BIAŁA KSIĘGA

Dane wizyjne jako materiał dowodowy

Zabezpieczanie integralności danych wizyjnych przy użyciu oprogramowania AXIS Camera Station

Lipiec 2021

AXIS COMMUNICATIONS

Spis treści

1 Streszczenie

Wysokiej jakości wiarygodne i niezmanipulowane dane wizyjne mogą posłużyć jako materiał dowodowy. Oto najlepsze praktyki dotyczące wykorzystania danych wizyjnych jako materiału dowodowego z udziałem oprogramowania AXIS Camera Station:

- Właściwe projektowanie, konfigurowanie i weryfikowanie systemu pod kątem uzyskania wymaganego obrazu, rodzaju nagrań oraz poziomu zabezpieczeń
- Regularna konserwacja
- Postępowanie z materiałem dowodowym według ustalonych procedur

2 Wprowadzenie

Materiał wizyjny pochodzący z systemu dozoru znakomicie nadaje się do wykorzystania jako dowód w sądzie. Przecież nikt nie zakwestionuje zdarzenia zarejestrowanego „na taśmie". Ale czy na pewno? Cóż, sędzia prawdopodobnie zaakceptuje dane wizyjne, jeśli będą one wysokiej jakości, wiarygodne i niezmanipulowane.

Są jednak czynniki, które obniżają wartość dowodową materiału wizyjnego. Przykładowo materiał z systemu dozoru, w którym występują luki czasowe albo w którym osoby lub pojazdy nagle znikają lub „przeskakują" z miejsca na miejsce, może zostać uznany za niewystarczająco wiarygodny w roli dowodu. Kolejnym powodem zakwestionowania materiału wizyjnego mogą być wątpliwości dotyczące metadanych, takich jak znaczniki czasowe czy adres MAC kamery. Każde podejrzenie, że materiał wizyjny mógł zostać zmodyfikowany, usunięty lub zmanipulowany, może zmniejszyć wiarygodność jego właściciela.

W tym dokumencie przedstawiono porady dotyczące sposobu zarządzania danymi wizyjnymi jako materiałem dowodowym. W szczególności omówiono rolę oprogramowania do zarządzania materiałem wizyjnym AXIS Camera Station w łańcuchu dowodowym, a także rolę właściciela materiału dowodowego.

Figure 1. System dozoru wizyjnego — rozmieszczony w strategicznych miejscach oraz prawidłowo skonfigurowany i zarządzany — może dostarczać wartościowy materiał dowodowy

3 Najlepsze praktyki dotyczące wykorzystania danych wizyjnych jako materiału dowodowego

Firmy i instytucje korzystające z systemów dozoru wizyjnego powinny wdrożyć procesy i procedury określające sposób postępowania z danymi wizyjnymi oraz ich przechowywania. Aby w pełni przygotować się na sytuację, gdy jedna z kamer wchodzących w skład systemu zarejestruje incydent, należy zadbać o ochronę materiału wizyjnego przed nadpisaniem, manipulacją i kradzieżą. Niezbędna jest także możliwość wyeksportowania materiału do bezpiecznej lokalizacji przechowywania i przekazania go organom ścigania.

Jednak tworzenie wysokiej jakości wizyjnego materiału dowodowego to proces, który zaczyna się od świadomego i przemyślanego zaprojektowania samego systemu wizyjnego. Niezmiernie ważne jest także bieżące aktualizowanie systemu i wychwytywanie ewentualnych nieprawidłowości. W tym rozdziale przedstawiono poszczególne kroki tego procesu oraz wyjaśniono, jak można je wykonać za pomocą oprogramowania AXIS Camera Station i związanego z nim pakietu narzędzi AXIS Camera Station Integrator Suite.

Jeśli materiał wizyjny z systemu dozoru będzie wytwarzany zgodnie z przedstawionymi tu zasadami dotyczącymi projektowania i konserwacji systemu oraz postępowania w razie incydentów, będzie

odpowiadał aktualnym wymaganiom z zakresu cyberbezpieczeństwa, a w razie potrzeby będzie stanowić wartościowy materiał dowodowy.

Figure 2. Oprogramowanie AXIS Camera Station ułatwia zarówno konfigurację i codzienną eksploatację systemu dozoru wizyjnego, jak i strategiczne zarządzanie tym systemem

3.1 Właściwe projektowanie systemu...

System dozoru wizyjnego należy projektować bardzo starannie. Trzeba wybrać sprzęt odpowiedni do potrzeb oraz skonfigurować go w celu uzyskania wymaganego obrazu, rodzaju nagrań i poziomu zabezpieczeń. Nieocenioną pomocą w tych aspektach jest narzędzie AXIS Site Designer.

