BIAŁA KSIĘGA

Październik 2026

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: podpisany system operacyjny, bezpieczny start i wideo z podpisem.

Podczas strumieniowego przesyłania materiału na żywo przez aplikację AXIS Body Worn Live organizacje mogą wybrać między wdrożeniem hostowanym przez firmę Axis (w chmurze) a wdrożeniem realizowanym we własnym zakresie (lokalnym). W obu przypadkach dane są szyfrowane w spoczynku i podczas przesyłania, a także w pełni szyfrowane od początku do końca bezpośrednio do klienta odbiorcy. Ponadto administrator ściśle kontroluje, kto może oglądać strumień na żywo, z dokładnością do konkretnego komputera, klienta i danych uwierzytelniających użytkownika.

Spis treści

1 Akronimy i terminologia 4
2 Wprowadzenie 4
3 Bezpieczeństwo w razie utraty kamery 4
4 Bezpieczeństwo przesyłania danych 4
5 Inne funkcje podnoszące bezpieczeństwo 5
6 Bezpieczeństwo z aplikacją AXIS Body Worn Live 6
6.1 Wdrożenie hostowane przez Axis 6
6.2 Wdrożenie z hostingiem samodzielnym 6

1 Akronimy i terminologia

BWC. Kamera nasobna

VMS. System zarządzania materiałem wizyjnym

EMS. Systemy 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. Pokazujemy również, w jaki sposób strumienie na żywo są szyfrowane za pomocą rozwiązania AXIS Body Worn Live w obu modelach jego wdrożenia.

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.

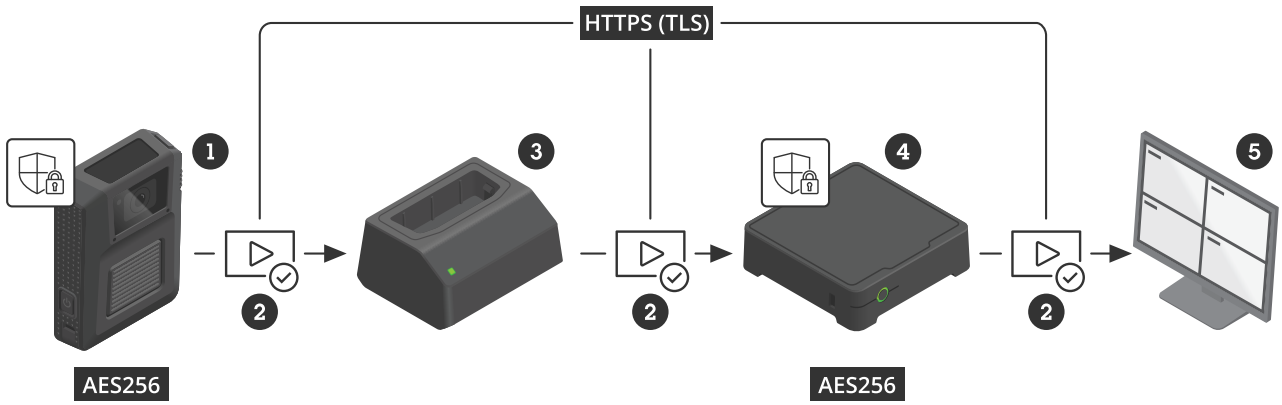
Kamera pozwoli na ściągnięcie danych tylko jednemu, konkretnemu kontrolerowi systemu lub systemowi, do którego należy. To zabezpieczenie realizowane jest w ten sposób, że kamera nasobna i kontroler systemu komunikują się ze sobą za pośrednictwem protokołu IPv6 i używają certyfikatów. Każdorazowo po zadokowaniu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

Jeśli kamera zostanie oddokowana i będzie pozostawać poza systemem przez osiem tygodni, ze względów bezpieczeństwa przełączy się w tryb bezpieczny i zablokuje połączenie. Aby kamera mogła ponownie uzyskać dostęp do systemu, konieczna jest weryfikacja manualna przy użyciu hasła klucza głównego. Dzięki temu kamery, 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 przechowywane w

kontrolerze systemu jedynie przez krótki czas, w jego pamięci masowej SSD szyfrowanej algorytmem AES-256. Następnie kontroler systemu przesyła dane przy użyciu 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. *Podpisany system operacyjny* sprawia, że urządzenia odrzucają uaktualnienia, jeśli integralność oprogramowania 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 na temat wideo z podpisem oraz rozwiązania Axis Edge Vault można znaleźć na stronach *developer.axis.com/video-streaming-and-recording/signed-video/* oraz *axis.com/solutions/edge-vault*

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.

