AXIS COMMUNICATIONS

Cyberbezpieczeństwo

WSPÓLNE ZAPEWNIANIE LEPSZEJ OCHRONY CYBERNETYCZNEJ

AXIS COMMUNICATIONS

SPIS TREŚCI

WSPÓLNY OBOWIĄZEK 3

NAJCZĘSTSZE CYBERZAGROŻENIA 4

Bezpieczeństwo fizyczne i cyberbezpieczeństwo — dwie strony jednego medalu 4

Na jakie zagrożenia uważać? 5

Łatwowierność i nieumyślne błędy ludzkie 6

Świadome użytkowanie systemu w sposób niewłaściwy 7

Ingerencje fizyczne lub próby sabotażu 8

Wykorzystywanie luk w oprogramowaniu 9

UWAGI DOTYCZĄCE CYBERBEZPIECZEŃSTWA 10

Co powinni uwzględnić klienci, aby ograniczyć ryzyko? 10

Co musisz wiedzieć o swoim dostawcy systemu dozoru — oraz o jego dostawcach? 11

Partnerzy łańcucha dostaw 12

Jaki jest poziom bezpieczeństwa produkcji u Twojego dostawcy? 13

Sieci „zero trust" 14

Czas na aparat zasad... 15

Dlaczego skuteczne zarządzanie cyklem istnienia ma kluczowe znaczenie 16

PODEJŚCIE AXIS DO CYBERBEZPIECZEŃSTWA 17

Fundament bezpieczeństwa 18

Uporządkowane i systemowe podejście do bezpieczeństwa wewnętrznego 18

Ochrona integralności produktów i ograniczanie ryzyka luk w oprogramowaniu 19

Zarządzanie nowo wykrytymi lukami 21

Produkcja i dystrybucja 22

Ograniczanie ryzyka komponentów sprzętowych i programowych z naruszonymi zabezpieczeniami 22

Wbudowane cyberzabezpieczenia 23

Wdrożenie 25

Cyberbezpieczeństwo podczas wdrożenia 25

Eksploatacja 26

Cyberbezpieczeństwo urządzeń podczas eksploatacji 26

Wycofanie z eksploatacji 28

Planowanie wycofania z eksploatacji 28

ZGODNOŚĆ Z PRZEPISAMI 29

DLACZEGO AXIS? 30

Ograniczanie ryzyka cyberincydentów

Ochrona produktów sieciowych i usług oprogramowania przed cyberzagrożeniami jest kluczowa dla zabezpieczenia danych i systemów w każdej sieci. System, którego zabezpieczenia zostały naruszone, może powodować utratę poufności i integralności danych lub uniemożliwiać dostęp do danych, gdy będzie on potrzebny.

Ponieważ jesteśmy odpowiedzialnym partnerem w obszarze cyberbezpieczeństwa, opracowaliśmy zestaw uwag i wytycznych ułatwiających zakup oraz zabezpieczanie produktów bezpieczeństwa fizycznego opartych na protokole IP. Chcemy ułatwić wprowadzanie zabezpieczeń, aby z rozwiązań Axis można było korzystać w jak najbezpieczniejszy sposób.

Poza kolejnymi stronami tego dokumentu więcej informacji na temat cyberbezpieczeństwa i tego, jak możemy wspólnie dbać o lepszą ochronę cybernetyczną, znajduje się na stronie www.axis.com/cybersecurity

Wspólny obowiązek

Cyberbezpieczeństwo dotyczy produktów, ludzi, technologii i bieżących procesów. Nie ulega wątpliwości, że wszyscy musimy połączyć siły, aby każde ogniwo łańcucha cyberbezpieczeństwa było jak najmocniejsze. Cyberbezpieczeństwo należy traktować jako wspólny obowiązek, którego realizacja wymaga współpracy poniższych podmiotów, w tym klientów.

Producenci urządzeń

Cyberbezpieczeństwo zaczyna się właśnie od nich. Producenci powinni stosować najlepsze praktyki związane z cyberbezpieczeństwem podczas projektowania, prac rozwojowych, produkcji oraz konserwacji oprogramowania, aby zminimalizować ryzyko wystąpienia wad w całym cyklu istnienia produktu. Ważne jest ścisłe kontrolowanie ich własnego łańcucha dostaw. Produkty powinny mieć wbudowane funkcje umożliwiające wdrażanie różnych mechanizmów kontroli bezpieczeństwa. Powinny istnieć narzędzia do sprawnego konfigurowania urządzeń i zarządzania nimi, które współgrają z procesami lub zasadami bezpieczeństwa stosowanymi przez klienta. Powinny także istnieć kanały informowania partnerów i klientów o nowo wykrytych lukach.

Dystrybutorzy

W przypadku dystrybutorów, którzy nie mają bezpośredniego kontaktu z obsługiwanymi produktami, kwestia cyberbezpieczeństwa jest stosunkowo prosta. Jednak dystrybutorzy oferujący wartość dodaną muszą pamiętać o tych samych kwestiach, które dotyczą integratorów i instalatorów — zwłaszcza w sytuacjach, w których kupują sprzęt od producenta, a następnie sprzedają go pod inną (lub własną) marką. Transparentność to podstawa. Pochodzenie sprzętu nie może pozostawiać żadnych wątpliwości.

