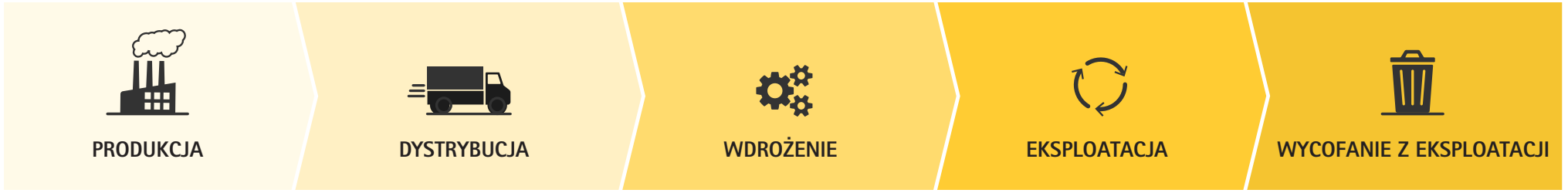
CYBERBEZPIECZEŃSTWO

Zarządzanie cyklem istnienia urządzeń

Na każdym etapie cyklu istnienia urządzenia sieciowego — od produkcji po wycofanie z eksploatacji — występuje ryzyko związane z cyberbezpieczeństwem. Jeśli jakiś czynnik tego ryzyka zostanie przeoczony, może spowodować zakłócenia funkcjonowania oraz utratę poufności, integralności i dostępności danych. Dlatego tak ważne jest, aby wszystkie związane z produktem podmioty, od dostawcy po klienta, dbały o zarządzanie ryzykiem.

Kwestie dotyczące cyklu istnienia zabezpieczeń urządzeń są więc naprawdę ważne z perspektywy zaopatrzenia. Producent powinien dysponować środkami umożliwiającymi ograniczenie zagrożeń dla cyberbezpieczeństwa, które występują przed dotarciem produktu do klienta, w czasie eksploatacji produktu, a także po jego wycofaniu z eksploatacji.

Na następnych stronach krótko przedstawiono technologie, narzędzia i wskazówki, a także podejścia i procesy, które Axis wspiera w celu ograniczenia ryzyka w całym cyklu istnienia urządzenia Axis.



Fundament bezpieczeństwa: Axis Edge Vault, AXIS OS, Axis Security Development Model

Fundament bezpieczeństwa — sprzęt, oprogramowanie i podejście

Ochrona integralności produktu i obniżenie ryzyka występowania luk w zabezpieczeniach od samego początku

Platforma cyberbezpieczeństwa Axis Edge Vault
Ta sprzętowa platforma obsługuje funkcje chroniące tożsamość i integralność urządzenia przed nieuprawnionym dostępem, dzięki czemu można bezpiecznie uruchomić i zintegrować urządzenie oraz zapewnić ochronę poufnych danych, na przykład kluczy.

System operacyjny AXIS OS
System AXIS OS jest używany w szerokiej gamie urządzeń Axis. Dzięki stosowaniu najlepszych praktyk branżowych w zakresie zarządzania lukami w zabezpieczeniach, AXIS OS stanowi platformę umożliwiającą szybkie i efektywne udostępnianie funkcji zabezpieczeń oraz poprawek oprogramowania dla ogromnej liczby produktów.

Axis Security Development Model (ASDM)
Jest to model rozwoju zabezpieczeń, czyli metodologia stosowana przez Axis w celu obniżenia ryzyka wydania produktów z lukami w zabezpieczeniach oprogramowania. ASDM sprawia, że kwestie bezpieczeństwa są integralnymi elementami prac nad oprogramowaniem, i obejmuje między innymi ocenę ryzyka, modelowanie zagrożeń, analizę kodu, testy penetracyjne, program nagród za wykryte błędy oraz skanowanie luk i zarządzanie nimi.

Transparentność
Budowanie zaufania jest ważnym aspektem pracy Axis. Axis jest organem numeracji w programie Common Vulnerability and Exposures (CVE). Publikujemy informacje i powiadamiamy wszystkie zainteresowane strony o lukach w zabezpieczeniach, aby klienci mogli podjąć odpowiednie działania. Publikujemy również programowy wykaz materiałów (software bill of materials – SBOM) dotyczący systemu AXIS OS.