3.1.1 W celu uzyskania wymaganego obrazu

Jakość obrazu zależy od kamery i jej umiejscowienia. Znając model kamery, obiektyw oraz odległość i kąt kamery w stosunku do obserwowanej sceny, można obliczyć rozdzielczość obrazu, a konkretnie gęstość pikseli w scenie. Do uzyskania odpowiedniej gęstości pikseli na twarzy obserwowanej osoby może być konieczne zastosowanie większej liczby kamer lub użycie kamer o wyższej rozdzielczości. Należy przeanalizować pole widzenia, wymagania oświetleniowe i inne parametry konkretnych kamer zastosowanych w danym obiekcie. Wszystko to można łatwo zaprojektować za pomocą narzędzia AXIS Site Designer.

3.1.2 W celu uzyskania wymaganego rodzaju nagrań

Do rejestrowania materiału wizyjnego należy używać wysokowydajnego, zweryfikowanego sprzętu z uwzględnieniem nadmiarowości. Aby zwiększyć niezawodność systemu, oprogramowanie AXIS Camera Station udostępnia tryb rejestrowania awaryjnego, który umożliwia czasowe przechowywanie obrazów na karcie SD kamery sieciowej. Jeśli klient korzysta z funkcji analiz z wizyjną detekcją ruchu, powinien

zadbać o to, by nagrania były wystarczająco długie i umożliwiały skuteczną weryfikację całego incydentu. Nieprawidłowa kalibracja rejestrowania z detekcją ruchu może doprowadzić do powstawania luk czasowych i przerw w zarejestrowanym materiale. W wielu przypadkach lepszym rozwiązaniem jest rejestrowanie ciągłe, ale wymaga ono znacznie więcej pamięci masowej, a także stałego dostępu do wystarczającej przepustowości.

3.1.3 W celu uzyskania wymaganego poziomu zabezpieczeń

W systemie należy zastosować niezbędne zabezpieczenia fizyczne, które uniemożliwią nieautoryzowany dostęp. Powinny one objąć wszystkie elementy sprzętowe, w tym kamery, urządzenia i kable sieciowe, serwery, pamięć masową, urządzenia zasilające oraz przewody. Zabezpieczenia mogą obejmować traktowanie serwerowni jako strefy zastrzeżonej, zamykanie szafy serwerowej na klucz, montaż serwera w stelażu, dezaktywację fizycznych portów w serwerze i schowanie kabli sieciowych.

Ponadto w systemie trzeba wprowadzić niezbędne cyberzabezpieczenia, aby ograniczyć ryzyko nadużycia danych, prób manipulowania danymi i złośliwych ataków. Do pewnego stopnia zabezpieczenia można wzmocnić przy użyciu odpowiednich narzędzi programowych i technologii, dzięki którym system będzie spełniać aktualne standardy bezpieczeństwa. Jednak do skutecznego wzmocnienia zabezpieczeń potrzebne jest także odpowiednie nastawienie właściciela systemu i aktywne promowanie go w całej firmie lub instytucji. Przykładowo wszyscy użytkownicy systemu muszą wiedzieć, jak ważne jest korzystanie z silnych, trudnych do odgadnięcia haseł, i uważać, by nikomu ich nie ujawnić. Warto ograniczyć dostęp użytkowników oraz ich uprawnienia, na przykład przez zastosowanie do ich kont zasady najniższych uprawnień. Do obowiązków właściciela systemu należy edukowanie pracowników w zakresie najlepszych praktyk oraz pilnowanie ich przestrzegania. Autoryzowany integrator może wzmocnić bezpieczeństwo systemu, ale niektóre cyberzabezpieczenia działają tylko przy aktywnej współpracy jego użytkowników.

