BOSCH
Technologie voor het leven

Videogegevens veilig bewaren

Videobeveiligingsgegevens zijn steeds meer verbonden in lokale en globale netwerken. Een stijgend aantal randcomponenten (camera's) stuurt hun gegevens naar hoofdcomponenten (servers) via internet, waar digitale indringers en hackers rondhangen.

De risico's

Een enkele zwakke schakel in een videobeveiligingsinstallatie kan een heel systeem in gevaar brengen. Vaardige hackers kunnen bijvoorbeeld zogenoemde 'man-in-the-middle' aanvallen uitvoeren en de communicatie tussen een camera en een videobeheersysteem (VMS) kapen. Zodra hackers toegang hebben, kunnen ze een andere videofeed invoeren om illegale activiteiten te verbergen of live-beelden manipuleren om bepaalde details of personen uit een scène te verwijderen.

Alle hoeken beschermen

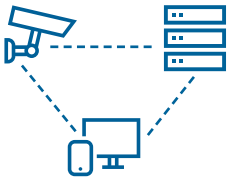
We realiseren de hoogste normen met een 4-staps benadering waarbij rekening wordt gehouden met de volledige infrastructuur van de videobeveiliging. We creëren vertrouwen door aan elke component binnen het netwerk een verificatiesleutel toe te wijzen. We beschermen gegevens tegen hackers door de gegevens te versleutelen op hardwareniveau met behulp van een cryptografische sleutel die veilig is opgeslagen in een unieke ingebouwde Trusted Platform Module (TPM). We bieden eenvoudige manieren om gebruikerstoegangsrechten te beheren, zodat alleen geautoriseerde personen toegang hebben tot uw gegevens. En ten slotte kunnen we een infrastructuur voor openbare sleutels (PKI) ondersteunen. U kunt dus niet veiliger zijn dan met Bosch.

Omdat videogegevens vaak zeer kritiek en gevoelig zijn, pakt Bosch maximale gegevensbeveiliging systematisch aan en houdt daarbij rekening met fysieke veiligheid en met cyberbeveiliging. Deze benadering van Bosch is de sleutel tot het realiseren van de hoogste normen op het gebied van end-to-end gegevensbeveiliging.

Bosch houdt rekening met alle belangrijke elementen van de infrastructuur voor videobeveiliging:

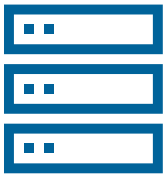
Hoe we onze camera's beveiligen

- Beveiligde verbindingen worden ondersteund (HTTPS)
- Wachtwoordafdwinging bij de eerste installatie
- Uitvoering van externe software is uitgeschakeld
- Firmware-updates uitsluitend via door fabrikant gesigneerde bestanden
- Cryptografische bewerkingen voor verificatie en codering worden uitsluitend uitgevoerd binnen de unieke ingebouwde Trusted Platform Module (TPM)



Hoe we netwerkcommunicatie beveiligen

- Onbeveiligde poorten worden standaard uitgeschakeld
- Wachtwoordafdwinging bij de eerste installatie
- Netwerkverificatie overeenkomstig het 802.1x-protocol
- Ondersteuning van de Advanced Encryption Standard (sleutels tot en met 256 bits voor codering)



Hoe we onze hoofdapparaten beveiligen

- Cryptografische bewerkingen voor verificatie en codering worden uitsluitend uitgevoerd binnen de unieke ingebouwde Trusted Platform Module (TPM)
- Ondersteuning van Microsoft Active Directory voor veilig beheer van gebruikerstoegangsrechten
- Uitsluitend Digest-toegangsverificatie
- Regelmatige updates via beveiligingspatches

Hoe we infrastructuren voor openbare sleutels (PKI, Public Key Infrastructures) ondersteunen

- Door de fabriek geleverde, unieke door Bosch ondertekende certificaten op alle camera's
- Unieke ingebouwde Trusted Platform Module (TPM) voor uiterst veilige cryptografische bewerkingen
- Eigen certificeringsinstantie (Escrypt)
- Ondersteuning voor klantspecifieke certificaten
- Ondersteuning voor externe PKI-oplossingen

Download voor meer informatie het volgende:
Handboek voor gegevensbeveiliging
Technische opmerking over netwerkverificatie
VS-EH-nl-06_ F01U561034_02