BIAŁA KSIĘGA

Kamery nasobne Axis

Bezpieczeństwo systemu

Luty 2024

Streszczenie

Choć system nasobny Axis jest zbudowany na platformie otwartej, został bardzo skutecznie zabezpieczony.

Aby bezpieczeństwo było zapewnione także w wypadku utraty kamery, jej oprogramowanie ograniczono do minimum i pozbawiono wszystkich składników poza niezbędnymi. Dodatkowe funkcje ulokowano w kontrolerze systemu, który jest zwykle mniej narażony na zagrożenia fizyczne. Co więcej, dane w wewnętrznej pamięci kamery są szyfrowane przy użyciu algorytmu AES-256 w celu wykluczenia nieautoryzowanego dostępu. Zastosowanie protokołu IPv6 i certyfikatów pozwoliło na zbudowanie rozwiązania, w którym dane z kamery można ściągnąć tylko do konkretnego kontrolera lub systemu, do którego należy.

Podczas ściągania danych z kamery do kontrolera systemu używane jest szyfrowane połączenie sieciowe HTTPS. Dane tylko przez krótki czas znajdują się w zaszyfrowanej algorytmem AES-256 pamięci masowej kontrolera systemu, a zaraz potem przekazywane są dalej, poprzez następne zaszyfrowane połączenie HTTPS, do miejsca przeznaczenia treści.

Bezpieczeństwo i integralność kontrolera systemu są dodatkowo wzmocnione przez moduł TPM (trusted platform module) zgodny ze standardem FIPS 140-2. Rozwiązaniami, które kamery nasobne dzielą z wieloma innymi urządzeniami Axis, są: podpisane oprogramowanie sprzętowe, bezpieczny start i wideo z podpisem.

Podczas strumieniowego przesyłania materiału na żywo przez aplikację AXIS Body Worn Live dane są szyfrowane w spoczynku, w transporcie i w przeglądarce WWW użytkownika. Są również szyfrowane na całej trasie przy użyciu protokołu XChaCha20-Poly1305. Administrator ma kontrolę nad tym, kto może oglądać strumień na żywo — z dokładnością do konkretnego komputera, przeglądarki WWW i danych uwierzytelniających użytkownika.

Spis treści

1 Akronimy i terminologia

BWC. Body worn camera (kamera nasobna)

VMS. Video management system (system zarządzania materiałem wizyjnym)

EMS. Evidence management system (system zarządzania materiałem dowodowym)

Miejsce przeznaczenia treści Miejsce, w którym przechowywane są nagrania i dane, na przykład z kamer nasobnych. Przykładami miejsc przeznaczenia treści są systemy zarządzania materiałem wizyjnym, systemy zarządzania materiałem dowodowym i serwery multimedialne.

2 Wprowadzenie

System nasobny Axis jest zbudowany w oparciu o otwartą platformę, którą można w prosty sposób zintegrować z zewnętrznymi systemami zarządzania materiałem wizyjnym i materiałem dowodowym. Jednocześnie system jest bardzo dobrze zabezpieczony, ponieważ właśnie bezpieczeństwo było priorytetem na każdym etapie jego implementacji.

W niniejszym artykule omawiamy przepływ danych między komponentami systemu nasobnego Axis. Szczególną uwagę poświęcamy środkom, jakie podjęto w celu zabezpieczenia systemu i jego danych na wszystkich etapach, od rejestracji w kamerze nasobnej aż do miejsca przeznaczenia treści. Opisujemy także różne nośniki danych oraz właściwe dla nich dodatkowe aspekty bezpieczeństwa.

3 Bezpieczeństwo w razie utraty kamery

W codziennym użytkowaniu kamery nasobne są fizycznie narażone na ryzyko kradzieży i wandalizmu. W konstrukcji systemu zastosowano kilka rozwiązań ograniczających skutki takich zdarzeń w celu zapewnienia bezpieczeństwa systemu i danych nawet w razie utraty kamery.