Ważnym sposobem na ogólne zwiększenie skuteczności cyberzabezpieczeń jest ochrona materiału wizyjnego przy użyciu zaszyfrowanej transmisji danych. Jeśli chodzi o transmisję danych między klientem i serwerem, oprogramowanie AXIS Camera Station używa szyfrowania AES na potrzeby materiału wizyjnego, materiału dźwiękowego i metadanych oraz szyfrowania TLS 1.2 na potrzeby pozostałych danych. Ponadto w oprogramowaniu AXIS Camera Station można skonfigurować szyfrowanie strumieni danych między kamerami i serwerem przy użyciu protokołu HTTPS. Inne sprawdzone praktyki z zakresu ochrony oprogramowania obejmują wyłączanie wszelkich nieużywanych urządzeń, filtrowanie adresów IP/MAC, wdrożenie standardu IEEE 802.1X, wdrożenie monitorowania SNMP, ustawienie prawidłowej daty i godziny w połączeniu z zaufanym serwerem NTP (zapewnia to dokładność znaczników czasowych w metadanych wideo) oraz nawiązywanie połączeń zdalnych wyłącznie za pośrednictwem technologii Axis Secure Remote Access (a nie przy użyciu funkcji przekierowania portów czy pulpitu zdalnego). Szczegółowe informacje na temat środków i zaleceń z obszaru cyberbezpieczeństwa można znaleźć w poradniku Axis dotyczącym wzmacniania cyberzabezpieczeń.

3.1.4 Konfiguracja i weryfikacja systemu

Już na etapie projektowania systemu w narzędziu AXIS Site Designer można skonfigurować jego najważniejsze elementy, określając nazwy poszczególnych kamer, rozdzielczości i okresy przechowywania materiału. Po zaprojektowaniu i zainstalowaniu systemu konfiguracje określone w narzędziu AXIS Site Designer można automatycznie zaimportować do oprogramowania AXIS Camera Station, które w razie potrzeby umożliwia ich szczegółowe dostosowanie.

Po zakończeniu instalacji system można zweryfikować za pomocą narzędzia AXIS Installation Verifier, które wchodzi w skład pakietu AXIS Camera Station Integrator Suite. Narzędzie weryfikacyjne testuje system w trybie normalnym, a także w trybie nocnym, sprawdzając, czy dostępna jest wystarczająca przepustowość przy słabym oświetleniu, gdy poziom szumów jest wyższy, a zapotrzebowanie na przepustowość większe. Następnie AXIS Installation Verifier wykonuje test obciążeniowy, stopniowo zwiększając ilość danych

generowanych w systemie do czasu wykrycia pierwszego wąskiego gardła. Pozwala to ustalić pozostałą pojemność systemu i określić, czy potrzebne są w nim udoskonalenia.

3.2 Regularna konserwacja

Uruchomiony system wymaga stałego monitorowania i aktualizowania.

Trzeba dbać o to, by zarówno sprzęt, jak i oprogramowanie działały zgodnie z oczekiwaniami. Należy kontrolować jakość materiału wizyjnego, czyścić obiektywy kamer zgodnie z harmonogramem, a także sprawdzać, czy nie doszło do manipulacji fizycznej oraz czy kamery zachowują prawidłowe pole widzenia i kierunek. Warto także regularnie przeglądać dzienniki systemowe, ponieważ zawierają one informacje na temat logowań, połączeń i problemów z urządzeniami. Oprogramowanie AXIS Camera Station przekazuje powiadomienia o wielu rodzajach nieprawidłowości i zapisuje je w dziennikach systemowych. Zalecamy przekazywanie dzienników do zdalnej pamięci masowej przeznaczonej tylko do odczytu, zwłaszcza w przypadku wystąpienia ważnego incydentu. Ponadto Axis w ramach pakietu Integrator Suite udostępnia funkcję monitorowania stanu systemu online, która umożliwia klientowi monitorowanie wszystkich posiadanych instalacji oraz udostępnia informacje o stanie systemu, ułatwiając prace serwisowe i konserwacyjne.

Zarówno sprzęt, jak i oprogramowanie (system operacyjny oraz oprogramowanie do zarządzania materiałem wizyjnym) wymagają regularnych aktualizacji. Dzięki najnowszym wersjom oprogramowania aplikacyjnego i sprzętowego system może korzystać z najnowszych łat zabezpieczeń i poprawek błędów. W idealnych warunkach system zarządzania materiałem wizyjnym automatycznie znajduje wszystkie aktualizacje oprogramowania aplikacyjnego i sprzętowego, a następnie albo monituje o instalację aktualizacji, albo przeprowadza ją automatycznie. Wszelkie pobierane oprogramowanie powinno pochodzić z zaufanych źródeł.

3.3 Postępowanie z materiałem dowodowym według ustalonych procedur

Jeśli zasady dotyczące projektowania i konserwacji systemu dozoru zostaną wdrożone prawidłowo, oprogramowanie AXIS Camera Station powinno dostarczać wiarygodny materiał dowodowy na temat wszelkich incydentów rejestrowanych przez kamery. Niezbędne jest określenie procedur dalszego postępowania z tym materiałem.