Doradcy, integratorzy i instalatorzy

Mogą pomóc klientom w identyfikacji, projektowaniu i wdrażaniu mechanizmów kontroli bezpieczeństwa oraz dbaniu o to, by urządzenia bezpieczeństwa fizycznego nie były słabym punktem sieci klienta. Może to obejmować opracowanie strategii dotyczącej haseł, zarządzania dostępem zdalnym oraz konserwacji oprogramowania i połączonych urządzeń. Może też obejmować dbanie o to, by w zainstalowanym sprzęcie były stosowane najnowsze poprawki i aktualizacje, a system był regularnie skanowany na obecność wirusów. Trudności towarzyszące użytkowaniu sprzętu OEM/ODM — w przypadku którego podział obowiązków w zakresie cyberbezpieczeństwa bywa niejasny — powinny stanowić część ogólnej dyskusji na temat bezpieczeństwa cybernetycznego.

Klienci końcowi

Potrzeby każdej organizacji w zakresie cyberbezpieczeństwa są specyficzne i niepowtarzalne. Nie istnieje coś takiego jak „uniwersalna" konfiguracja cyberzabezpieczeń. Dlatego należy opracować zasady dotyczące bezpieczeństwa informacji, które określałyby zakres wymaganych zabezpieczeń. Usunięcie kont domyślnych, ustawienie unikatowych i silnych haseł — przechowywanych bezpiecznie i regularnie zmienianych — przydzielenie odpowiednich uprawnień oraz instalowanie wszystkich aktualizacji i poprawek: to tylko kilka niezbędnych kroków.

Badacze

Często to właśnie oni wykrywają słabe punkty urządzeń. Jeśli takie słabości lub luki nie są celowe, badacz zazwyczaj informuje o nich producenta i pozwala je wyeliminować przed opublikowaniem stosownego komunikatu. Jeśli jednak luka ma charakter krytyczny i wygląda na pozostawioną celowo, badacze często powiadamiają o niej użytkowników za pośrednictwem publicznego komunikatu.

Bezpieczeństwo fizyczne i cyberbezpieczeństwo — dwie strony jednego medalu

Większość osób doskonale rozumie specyfikę zagrożeń fizycznych. Przez niezamknięte drzwi mogą przemknąć niepowołane osoby. Cenne rzeczy pozostawione na widoku łatwo ukraść. Błędy i wypadki mogą powodować urazy lub szkody materialne. Kwestie bezpieczeństwa fizycznego i cyberbezpieczeństwa wymagają niemal identycznego podejścia.

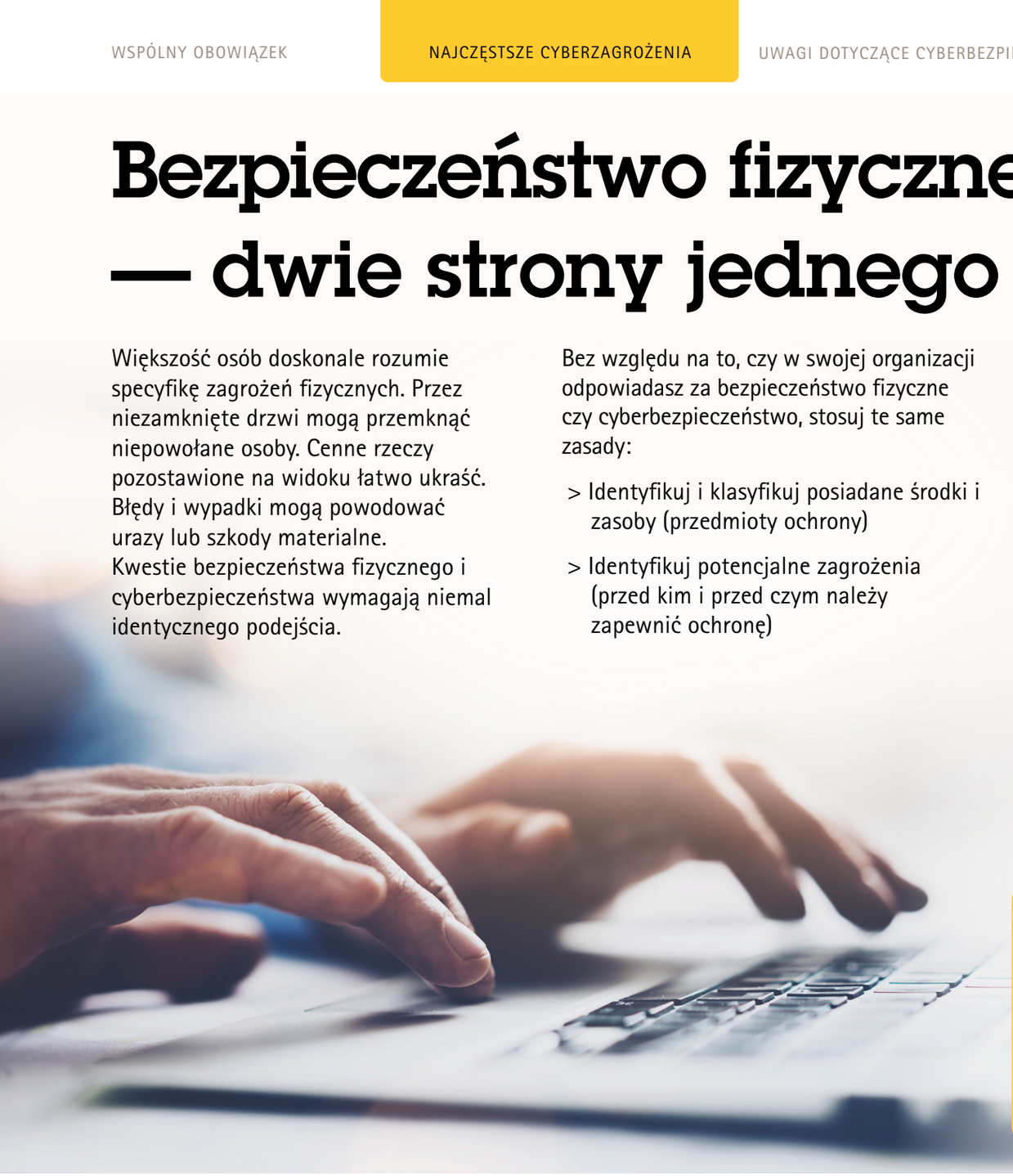
Bez względu na to, czy w swojej organizacji odpowiadasz za bezpieczeństwo fizyczne czy cyberbezpieczeństwo, stosuj te same zasady:

> Identyfikuj i klasyfikuj posiadane środki i zasoby (przedmioty ochrony)

> Identyfikuj potencjalne zagrożenia (przed kim i przed czym należy zapewnić ochronę)

> Identyfikuj słabe punkty, które mogą zostać wykorzystane (prawdopodobieństwo)

> Identyfikuj potencjalne koszty niekorzystnego scenariusza (konsekwencje). Ryzyko często definiuje się jako iloczyn prawdopodobieństwa wystąpienia zagrożenia oraz poniesionych szkód. Po ustaleniu ryzyka należy się zastanowić, w jaki sposób można zapobiec jego negatywnym skutkom.



Co to jest cyberbezpieczeństwo?

Cyberbezpieczeństwo to ochrona systemów i usług komputerowych przed cyberzagrożeniami. Praktyki z zakresu cyberbezpieczeństwa obejmują procesy zapobiegania szkodom oraz przywracania komputerów, systemów i usług łączności elektronicznej, komunikacji przewodowej i elektronicznej oraz przechowywanych informacji w celu zapewnienia ich poufności, integralności, dostępności, bezpieczeństwa i niezaprzeczalności.

Na jakie zagrożenia uważać?

Kluczowymi elementami ochrony systemu IT (technologii informatycznej) lub OT (technologii operacyjnej) są poufność, integralność, dostępność i bezpieczeństwo. Każda sytuacja, która niekorzystnie wpływa na którykolwiek z nich, stanowi incydent naruszający cyberbezpieczeństwo.

Przyjrzyjmy się najczęstszym zagrożeniom cyberbezpieczeństwa i słabym punktom, które sprzyjają naruszeniom. Systemy bezpieczeństwa fizycznego oparte na protokole IP są narażone na cztery najczęstsze cyberzagrożenia:

1. **Łatwowierność i nieumyślne błędy ludzkie**
2. **Świadome użytkowanie systemu w sposób niewłaściwy**
3. **Ingerencje fizyczne i próby sabotażu**
4. **Wykorzystywanie luk w oprogramowaniu**

1 Łatwowierność i nieumyślne błędy

Niezależnie od tego, jak znakomita technologia służy do ochrony systemu, jednym z głównych czynników w naruszeniach zabezpieczeń jest element ludzki.

Błędy ludzkie, które otwierają drogę do cyberataku, to m.in.:

> **Socjotechnika**
Polega na zmanipulowaniu użytkownika w taki sposób, że ten łamie zasady bezpieczeństwa lub udostępnia wrażliwe informacje. Przykładami zastosowania socjotechniki są phishing i oprogramowanie scareware.

> **Niewłaściwe korzystanie z haseł**
Obejmuje brak korzystania z silnych haseł czy brak odpowiedniej ochrony i/lub aktualizacji haseł.

> **Niewłaściwe obchodzenie się z krytycznymi elementami**
Polega na utracie lub zagubieniu przedmiotu umożliwiającego dostęp do systemu, takiego jak karta dostępu, telefon, laptop czy dokumentacja.

> **Słabe zarządzanie systemem**
Polega na nieinstalowaniu aktualizacji systemu i poprawek zabezpieczeń.

> **Nieudane usprawnienia**
Spadek wydajności systemu spowodowany samodzielną próbą naprawienia usterki.

Słabe punkty a błędy ludzkie

Niedostateczna wiedza na temat cyberprzestrzeni oraz brak zasad i długoterminowych procesów zarządzania ryzykiem to najczęstsze słabości, które wynikają z błędów człowieka. Aby zmniejszyć ryzyko popełnienia błędu przez człowieka, każdy członek organizacji powinien zapoznać się ze sprawdzonymi procedurami w dziedzinie bezpieczeństwa cybernetycznego. Ponadto dostęp do urządzeń sieciowych należy ograniczyć do kilku zaufanych osób za pośrednictwem systemu do zarządzania materiałem wizyjnym lub menedżera urządzeń.