Przykładem takiego rozwiązania jest wyposażenie kamery nasobnej w oprogramowanie pozbawione wszystkich komponentów, które nie są niezbędne — taka platforma programowa jest znacznie ograniczona w porównaniu z innymi kamerami Axis. Kamera ani kontroler systemu nie obsługują VAPIX ani takich protokołów, jak FTP, SSH lub SNMP. Poza tym kamera nie udostępnia funkcji serwera. Za integrację z innymi systemami, takimi jak VMS i EMS, odpowiada kontroler systemu, który zwykle jest mniej narażony na zagrożenia fizyczne niż same kamery.

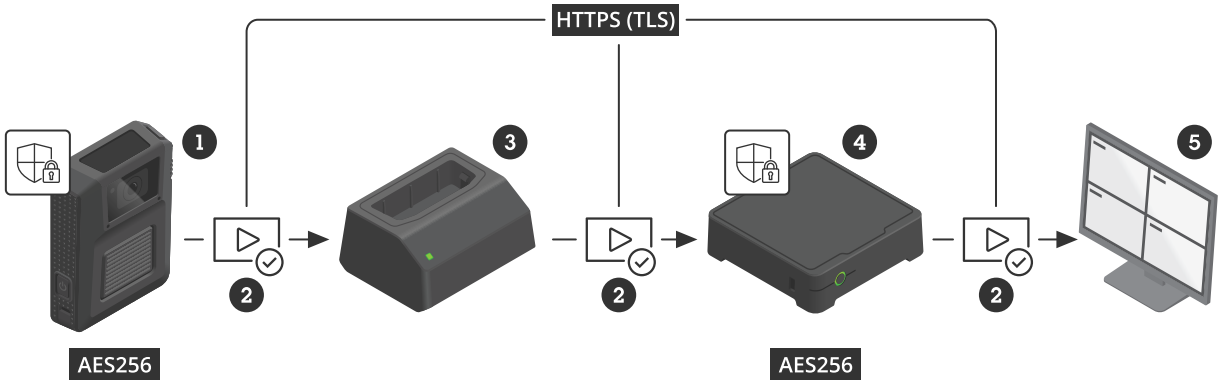
Dane w wewnętrznej pamięci kamery nasobnej są zaszyfrowane przy użyciu algorytmu AES-256 w celu wykluczenia nieautoryzowanego dostępu do nich w razie utraty kamery.

Kamera pozwoli na ściągnięcie danych tylko jednemu, konkretnemu kontrolerowi systemu lub systemowi, do którego należy. To zabezpieczenie realizowane jest w ten sposób, że kamera nasobna i kontroler systemu komunikują się ze sobą przy użyciu protokołu IPv6 i certyfikatów. Każdorazowo po zadokowaniu kamery certyfikaty są automatycznie odnawiane, tak by były zgodne z najnowszym certyfikatem kontrolera systemu.

Jeśli kamera nie będzie umieszczana na stacji dokującej i nie połączy się z systemem przez czas dłuższy niż cztery tygodnie, kontroler systemu będzie akceptował starsze certyfikaty jeszcze przez osiem tygodni. Po tym czasie konieczne będzie ponowne ręczne zaakceptowanie kamery w systemie przy użyciu centralnego hasła. Dzięki temu kamera, która przez długi czas pozostawała bez kontroli i/lub poza systemem, nie da się w sposób niezauważony ponownie dodać, co byłoby potencjalnie niebezpieczne.

4 Bezpieczeństwo przesyłania danych

W typowym scenariuszu kamera nasobna zawierająca materiał i metadane jest po zakończeniu zmiany/służby umieszczana w stacji dokującej. Wszystkie dane są ściągane przez stację dokującą do kontrolera systemu za pośrednictwem połączenia sieciowego szyfrowanego protokołem HTTPS (HTTP z TLS). Dane są obecne w kontrolerze systemu tylko przez krótki czas, w jego pamięci masowej SSD szyfrowanej algorytmem AES-256. Następnie kontroler systemu przesyła dane, korzystając z protokołu HTTPS, do miejsca przeznaczenia treści.



Bezpieczne przesyłanie i przechowywanie danych z kamery nasobnej (1) do miejsca przeznaczenia (5).