Należy bezwzględnie zastosować się do ewentualnych wytycznych organów ścigania. W razie poważnego przestępstwa policja lub inny właściwy organ ma prawo zdecydować o sposobie zabezpieczenia materiału dowodowego: wówczas należy postępować ściśle według otrzymanych instrukcji.

W innych przypadkach kluczowym procesem jest bezpieczny eksport materiału dowodowego. Jego celem jest udostępnienie materiału na zewnątrz systemu tej samej niezmodyfikowanej, wiarygodnej formie, w jakiej znajduje się on wewnątrz systemu.

Operację eksportu powinien wykonywać wyznaczony operator, najlepiej w towarzystwie świadka. Operatorem może być specjalista zewnętrzny, zatrudniony wyłącznie w celu przeprowadzenia i udokumentowania wiarygodnej operacji eksportu. Zlecenie eksportu niezależnemu podmiotowi zewnętrznemu powinno zminimalizować ewentualne podejrzenia pod adresem właściciela danych wizyjnych, że manipulował materiałem dowodowym. Operator musi pamiętać, aby eksportowany materiał wizyjny nie tylko przedstawiał sam incydent, ale także zawierał wystarczająco dużo informacji na temat ewentualnych zdarzeń, które do niego doprowadziły, oraz jego ewentualnych następstw.

Wybrane klipy wideo można wyeksportować na płyty przeznaczone tylko do odczytu, takie jak CD-R, DVD-R lub Blu-ray (-R), które następnie zostaną przekazane organom ścigania. Inna możliwość to

wyeksportowanie klipów wideo do plików ZIP z zastosowaniem szyfrowania i ochrony hasłem. Pliki można podpisać cyfrowo przy użyciu podpisu zaszyfrowanego hasłem użytkownika. Aby potwierdzić klucz i porównać go z bieżącym kluczem pliku, należy wprowadzić podpis w aplikacji AXIS File Player. Jeśli klucze będą zgodne, będzie to oznaczać, że dane zawarte w bieżącym pliku nie zostały zmienione.

Axis udostępnia także operatorom zaawansowane narzędzie do eksportowania pod nazwą AXIS Camera Station Incident Report. Narzędzie to powinien najpierw skonfigurować administrator, podając takie dane jak znaczniki incydentów i lokalizacja eksportu. Następnie narzędzie automatyzuje operacje eksportu, umożliwiając eksportowanie plików wideo uporządkowanych według incydentów z użyciem znaczników jako nazw folderów. Jako lokalizację można określić zasób lokalny, na przykład sieciową pamięć masową (NAS), lub zasób zdalny, na przykład pamięć masową w chmurze, jeśli jest ona dostępna przy użyciu protokołu SMB. Wyeksportowany raport obejmuje pliki wideo, migawki w formacie .jpg (ręcznie utworzone przez operatora w oprogramowaniu AXIS Camera Station podczas przygotowywania raportu), zakładki w formacie .txt oraz wszystkie informacje zebrane w raporcie w formacie .pdf.

4 Zasoby z zakresu cyberbezpieczeństwa

Podczas projektowania, rozwijania i testowania swoich urządzeń Axis wprowadza w nich cyberzabezpieczenia, aby zminimalizować ryzyko powstania słabych punktów możliwych do wykorzystania w ataku. Stosujemy najlepsze praktyki branżowe z zakresu cyberbezpieczeństwa, na przykład dotyczące zarządzania lukami w zabezpieczeniach, wymagań odnoszących się do bezpiecznego przesyłania i przechowywania danych oraz szyfrowania. Staramy się ułatwić klientom ekonomiczne wdrażanie odpowiednich mechanizmów kontroli bezpieczeństwa, a nasze urządzenia obsługują szyfrowanie i zarządzanie zabezpieczeniami.

Chociaż Axis jako producent i dostawca systemu dokłada wszelkich starań, aby był on rozwiązaniem maksymalnie kompleksowym i bezpiecznym, duża odpowiedzialność spoczywa także na kliencie, który powinien u siebie wdrożyć najlepsze praktyki z obszaru bezpieczeństwa. Axis udostępnia szereg narzędzi, poradników i samouczków, które ułatwiają to zadanie. Zapraszamy na stronę www.axis.com/cybersecurity, na której można znaleźć na przykład poradniki dotyczące wzmacniania zabezpieczeń, informacje na temat zarządzania zabezpieczeniami oraz blog z artykułami z dziedziny cyberbezpieczeństwa.

T10169774/PL/M1.2/2107

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