2 Świadome użytkowanie systemu w sposób niewłaściwy

Kolejnym nazbyt częstym cyberzagrożeniem jest świadome korzystanie z systemu w sposób niewłaściwy przez jego uprawnionych użytkowników.

Umyślne łamanie zasad obejmuje następujące działania:

Manipulowanie usługami i zasobami systemowymi

Kradzież danych

Celowe uszkadzanie systemu

Słabe punkty a świadome łamanie zasad
To ważne, aby wdrożyć zasady i długofalowe procesy pomagające zarządzać słabymi punktami i lukami oraz ograniczać ryzyko celowego niewłaściwego korzystania z systemu. Istotna jest właściwa weryfikacja osób mających uprawnienia dostępu do wrażliwych danych, a także ograniczenie liczby osób z takimi uprawnieniami.

Oprogramowanie służące do zarządzania urządzeniami bezpieczeństwa fizycznego podłączonymi do sieci, takimi jak kamery, powinno korzystać z konta administratora z własnymi poświadczeniami.
Powinno to być konto unikatowe i nie współużytkowane. Operatorzy lokalizacji powinni mieć indywidualne konta w oprogramowaniu do zarządzania. Żadna osoba nie powinna mieć bezpośredniego dostępu do fizycznych urządzeń bezpieczeństwa. Jeśli wystąpi okoliczność uzasadniająca przyznanie bezpośredniego dostępu, należy go przyznać czasowo.

3 Ingerencje fizyczne lub próby sabotażu

Fizyczna ochrona jest niezwykle ważna z perspektywy cyberbezpieczeństwa:

> Wyeksponowany sprzęt jest narażony na niepowołane ingerencje.

> Wyeksponowany sprzęt może zostać skradziony.

> Wyeksponowane kable mogą zostać rozłączone, przekierowane lub przecięte.

Słabe punkty a zagrożenia fizyczne

Typowe słabe punkty obejmują sprzęt sieciowy, taki jak serwery czy przełączniki, umieszczony w ogólnodostępnych miejscach, kamery bez obudowy ochronnej, które pozostają w zasięgu użytkowników, czy przewody niezabezpieczone ścianami ani kanałami. Ponadto urządzenia sieciowe mogą otwierać drogę do innych zasobów w tej samej sieci.

Pamiętaj o konsekwencjach

Systemy wizyjne, dźwiękowe i kontroli dostępu nie przetwarzają transakcji finansowych ani nie przechowują danych klientów. To oznacza, że atak wymierzony w taki system nie przynosi bezpośrednich korzyści finansowych, a więc z perspektywy cyberprzestępczości zorganizowanej jest średnio opłacalny. Jednak system, którego zabezpieczenia zostały naruszone, może stanowić zagrożenie dla innych systemów. Dlatego tak naprawdę trudno oszacować koszty ataku. Niestety w wielu przypadkach organizacje przekonują się o tym na własnej skórze. Z ochroną jest jak z jakością — otrzymuje się to, za co się płaci. A zakup taniego systemu może doprowadzić do znacznie wyższych długofalowych kosztów, jeśli dostawcy nie uwzględnili cyberbezpieczeństwa w całym cyklu istnienia produktów.

4 Wykorzystywanie luk w oprogramowaniu

W obszarze rozwoju oprogramowania występują pewne czynniki ryzyka — najczęściej błędy kodu — które mogą prowadzić do powstawania luk w zabezpieczeniach (tzw. podatności) możliwych do wykorzystania podczas ataku. Im większa liczba luk występuje w oprogramowaniu, tym większe jego narażenie na ataki. Zanim producent zacznie wprowadzać oprogramowanie na rynek, powinien wdrożyć model prac rozwojowych obejmujący procesy i narzędzia, które minimalizują ryzyko powstawania luk na wszystkich etapach tworzenia oprogramowania.

Chociaż w branży trudno spotkać oprogramowanie całkowicie wolne od błędów, producenci powinni dążyć do identyfikacji i usuwania błędów kodu i innych nieprawidłowości implementacji, które zagrażają bezpieczeństwu, oraz informowania o nich klientów. Dlatego producent musi jasno komunikować nowo wykryte luki w oprogramowaniu i w szybkim czasie oferować klientom stosowne rozwiązania. Natomiast po stronie klienta ważne jest regularne wdrażanie aktualizacji oprogramowania zawierających ulepszenia zabezpieczeń i poprawki błędów bezpośrednio po ich udostępnieniu przez producenta.

Co powinni uwzględnić klienci, aby ograniczyć ryzyko?

Przede wszystkim na etapie zakupu produktów bezpieczeństwa fizycznego z uwzględnieniem cyberbezpieczeństwa należy uwzględnić kilka aspektów.

Po pierwsze należy przeanalizować podejście dostawcy produktów do cyberbezpieczeństwa: czy wdrożył w firmie zasady dotyczące cyberbezpieczeństwa, zgodnie z którymi stale identyfikuje i ocenia posiadane zasoby i przeprowadza związane z nimi oceny ryzyka? Ważne jest także poznanie sposobu współpracy dostawcy z podmiotami w łańcuchu dostaw. Ponadto czy projektowane i wytwarzane przez niego produkty zawierają wbudowane cyberzabezpieczenia?