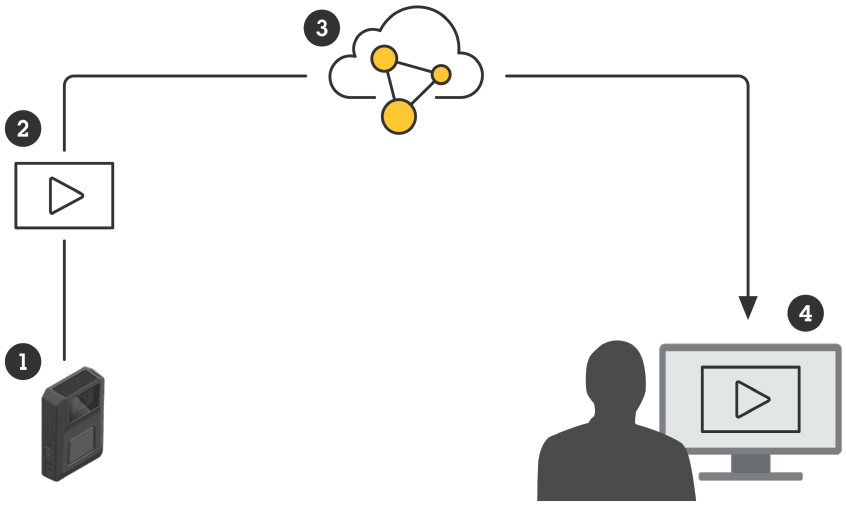
6 Bezpieczeństwo z aplikacją AXIS Body Worn Live

AXIS Body Worn Live to aplikacja umożliwiająca dostęp do danych przekazywanych na żywo z kamer nasobnych Axis. Udostępniając użytkownikom przesyłany na żywo strumień wideo, audio i innych danych, takich jak współrzędne położenia, aplikacja AXIS Body Worn Live zapewnia im wysoki poziom świadomości sytuacyjnej w trakcie incydentu. Aby sprostać różnym wymaganiom organizacyjnym w zakresie infrastruktury i suwerenności danych, jest ona dostępna w dwóch modelach wdrożenia: hostowana przez Axis oraz hostowana samodzielnie.

Niezależnie od modelu wdrożenia, administrator systemu kamer nasobnych ma pełną kontrolę nad tym, kto może oglądać strumień na żywo. Dane są szyfrowane w taki sposób, że tylko użytkownicy wyraźnie dopuszczeni przez administratora mogą deszyfrować i oglądać wideo. Administrator może również cofnąć uprawnienia dostępu przypisane na podstawie ról, aby chronić integralność danych. W przypadku wdrożeń hostowanych przez firmę Axis użytkownik musi mieć dostęp do zatwierdzonej przeglądarki internetowej, systemu VMS oraz odpowiednich danych uwierzytelniających. W przypadku wdrożeń hostowanych samodzielnie użytkownik musi mieć dostęp do sieci lokalnej oraz odpowiednich danych uwierzytelniających. Nikt inny, nawet firma Axis, nie ma dostępu do strumienia na żywo, a firma Axis nie ma dostępu do kluczy szyfrowania typu end-to-end utworzonych przez użytkowników.

6.1 Wdrożenie hostowane przez Axis

W przypadku korzystania z usługi w chmurze wszystkie dane i pliki hostowane w AXIS Body Worn Live są szyfrowane algorytmem AES-256 w stanie spoczynku. Wszystkie kanały komunikacji są zabezpieczone przy użyciu protokołu HTTPS z TLS, wykorzystującego certyfikaty podpisane przez zaufane urzędy certyfikacji. Oprócz szyfrowania podczas przesyłania, rozwiązanie AXIS Body Worn Live zapewnia dodatkową warstwę prawdziwego szyfrowania typu end-to-end przy użyciu protokołu XChaCha20-Poly1305.



Bezpieczne przesyłanie strumieniowe na żywo z szyfrowaniem end-to-end w ramach wdrożenia hostowanego przez firmę Axis

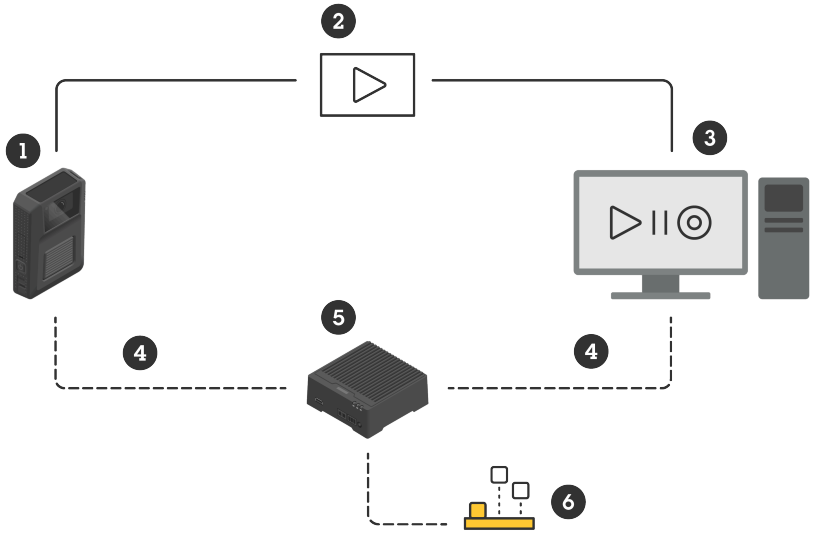
1. *Kamera nasobna rejestruje wideo na żywo oraz inne dane. Dane są szyfrowane już w kamerze.*
2. *Przesyłanie strumieniowe na żywo (szyfrowane na wszystkich etapach).*
3. *Chmura hostowana przez Axis. Dane i pliki są szyfrowane przy użyciu algorytmu AES-256.*
4. *Klient internetowy. Dane są odszyfrowywane w przeglądarce WWW użytkownika.*