1 *Kamera nasobna z platformą Axis Edge Vault*
2 *Wideo z podpisem (funkcja cyberzabezpieczeń)*
3 *Stacja dokująca*
4 *Kontroler systemu z platformą Axis Edge Vault*
5 *Miejsce przeznaczenia treści*

Przewidziano także możliwość wykorzystania klucza szyfrującego z miejsca przeznaczenia treści do szyfrowania danych w kamerze nasobnej i kontrolerze systemu — jeśli miejsce przeznaczenia udostępnia publiczny klucz szyfrujący. W takim przypadku przy przesyłaniu danych do miejsca przeznaczenia dane będą zabezpieczone dodatkową warstwą szyfrowania.

5 Inne funkcje podnoszące bezpieczeństwo

Bezpieczeństwo i integralność kontrolera systemu są dodatkowo wzmocnione przez moduł TPM (trusted platform module) zgodny ze standardem FIPS 140-2.

Zarówno kamera nasobna, jak i kontroler systemu są wyposażone w Axis Edge Vault, sprzętową platformę cyberbezpieczeństwa, która chroni wszystkie dane w urządzeniach i udostępnia kilka funkcji zabezpieczeń. Przykładowo system plików jest zaszyfrowany, a ochronę klucza zapewnia Axis Edge Vault. Dzięki funkcji *bezpiecznego startu* urządzenia można uruchomić tylko pod warunkiem, że mają one autoryzowane oprogramowanie sprzętowe. *Podpisane oprogramowanie sprzętowe* sprawia, że urządzenia odrzucają uaktualnienia oprogramowania sprzętowego, jeśli jego integralność została naruszona. *Wideo z podpisem* tworzy dodatkową warstwę ochrony, uzupełniając strumień wideo o kryptograficzną sumę kontrolną. Dzięki temu możliwe jest wiarygodne przypisanie materiału wideo do konkretnej kamery Axis, która go wygenerowała, i potwierdzenie, że materiał nie został zmanipulowany.

Więcej informacji o wideo z podpisem można znaleźć na stronie *www.axis.com/developer-community/signed-video*, a dodatkowe informacje o

rozwiązaniach Axis zwiększających cyberbezpieczeństwo dostępne są na stronie *www.axis.com/solutions/built-in-cybersecurity-features*.

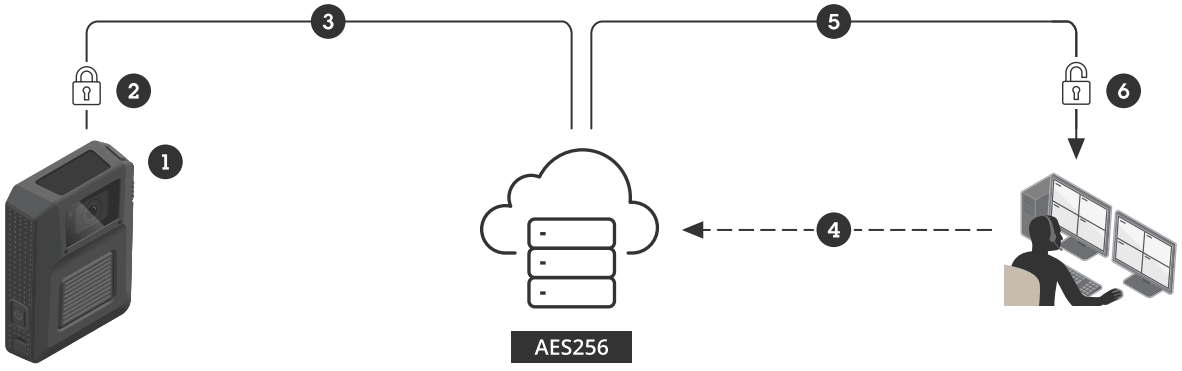
Użytkownik kamery przebywający w terenie może obejrzeć obraz zarejestrowany przez kamerę wyłącznie za pomocą aplikacji AXIS Body Worn Assistant. Jeśli aplikacja jest włączona, kamera nasobna przesyła strumień wideo bezpośrednio do aplikacji, ale materiał nie jest zapisywany i dostępny w pamięci podręcznej lub operacyjnej urządzenia, na którym aplikacja działa. Do strumienia wideo jest także dodawana nakładka zniechęcająca do wtórnego nagrywania wideo za pomocą zewnętrznego urządzenia. Jeśli mimo to obraz zostanie tak zarejestrowany, nakładka pozwoli na powiązanie nagrania z użytkownikiem kamery nasobnej. Za pomocą złącza USB-C kamery nasobnej nie można w żaden sposób wyświetlić, usunąć ani ściągnąć materiału wizyjnego.