Jakie środki i mechanizmy wsparcia cyberbezpieczeństwa oferuje producent w całym cyklu istnienia produktu sieciowego? A jeśli dojdzie do ataku na system? Czy dostawca udostępnia wytyczne, które pomagają w reakcji na cyberincydent z udziałem jego produktów?

To zaledwie kilka kwestii, które należy wziąć pod uwagę. Bardziej szczegółowe informacje podamy na dalszych stronach.

Co musisz wiedzieć o swoim dostawcy systemu dozoru — oraz o jego dostawcach?

Zagrożenia bezpieczeństwa są stale obecne. Wciąż pojawiają się nowe, a dotychczasowe mogą się w każdej chwili zmienić. Wiele organizacji koncentruje się wyłącznie na tym, jak dostawcy oceniają te zagrożenia i jak im przeciwdziałają. Ale co z dostawcami dostawców? W jaki sposób dostawcy kontrolują i utrzymują cały łańcuch dostaw, dbając o bezpieczeństwo produktów od etapu wytwarzania poszczególnych komponentów po sprzedaż gotowego produktu?

Czy Twój dostawca dąży do minimalizacji ryzyka?

> Czy kontroluje cały łańcuch dostaw, od etapu wytwarzania komponentów po sprzedaż gotowego produktu?

> Czy ma model rozwoju oprogramowania, którego integralną częścią są kwestie bezpieczeństwa?

> Czy projektuje i wytwarza produkty z wbudowanymi zabezpieczeniami?

> Czy dzieli się wiedzą i narzędziami dotyczącymi stosowanych mechanizmów ochronnych?

> Czy zapewnia szybką reakcję i bezpłatne aktualizacje w przypadku nowo wykrytych luk w oprogramowaniu?

Partnerzy łańcucha dostaw

Bezpieczeństwo łańcucha dostaw zaczyna się od wyboru właściwych, podlegających rygorystycznej ocenie partnerów. Proces ewaluacji powinien obejmować analizę jakości każdej firmy i jej procedur zarządzania rozwojem. Partner powinien posiadać co najmniej certyfikat ISO 9001 lub IATF 16949.

Ocena poddostawców

Wybrany dostawca powinien poddawać ocenie procedury zarządzania ryzykiem u własnych dostawców, a także ich zakłady i procesy produkcyjne. Powinien przeprowadzać wizyty i audyty lokalne mające na celu ocenę, czy zakłady spełniają określone wymogi i standardy dotyczące kwalifikacji zatwierdzonych dostawców. W ramach ewaluacji potencjalnego nowego partnera w łańcuchu dostaw należy wykonać szczegółową analizę sytuacji finansowej i struktury właścicielskiej poddostawców.

Strategiczni poddostawcy

Współpraca z dostawcami kluczowych komponentów i partnerami produkcyjnymi zwykle jest bliska i długotrwała. Pełnią oni rolę strategicznych poddostawców, z którymi Twój dostawca realizuje wspólne projekty i działania rozwojowe, wyznacza cele oraz decyduje się na długotrwałe wzajemne zobowiązania i plany. Zakup wszystkich komponentów kluczowych dla produktów Twojego dostawcy powinien odbywać się bezpośrednio u strategicznego poddostawcy. Ponadto dostawca powinien zadbać o ich magazynowanie we własnych obiektach. Komponenty inne niż kluczowe mogą być nabywane przez partnerów produkcyjnych, ale jedynie od podmiotów znajdujących się na liście zatwierdzonych dostawców.

Jaki jest poziom bezpieczeństwa produkcji u Twojego dostawcy?

> Czy procesy produkcji są ściśle określone i monitorowane?

> Czy dostawca zajmuje się projektowaniem i wytwarzaniem kluczowych urządzeń produkcyjnych?

> Czy dostawca stosuje system testowania komponentów, modułów i produktów na etapie produkcji, wraz z odpowiednim oprogramowaniem, komputerami testowymi oraz innym sprzętem IT?

> Czy dostawca pozyskuje dane produkcyjne na bieżąco, tak by analizować je w czasie rzeczywistym, wykrywać potencjalne zagrożenia i podejmować działania zaradcze?

Najlepszym sposobem na ocenę zgodności poddostawcy z określonymi wymogami jest przeprowadzanie regularnych audytów na miejscu, co rok lub co dwa lata. Audyty powinny obejmować szereg ważnych aspektów, takich jak zgodność procesów z wymogami, kontrola jakości i identyfikowalność. W ich skład powinny także wchodzić przeglądy fizycznego ruchu produktów i komponentów w zakładzie, gospodarki magazynowej oraz urządzeń produkcyjnych.

Skutecznym sposobem na konfrontację wyników z oczekiwaniami są kwartalne przeglądy biznesowe. W przypadku strategicznych poddostawców takie przeglądy powinny być wykonywane na szczeblu najwyższego kierownictwa.

