BOSCH
Technologia bliżej nas

Bezpieczne przechowywanie danych wideo

Dane dotyczące dozoru wizyjnego w coraz większym stopniu są dostępne w sieciach lokalnych i globalnych. Wzrasta liczba urządzeń końcowych (kamer), które przez Internet wysyłają dane do urządzeń podstawowych (serwerów), narażając je na działania hakerów i innych niepożądanych osób.

Ryzyko

Nawet jeden słaby punkt w konfiguracji dozoru może narazić na szwank cały system. Zdolni hakerzy potrafią przeprowadzać ataki typu „man in the middle", przejmując kontrolę nad komunikacją pomiędzy kamerą i systemem zarządzania sygnałem wizyjnym (VMS). Gdy już uzyskają dostęp, mogą rozprowadzać inny sygnał wizyjny, by ukryć niedozwolone działania, lub manipulować obrazem na żywo i wybiórczo usuwać określone szczegóły lub osoby z kadru.

Kontrola pod każdym kątem

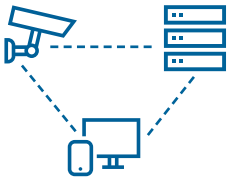
Nasze czterostopniowe podejście zapewnia kompleksową infrastrukturę nadzoru wizyjnego. Przypisanie klucza uwierzytelniającego do każdego składnika sieci sprawia, że klienci nam ufają. Chronimy dane przed hakerami, kodując je na poziomie sprzętowym. Nasze rozwiązania korzystają z klucza kryptograficznego bezpiecznie przechowywanego w unikatowej, wbudowanej platformie Trusted Platform Module (TPM). Oferujemy proste narzędzia do zarządzania uprawnieniami dostępu użytkowników, dzięki którym tylko upoważnione osoby mają dostęp do Twoich danych. Zapewniamy także pomoc przy konfigurowaniu infrastruktury klucza publicznego. Innymi słowy — z firmą Bosch możesz czuć się bezpiecznie.

W związku z tym, że dane wideo są często niezwykle ważne i poufne, firma Bosch ciągle dąży do zwiększania poziomu bezpieczeństwa danych zarówno fizycznie, jak i w cyberprzestrzeni. Podejście systemowe firmy Bosch jest kluczem do uzyskania najwyższych standardów kompleksowej ochrony danych.

Firma Bosch oferuje wszystkie najważniejsze elementy infrastruktury dozoru wizyjnego:

Jak chronimy nasze kamery

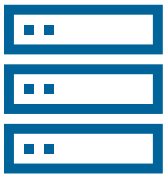
- Bezpieczne połączenia są obsługiwane (HTTPS)
- Wymóg podania hasła podczas konfiguracji wstępnej
- „Wyłączono” oprogramowania innych producentów
- Aktualizacja oprogramowania układowego odbywa się jedynie za pomocą podpisanych plików producenta
- Działania kryptograficzne w zakresie uwierzytelniania i szyfrowania mają miejsce tylko we wbudowanej, unikatowej platformie Trusted Platform Module (TPM)



Jak chronimy komunikację sieciową

- Domyślnie wyłączone niezabezpieczone porty
- Wymóg podania hasła podczas konfiguracji wstępnej
- Uwierzytelnianie sieciowe za pomocą protokołu 802.1x
- Zgodność ze standardem Advance Encryption Standard (maksymalnie 256-bitowe klucze szyfrujące).

Aby uzyskać więcej informacji, pobierz nasz:
Poradnik dotyczący bezpieczeństwa danych
Uwagę techniczną dotycząca uwierzytelniania sieciowego
VS-EH-pl-06_F01U561103_02



Jak chronimy nasze urządzenia podstawowe

- Działania kryptograficzne w zakresie uwierzytelniania i szyfrowania mają miejsce tylko we wbudowanej, unikatowej platformie Trusted Platform Module (TPM)
- Obsługa programu Microsoft Active Directory zapewniającego bezpieczne zarządzanie uprawnieniami dostępu użytkowników
- Tylko szyfrowane uwierzytelnianie dostępu
- Regularne aktualizacje z poprawkami bezpieczeństwa

Jak obsługujemy infrastrukturę kluczy publicznych (PKI)

- Preinstalowane podpisane certyfikaty Bosch na wszystkich kamerach
- Bezpieczeństwo działań kryptograficznych dzięki unikatowej, wbudowanej platformie Trusted Platform Module (TPM)
- Wewnętrzne centrum certyfikacji (Escrypt)
- Obsługa niestandardowych certyfikatów klienta
- Obsługa rozwiązań PKI innych producentów