6 Bezpieczeństwo z aplikacją AXIS Body Worn Live

AXIS Body Worn Live to aplikacja umożliwiająca dostęp do danych przekazywanych na żywo z kamer nasobnych Axis. Udostępniając użytkownikom przesyłany na żywo strumień wideo, dźwięku i innych danych, takich jak współrzędne położenia, aplikacja AXIS Body Worn Live zapewnia im wysoki poziom świadomości sytuacyjnej w trakcie incydentu. Początkowo dostępna jest jako usługa w chmurze.

Aplikacja AXIS Body Worn Live szyfruje dane nie tylko w spoczynku (w pamięci) i podczas przesyłania, lecz także na całej trasie od kamery do przeglądarki WWW użytkownika.

Wszystkie dane i pliki utrzymywane przez aplikację AXIS Body Worn Live są szyfrowane w spoczynku za pomocą algorytmu AES-256. Wszystkie kanały komunikacyjne są zabezpieczone przy użyciu protokołu HTTPS z TLS i certyfikatów podpisanych przez zaufane ośrodki certyfikacji. AXIS Body Worn Live dodaje także jeszcze jedną warstwę szyfrowania na całej trasie, stosując protokół XChaCha20-Poly1305.



Bezpieczne przesyłanie strumieniowe na żywo z szyfrowaniem na całej trasie w aplikacji AXIS Body Worn Live

1 *Kamera nasobna uzyskuje na żywo materiał wizyjny i inne dane.*
2 *Dane są szyfrowane w kamerze nasobnej.*
3 *Dane są przesyłane z kamery nasobnej do aplikacji AXIS Body Worn Live.*
4 *Użytkownik prosi o dane z aplikacji AXIS Body Worn Live.*
5 *Dane są przesyłane strumieniowo z aplikacji AXIS Body Worn Live do użytkownika.*
6 *Dane są odszyfrowywane w przeglądarce WWW użytkownika.*

Administrator systemu kamer nasobnych ma pełną kontrolę nad tym, kto może oglądać strumień na żywo. Dane są szyfrowane w taki sposób, że tylko użytkownicy zatwierdzeni przez administratora mogą deszyfrować i oglądać materiał wizyjny, a ponadto administrator może cofnąć uprawnienia dostępu. Użytkownik potrzebuje do tego właściwego komputera, właściwej przeglądarki WWW i właściwych danych

uwierzytelniających. Nikt, nawet firma Axis, nie ma dostępu do strumienia przekazywanego na żywo. Axis nie ma dostępu do utworzonych przez użytkownika kluczy szyfrujących.

O firmie Axis Communications

Axis umożliwia tworzenie mądrzejszego i bezpieczniejszego świata, tworząc rozwiązania zwiększające bezpieczeństwo i wydajność biznesową. Jako firma z branży technologicznej będąca liderem na rynku, Axis oferuje systemy dozoru wizyjnego, kontroli dostępu, domofonowe i rozwiązania audio. Rozwiązania te są wzbogacone o inteligentne aplikacje analityczne i wysokiej jakości szkolenia

Firma Axis zatrudnia około 4000 zaangażowanych pracowników w ponad 50 krajach i współpracuje z partnerami z sektora technologii oraz integracji systemów na całym świecie, aby dostarczać rozwiązania dla klientów. Firma Axis powstała w 1984 roku, a jej siedziba znajduje się w Lund w Szwecji