Bezpieczeństwo fizyczne

Każdy ośrodek uczestniczący w łańcuchu dostaw — od dostawcy komponentów po centrum dystrybucji — musi spełniać wysokie standardy bezpieczeństwa. Przykładowo musi być zapewniona stała ochrona wejść i wyjść oraz rejestrowanie i przechowywanie danych dotyczących kontroli dostępu i rejestracji gości. Ponadto powinny być stosowane skanery umożliwiające detekcję niepożądanych obiektów i materiałów. Za transport powinni odpowiadać wyłącznie sprawdzeni i znani spedytorzy, którzy przestrzegają rygorystycznych przepisów i stosują właściwe środki kontroli bezpieczeństwa. Zalecane jest także częste dozorowanie oraz dokumentowanie przywożonych i wywożonych towarów przy użyciu kamer.

Sieci „zero trust”

Podatność sieci na zagrożenia rośnie. Na skutek dynamicznego wzrostu liczby połączonych urządzeń w sieci powstają punkty końcowe narażone na ataki. Cyberataki są nie tylko coraz liczniejsze, ale też coraz bardziej wyrafinowane. Dlatego powstała koncepcja „zero trust” (zerowego zaufania).

Nie ufaj nikomu i niczemu w sieci

Koncepcja sieci „zero trust” zakłada, że nie można ufać żadnemu podmiotowi — człowiekowi ani maszynie — łączącemu się spoza sieci i w jej obrębie. Nie ma znaczenia, gdzie znajduje się ten podmiot i jak nawiązuje połączenie. Sieciom „zero trust” przyświeca zasada „nigdy nie ufaj, zawsze sprawdzaj”.

Koncepcja sieci „zero trust” zakłada, że nie można ufać żadnemu podmiotowi łączącemu się spoza sieci i w jej obrębie.

Przyznawaj minimalne uprawnienia dostępu

W tej sytuacji tożsamość każdego podmiotu uzyskującego dostęp do sieci lub poruszającego się po niej musi być wielokrotnie weryfikowana na różne sposoby, zależnie od zachowania podmiotu i wrażliwości konkretnych danych, do których uzyskuje on dostęp. Zasadniczo podmiotom przyznaje się minimalny poziom dostępu pozwalający wykonać powierzone im zadanie.

Sieci i architektury „zero trust”

W miarę poszerzania swojej wiedzy na temat konieczności wzmacniania cyberzabezpieczeń klienci wdrażają sieci i architektury „zero trust”, w tym protokół HTTPS i bardziej zaawansowany standard IEEE 802.1X, które umożliwiają automatyczne wpuszczanie uwierzytelnionych urządzeń do sieci lub blokowanie urządzeń nieuwierzytelnionych. Dlatego producenci urządzeń sieciowych muszą spełniać odpowiednie wymogi, stosując technologie lub interfejsy obsługujące takie sieci.

Czas na aparat zasad...

Każda sieć typu „zero trust" bazuje na aparacie zasad — oprogramowaniu, które pozwala organizacji tworzyć, monitorować i egzekwować zasady dostępu do danych i zasobów sieciowych. Aparaty zasad łączą analizy sieciowe z programowanymi regułami, skutkiem czego proces przyznawania dostępu na podstawie ról jest uwarunkowany kilkoma czynnikami.

„Tak" lub „nie" na każde żądanie

W uproszczeniu wygląda to tak, że aparat zasad porównuje każde żądanie dostępu sieciowego z obowiązującą zasadą, a następnie informuje użytkownika, czy żądanie zostanie spełnione czy nie. W sieciach typu „zero trust" aparat zasad definiuje i egzekwuje zasady bezpieczeństwa danych i uzyskiwania do nich dostępu, które odnoszą się do modeli i lokalizacji hostingu oraz użytkowników i urządzeń.

Ustalanie i stosowanie reguł

Aby aparat zasad funkcjonował prawidłowo, organizacja musi starannie zdefiniować reguły i zasady mające obowiązywać w kluczowych elementach zabezpieczających, takich jak zapory nowej generacji, bramki poczty e-mail i chmury oraz oprogramowanie zapobiegające utracie danych. Wszystkie te rozwiązania współpracują ze sobą, egzekwując mikrosegmentację sieci poza modelami i lokalizacjami hostingu.

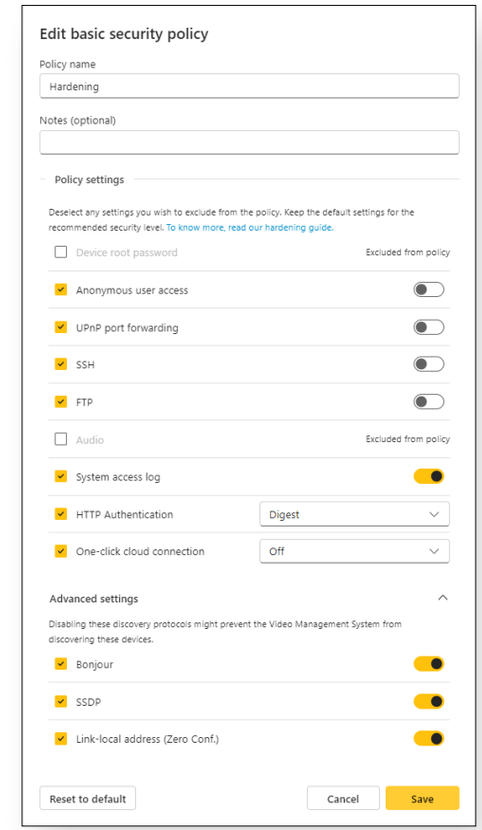
Jak można uzyskiwać dostęp do danych i zasobów sieciowych?

