbindungen werden unterstützt (HTTPS)
- Festlegen eines Passworts bei Inbetriebnahme
- Ausführen von Drittanbietersoftware ist deaktiviert
- Firmware-Updates nur mit vom Hersteller signierten Dateien
- Kryptografische Operationen für Authentifizierung und Verschlüsselung werden nur innerhalb des einzigartigen integrierten Trusted Platform Module (TPM) ausgeführt



So schützen wir die Netzwerkkommunikation

- Standardmäßige Deaktivierung unsicherer Ports
- Festlegen eines Passworts bei Inbetriebnahme
- Netzwerkauthentifizierung mit dem IEEE 802.1x-Standard
- Unterstützung des Advanced Encryption Standard (AES, Schlüssellängen bis 256 Bit)



So schützen wir unsere zentralen Geräte

- Kryptografische Operationen für Authentifizierung und Verschlüsselung werden nur innerhalb des einzigartigen integrierten Trusted Platform Module (TPM) ausgeführt
- Unterstützung von Microsoft Active Directory für die sichere Verwaltung von Benutzerzugriffsrechten
- Nur Digest Access Authentication
- Regelmäßige Aktualisierungen über Sicherheitspatches

So unterstützen wir die Publik-Key-Infrastruktur (PKI)

- Werkseitig geladene, einzigartige von Bosch signierte Zertifikate auf allen Kameras
- Einzigartiges integriertes Trusted Platform Module (TPM) für äußerst sichere kryptografische Operationen
- Interne Zertifizierungsstelle (Escrypt)
- Unterstützung von kundenspezifischen Zertifikaten
- Unterstützung von Drittanbieter-PKI-Lösungen

Weitere Informationen finden Sie in den folgenden Dokumenten:
Datensicherheitshandbuch
Veröffentlichung zur Netzwerkauthentifizierung
VS-EH-de-06_F01U561098_02