

**BOSCH**

Yaşam için teknoloji

Video verilerini güvenli tutun

Video güvenliği verileri, yerel ve küresel ağlar arasında artan bir şekilde bağlı duruma gelmektedir. Artan sayıda uç bileşen (kameralar), verilerini dijital davetsiz misafirler ve bilgisayar korsanlarının görüldüğü İnternet üzerinden temel bileşenlere (sunucular) aktarmaktadır.

Riskler

Video güvenliği düzenindeki tek bir zayıf halka bile bir sistemin tamamını tehlikeye atabilir. Örneğin, yetenekli bilgisayar korsanları bir kamera ile video yönetim sistemi (VMS) arasındaki iletişimi çalarak sözde izinsiz izleme saldırılarını yönlendirebilir. Korsanlar erişim sağladıktan sonra, yasadışı faaliyetleri gizlemek için alternatif bir video akışını araya ekleyebilir ya da belli ayrıntıları veya kişileri seçerek sahneden kaldırmak için canlı kamera görüntülerini değiştirebilir.

Tüm açılırları kapsama

Tüm video güvenliği altyapısını dikkate alan dört adımlı bir yaklaşımla en yüksek standartlara ulaşıyoruz. Ağdaki her bileşene bir kimlik denetimi anahtarı atayarak güven oluşturuyoruz. Verileri, benzersiz bir yerleşik Güvenilir Platform Modülü'nde (TPM) güvenli bir şekilde saklanan kriptografik bir anahtar kullanarak donanım seviyesinde şifrelemek yoluyla bilgisayar korsanlarına karşı güvenlik altına alıyoruz. Yalnızca yetkili kişilerin verilerinize erişmesini sağlayan kullanıcı erişim haklarını yönetmek için kolay yollar sunuyoruz. Ayrıca son olarak, Genel Anahtar Altyapısı düzenini destekleyebiliyoruz. Yani Bosch sayesinde, hiç olmadığı kadar güvendesiniz.



Video verileri genellikle son derece kritik ve hassas olduğundan, Bosch fiziksel güvenlik ile siber güvenliği aynı anda dikkate alarak veri güvenliğini en üst seviyeye çıkarmak için sistematik bir yaklaşımı desteklemektedir. Bosch'un sistem yaklaşımı, uçtan uca veri güvenliğinde en yüksek standartlara ulaşmanın anahtarıdır.

Bosch, video güvenliği altyapısının tüm önemli ögelerini karşılar:



Kameralarımızın güvenliğini nasıl sağlıyoruz?

- Güvenli bağlantılar desteklenir (HTTPS)
- İlk kurulumda parola uygulaması
- “Devre dışı bırakılan” 3. taraf yazılımlarının yürütülmesi
- Yalnızca üreticinin imzaladığı dosyalarla cihaz yazılımı güncellemeleri
- Yalnızca benzersiz yerleşik Güvenilir Platform Modülü'nün (TPM) içinde yürütülen kimlik denetimine ve şifrelemeye yönelik kriptografik işlemler



Ağ iletişiminin güvenliğini nasıl sağlıyoruz?

- Varsayılan olarak devre dışı bırakılmış güvenli olmayan portlar
- İlk kurulumda parola uygulaması
- 802.1x protokolüyle ağ kimlik denetimi
- Gelişmiş Şifreleme Standardı desteği (şifreleme için 256 bit'e kadar)



Temel cihazlarımızı nasıl güvenlik altına alıyoruz?

- Yalnızca benzersiz yerleşik Güvenilir Platform Modülü'nün (TPM) içinde yürütülen kimlik denetimine ve şifrelemeye yönelik kriptografik işlemler
- Kullanıcı erişim haklarının güvenli biçimde yönetimi için Microsoft Active Directory desteği
- Yalnızca özet erişim kimlik denetimi
- Güvenlik yamalarıyla düzenli güncellemeler



Genel Anahtar Altyapılarını (PKI) nasıl destekliyoruz?

- Tüm kameralarda fabrikada yüklenmiş benzersiz Bosch imzalı sertifikalar
- Son derece güvenli kriptografik işlemler için benzersiz yerleşik Güvenilir Platform Modülü (TPM)
- Şirket İçi Sertifika Yetkilisi (Escript)
- Müşteriye özel sertifika desteği
- 3. taraf PKI çözümleri desteği

Daha fazla bilgi için aşağıdakileri indirin:

[Veri güvenliği rehberi](#)

[Ağ kimlik denetimi teknik notu](#)

VS-EH-tr-06_F01U561106_02