Aparaty zasad umożliwiają:

> Tworzenie reguł
> Monitorowanie reguł
> Egzekwowanie reguł

Aparaty zasad dziś i w przyszłości

Obecnie zasady trzeba zwykle wprowadzać osobno w konsoli zarządzania każdego rozwiązania, jednak coraz lepiej zintegrowane konsole mogą automatycznie definiować i aktualizować zasady w różnych produktach. Zarządzanie tożsamością i dostępem, uwierzytelnianie wieloczynnikowe, powiadomienia push, uprawnienia do plików, szyfrowanie i orkiestracja zabezpieczeń — wszystkie te rozwiązania odgrywają określoną rolę w projektowaniu architektur sieci typu „zero trust".



Konfigurowanie aparatu zasad.

Dlaczego skuteczne zarządzanie cyklem istnienia ma kluczowe znaczenie

Dotrzymywanie kroku zagrożeniom
Skuteczne zarządzanie cyklem istnienia może pomóc organizacjom w zabezpieczaniu działalności i lepszym przygotowywaniu się na przyszłe wyzwania. Trzeba wiedzieć, gdzie występuje zagrożenie i stale monitorować podatne na nie obszary. Jest to szczególnie ważne w przypadku systemów bezpieczeństwa, ponieważ ewentualna usterka kamery do dozoru sieciowego grozi poważnymi konsekwencjami.

Urządzenia sieciowe trzeba aktualizować
Wszystkie urządzenia sieciowe — od kamer po system zarządzania materiałem wizyjnym — wymagają aktualizacji i poprawek, aby uniemożliwić przestępcom wykorzystywanie znanych luk i omijanie istniejących mechanizmów ochrony.

Producenci regularnie wydają aktualizacje i poprawki zabezpieczeń oprogramowania urządzeń, które eliminują luki, naprawiają błędy oraz rozwiązują inne problemy z wydajnością i w ten sposób przyczyniają się do stabilności i bezpieczeństwa systemu. Jednak organizacje często nie aktualizują oprogramowania sprzętowego czy systemu operacyjnego, z których korzystają urządzenia.

Zwykle wynika to z braku całościowego obrazu wszystkich urządzeń działających w ich sieci. A nawet jeśli taki całościowy obraz istnieje, aktualizowanie wszystkich urządzeń bywa uciążliwe i czasochłonne.

Zaniedbywanie aktualizacji oprogramowania urządzeń może zwiększyć ich podatność na cyberataki i narazić firmę na nieprzyjemne konsekwencje, od przerw w działalności po wysokie kary pieniężne z tytułu nieprzestrzegania przepisów nałożone przez organy regulacyjne.

Zgodnie z popularnym powiedzeniem sieć jest tylko tak bezpieczna jak podłączone do niej urządzenia, dlatego ważne jest skuteczne zarządzanie cyklem istnienia sieciowych zasobów fizycznych.

Jedno urządzenie — dwa istnienia
Urządzenia z oprogramowaniem mają dwa cykle istnienia:

1) Okres zdatności funkcjonalnej — jak długo urządzenie może faktycznie działać i pełnić swoją funkcję. Przykładowo czas zdatności funkcjonalnej kamery sieciowej wynosi około 10–15 lat.

2) Ekonomiczny cykl istnienia — ile czasu upłynie, zanim utrzymanie urządzenia zacznie kosztować więcej niż wdrożenie nowego rozwiązania. Chociaż kamera IP może działać nawet 15 lat, jej rzeczywisty czas eksploatacji będzie krótszy z powodu dynamicznego rozwoju rynku cyberzabezpieczeń.

Proaktywnie zarządzaj zasobami
Zarządzanie cyklem istnienia polega na skutecznym kontrolowaniu zarówno czasu zdatności funkcjonalnej, jak i ekonomicznego cyklu istnienia zasobów fizycznych. Organizacje potrzebują wglądu we wszystkie urządzenia wdrożone w sieci, aby skutecznie zabezpieczyć się przed zagrożeniami.

Podejście Axis do cyberbezpieczeństwa

Axis dąży do zapewnienia wysokiego poziomu cyberbezpieczeństwa. Stale pracujemy nad doskonaleniem oferowanych produktów i rozwiązań oraz procesów związanych z cyberbezpieczeństwem. Zależy nam na transparentnym przekazywaniu informacji na temat tego, jak zabezpieczamy swoją działalność i łańcuch dostaw, jak tworzymy oprogramowanie z myślą o obniżeniu ryzyka wystąpienia luk, jak reagujemy na nowo wykryte luki oraz jak wprowadzamy zabezpieczenia do naszych produktów i wspieramy cyberbezpieczeństwo w całym cyklu ich istnienia.

Na kolejnych stronach opisano, jakie działania i środki stanowią nasz fundament bezpieczeństwa, a także co robimy i zapewniamy na różnych etapach cyklu istnienia produktu — od produkcji przez wdrożenie i eksploatację po wycofanie z eksploatacji — aby ograniczać ryzyko i pomagać klientom w zabezpieczaniu produktów Axis.