PRODUKCJA I DYSTRYBUCJA

Obniżanie ryzyka zastosowania niezabezpieczonych elementów

- **Łańcuch dostaw:** kluczowe elementy są nabywane bezpośrednio od dostawców strategicznych. Axis ściśle współpracuje z partnerami produkcyjnymi. Procesy produkcyjne są monitorowane, a dane są przekazywane Axis w trybie 24/7, co pozwala na ich analizowanie w czasie rzeczywistym i zapewnia transparentność.
- **Axis Edge Vault:** moduł Axis Edge Vault, instalowany w urządzeniu Axis na etapie produkcji, zawiera następujące funkcje:
  - **Bezpieczny magazyn kluczy**, który używa kryptograficznych modułów obliczeniowych (takich jak bezpieczny element, Trusted Platform Module i Trusted Execution Environment) do skutecznego chronienia przechowywanych kluczy przed manipulacjami.
  - **Podpisane oprogramowanie sprzętowe**, które gwarantuje, że zainstalowany system operacyjny AXIS OS pochodzi od firmy Axis. Rozwiązanie to zapewnia, że każde nowe oprogramowanie sprzętowe, które ma zostać pobrane i zainstalowane na urządzeniu, również jest podpisane przez Axis.
  - **Bezpieczny start**, dzięki któremu urządzenie może sprawdzić, czy dane oprogramowanie sprzętowe zawiera podpis Axis. Jeśli oprogramowanie sprzętowe nie jest autoryzowane lub zostało zmodyfikowane, uruchamianie zostanie przerwane i urządzenie przestanie działać. Połączenie podpisanego oprogramowania sprzętowego, bezpiecznego startu i przywrócenia ustawień fabrycznych na urządzeniu stanowi linię obrony przed ewentualnymi złośliwymi modyfikacjami wprowadzonymi w czasie transportu urządzenia.
  - **Identyfikator urządzenia Axis**, czyli unikatowy dla urządzenia certyfikat i powiązane z nim klucze, za pomocą których można potwierdzić autentyczność urządzenia Axis. Zgodnie ze standardem IEEE 802.1AR identyfikator urządzenia Axis umożliwia bezpieczną identyfikację urządzenia i wdrożenie go w sieci.
  - **Zaszyfrowany system plików**, który chroni specjalne konfiguracje klienta i informacje przechowywane w systemie plików przed wykradzeniem lub zmanipulowaniem, gdy urządzenie nie jest używane, na przykład w drodze od integratora systemu do klienta.

WDROŻENIE

Eliminowanie ryzyka związanego z wprowadzeniem do sieci niezabezpieczonych lub nieodpowiednio chronionych produktów, co może skutkować nieuprawnionym dostępem, wykradzeniem poufnych danych i przesłaniem zmienionych danych między urządzeniami końcowymi w sieci

- **Przywrócenie domyślnych ustawień fabrycznych:** przed przystąpieniem do konfigurowania urządzenia należy przywrócić jego domyślne ustawienia fabryczne. Daje to pewność, że urządzenie jest całkowicie wolne od niechcianego oprogramowania i ustawień konfiguracyjnych, ponieważ pozostanie w nim wyłącznie system AXIS OS i jego ustawienia domyślne.
- **Sprawdzenie, czy jest dostępne nowsze oprogramowanie sprzętowe urządzenia:** między produkcją a wdrożeniem mogło upłynąć trochę czasu, więc warto sprawdzić w witrynie internetowej Axis, czy jest dostępne nowsze oprogramowanie sprzętowe, które może zawierać najnowsze poprawki błędów przeznaczone dla danego urządzenia.
- **Identyfikator urządzenia Axis:** aby w sieci zostały wdrożone wyłącznie oryginalne urządzenia Axis, warto zweryfikować identyfikator urządzenia Axis przy użyciu funkcji uwierzytelniania IEEE 802.1X lub podczas nawiązywania bezpiecznego połączenia sieciowego za pośrednictwem protokołu HTTPS. W sieci IEEE 802.1X identyfikator urządzenia Axis pozwala zwiększyć bezpieczeństwo i przyspieszyć wdrożenie.
- **Bezpieczny magazyn kluczy:** korzystając z kryptograficznych modułów obliczeniowych, bezpieczny magazyn kluczy przechowuje poufne informacje, takie jak identyfikator urządzenia Axis i klucze załadowane przez klienta, uniemożliwiając uzyskanie nieuprawnionego dostępu i złośliwe wykradzenie poufnych informacji nawet w przypadku złamania zabezpieczeń urządzenia.
- **Zaszyfrowany system plików:** gwarantuje, że żadne dane przechowywane w systemie plików nie mogą zostać wykradzione ani zmanipulowane w czasie, gdy urządzenie nie jest używane.
- **Wskazówki dotyczące wzmacniania zabezpieczeń:** w Przewodniku po zabezpieczeniach systemu AXIS OS, dostępnym w portalu AXIS OS w witrynie internetowej Axis, określono podstawową konfigurację, która uwzględnia typowe zagrożenia, i przedstawiono najlepsze praktyki oraz porady techniczne. Dostępne są też przewodniki po zabezpieczeniach dotyczące oprogramowania do zarządzania materiałem wizyjnym AXIS Camera Station oraz przełączników sieciowych Axis.
- **Przewodnik po skanerze zabezpieczeń systemu AXIS OS:** Axis zaleca skanowanie zabezpieczeń urządzenia Axis w celu sprawdzenia, czy nie ma ono luk w zabezpieczeniach lub słabej konfiguracji. Przewodnik po skanerze zabezpieczeń systemu AXIS OS zawiera zalecenia dotyczące obsługi niektórych zgłoszeń ze skanera i przedstawia najczęstsze „fałszywe alarmy".
- **AXIS Device Manager:** narzędzie to pozwala na efektywną konfigurację urządzeń Axis i lokalne zarządzanie nimi. Umożliwia ono zbiorcze wykonywanie zadań z zakresu instalacji i ochrony bezpieczeństwa, takich jak zarządzanie poświadczeniami urządzeń, wdrażanie certyfikatów, wyłączanie nieużywanych usług i aktualizowanie systemu AXIS OS.