6.2 Wdrożenie z hostingiem samodzielnym

Organizacje stosujące rygorystyczne zasady, zgodnie z którymi infrastruktura musi pozostawać w całości w obrębie kontrolowanych przez nie środowisk sieciowych, mogą zainstalować aplikację serwerową AXIS Body Worn Live, samodzielnie hostowaną lokalnie na urządzeniu. Urządzeniem serwerowym może być zestaw AXIS W401 Body Worn Activation Kit albo koncentrator AXIS D3110 Mk II Connectivity Hub. Na lokalnym

urządzeniu serwerowym nigdy nie są przechowywane w stanie spoczynku żadne materiały wideo ani dane wrażliwe; służy ono wyłącznie do utrzymania połączenia. Kanał komunikacyjny służący do przesyłania danych multimedialnych między kamerami a integracjami jest zabezpieczony za pomocą protokołu DTLS w wersji 1.0 lub nowszej. Kanał komunikacyjny służący do przesyłania sygnałów i zdarzeń między serwerem a integracjami jest zabezpieczony protokołem HTTPS przy użyciu certyfikatów dostarczonych przez klienta oraz protokołu TLS w wersji 1.2 lub nowszej.

Podczas przesyłania strumienia danych w wersji hostowanej samodzielnie lokalny serwer w bezpieczny sposób nawiązuje połączenie sygnalizacyjne WebRTC z uwierzytelnianiem opartym na certyfikatach między serwerem a kamerą nasobną. Po nawiązaniu połączenia, między kamerą nasobną a klientem WebRTC dozorcy (np. systemem VMS) tworzone jest zaszyfrowane połączenie typu peer-to-peer. Ponieważ strumień wideo jest przesyłany bezpośrednio przez to zaszyfrowane połączenie bez pośredniego przechowywania, uniemożliwia to jego nieuprawnione przechwycenie. System został zaprojektowany do pracy w zamkniętych, podzielonych na segmenty sieciach bez konieczności korzystania z dostępu do Internetu, co pozwala zminimalizować płaszczyznę ataku w przypadku zagrożeń zewnętrznych.



Bezpieczne strumieniowanie na żywo w ramach wdrożenia z hostingiem samodzielnym

1. *Kamera nasobna rejestruje wideo na żywo oraz inne dane. Dane są szyfrowane już w kamerze.*
2. *Strumień peer-to-peer (zaszyfrowany).*
3. *Klient WebRTC dozorcy.*
4. *Sygnalizacja WebRTC.*
5. *Urządzenie serwerowe AXIS Body Worn Live, Self Hosted.*
6. *Aplikacja serwerowa AXIS Body Worn Live, Self Hosted. Służy to do skonfigurowania sygnalizacji WebRTC.*

O firmie Axis Communications

Axis wspiera rozwój inteligentnego oraz bezpiecznego świata przez poprawę bezpieczeństwa, ochrony, efektywności działania i wiedzy biznesowej. Jako firma zajmująca się technologiami sieciowymi oraz lider branży, Axis oferuje rozwiązania z zakresu dozoru wizyjnego, kontroli dostępu, systemów domofonowych i systemów audio. Ich rozszerzeniem i uzupełnieniem są inteligentne aplikacje analityczne oraz wysokiej jakości szkolenia.

Axis zatrudnia około 5000 pracowników w ponad 50 krajach oraz współpracuje z partnerami z obszaru technologii i integracji systemów na całym świecie w celu dostarczania swoich rozwiązań klientom. Firma została założona w 1984 roku i ma swoją siedzibę w Lund w Szwecji.

© 2020 — 2026 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC i VAPIX są zarejestrowanymi znakami towarowymi firmy Axis AB w różnych jurysdykcjach. Wszystkie inne znaki towarowe są własnością odpowiednich podmiotów.Zastrzegamy sobie prawo do wprowadzania zmian bez uprzedniego powiadomienia.