EKSPLOATACJA

Eliminowanie ryzyka związanego z uruchamianiem oprogramowania sprzętowego ze znanymi lukami w zabezpieczeniach, aktualizowaniem urządzeń przy użyciu nieuwierzytelnionego oprogramowania sprzętowego lub naruszaniem bezpiecznych konfiguracji

- **Uaktualnianie oprogramowania sprzętowego:** konieczne jest podtrzymywanie cyberbezpieczeństwa urządzenia Axis przez aktualizowanie oprogramowania sprzętowego przy użyciu aktywnej ścieżki systemu AXIS OS lub ścieżki wsparcia długoterminowego. Udostępniane bezpłatnie aktualizacje oprogramowania sprzętowego z użyciem dowolnej z tych ścieżek będą zawierać poprawki zabezpieczeń. Podpisane oprogramowanie sprzętowe daje pewność, że może zostać zainstalowane tylko oryginalne oprogramowanie sprzętowe Axis.
- **AXIS Device Manager Extend:** narzędzie to, uzupełniające narzędzie AXIS Device Manager, umożliwia zdalne zarządzanie urządzeniami AXIS i upraszcza skalowanie zadań związanych z konserwacją, takich jak aktualizacja oprogramowania sprzętowego urządzeń.
- **Zarządzanie lukami w zabezpieczeniach:** Axis udostępnia usługę powiadomień dotyczących bezpieczeństwa, w której można się zarejestrować, aby otrzymywać informacje o lukach w zabezpieczeniach i innych kwestiach związanych z zabezpieczeniami.
- **Przewodnik po pracach wyjaśniających w systemie AXIS OS:** przewodnik ten zawiera porady techniczne dotyczące wykonywania analiz na potrzeby prac wyjaśniających związanych z urządzeniami Axis w razie cyberataku na sieć i infrastrukturę IT, w której jest zainstalowane dane urządzenie Axis.
- **Podpisany materiał wizyjny:** w przypadku włączenia tej funkcji w obsługiwanej kamerze do strumienia wideo są dodawane podpisy kryptograficzne, zanim opuści on urządzenie, co umożliwia oglądającym sprawdzenie, czy materiał wizyjny nie został zmanipulowany. Jest to szczególnie ważne z perspektywy prac wyjaśniających lub postępowania sądowego.

WYCOFANIE Z EKSPLOATACJI

Eliminowanie ryzyka związanego z urządzeniami, które nie są już obsługiwane i mają nieusunięte znane luki, a także z poufnymi danymi pozostawionymi na urządzeniach wycofanych z eksploatacji

- **Termin zakończenia wsparcia technicznego dla oprogramowania sprzętowego:** na stronie internetowej pomocy technicznej dotyczącej wielu produktów w witrynie Axis.com można znaleźć termin zakończenia wsparcia technicznego dla oprogramowania sprzętowego danego produktu, co pozwala klientom na zaplanowanie wycofania i wymiany produktu w odpowiednim czasie.
- **AXIS Device Manager Extend:** narzędzie to umożliwia łatwe monitorowanie statusu gwarancji wszystkich urządzeń w danym systemie, w tym informacji o zaprzestaniu produkcji i zakończeniu wsparcia technicznego. Informacje te pozwalają przygotować urządzenie do wycofania z eksploatacji i wyeliminować ryzyko związane z użytkowaniem urządzenia pozbawionego wsparcia.
- **Wskazówki:** portal AXIS OS w witrynie internetowej Axis zawiera wskazówki dotyczące wycofywania urządzenia Axis z eksploatacji. Przywrócenie domyślnych ustawień fabrycznych urządzenia powoduje wymazanie z niego wszystkich konfiguracji i danych.

Więcej informacji można znaleźć na stronie: **www.axis.com/about-axis/cybersecurity**