Fundament bezpieczeństwa

Uporządkowane i systemowe podejście do bezpieczeństwa wewnętrznego

W Axis promujemy współpracę w obszarze bezpieczeństwa, dzięki czemu wszyscy pracownicy stymulują ciągłe udoskonalenia w obszarze naszego bezpieczeństwa wewnętrznego. Fundament naszej platformy cyberbezpieczeństwa stanowi certyfikowany system zarządzania bezpieczeństwem informacji zgodny ze standardem ISO 27001. W ramach tego systemu wdrożyliśmy mechanizmy kontroli cyberbezpieczeństwa, które zapewniają stosowanie najlepszych praktyk w zakresie zarządzania infrastrukturą IT i platformą rozwojową na potrzeby oprogramowania oraz połączonych urządzeń.

Nasze uporządkowane i systemowe podejście umożliwia ochronę poufności, integralności i dostępności naszych zasobów. Ponadto Axis przestrzega różnych wymogów prawnych oraz strategicznie wybranych ram i standardów, w tym standardu cyberbezpieczeństwa ETSI EN 303 645 w odniesieniu do urządzeń z systemem AXIS OS. Jednak nie polegamy wyłącznie na przepisach i certyfikacjach, ponieważ duża liczba certyfikacji nie musi się przekładać na lepsze cyberbezpieczeństwo.

RI. SE

CERTIFIKAT

ISO/IEC 27001

Härmed intygas att/This is to certify that

Axis Communications AB

Gränden 1, 223 69 LUND, SWEDEN

har ett ledningssystem för informationssäkerhet som uppfyller kraven enligt ISO/IEC 27001:2022 vad gäller
has an information security management system that fulfils the requirements of ISO/IEC 27001:2022 with respect to

Product management, utveckling och drift inom IT-infrastrukturtjänster och Axis Connected Services
Allt i enlighet med uttalande om tillämplighet fastställt 2023-11-14

Product management, development and operations within IT infrastructure services and Axis Connected Services
All in accordance with Statement of Applicability established 2023-11-14

Ursprungligen utfärdat/Originally issued	2019-02-27
Giltigt till och med/Expiry date	2025-02-26
Beslutsdatum/Decision date	2023-12-07

Jonas Madsen

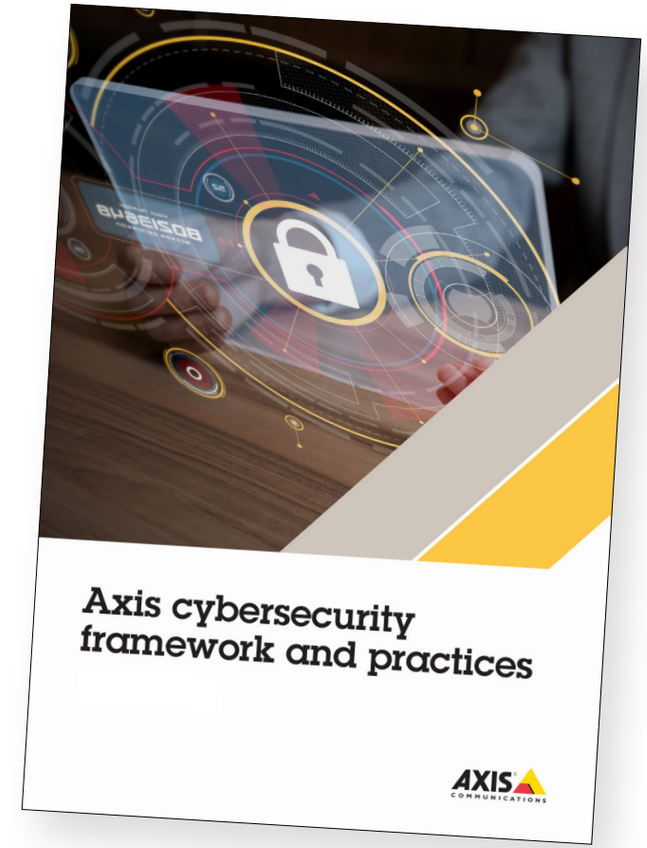
RISE Research Institutes of Sweden AB | Certification
Box 857, SE-501 15 Borås, Sweden
+46 10-516 50 00
certifiering@ri.se | www.ri.se

SP

Certifikat/Certificate 6134 | | version/issue 5 | 2023-12-07

This document is the property of RISE and may not be reproduced other than in full, except with the prior written approval by RISE.

Sida/Page: 1(1)



Dowiedz się więcej o zgodności Axis z przepisami

Ochrona integralności produktów i ograniczanie ryzyka luk w oprogramowaniu

Przechodząc od bezpieczeństwa wewnętrznego do bezpieczeństwa produktów, przedstawiamy elementy tworzące fundament zabezpieczeń sprzętu i oprogramowania Axis, które odzwierciedlają naszą naczelną zasadę transparentności.

Platforma cyberbezpieczeństwa Axis Edge Vault

Ta platforma sprzętowa wbudowana w urządzenia Axis obejmuje funkcje chroniące ich integralność, dzięki czemu umożliwia ich bezpieczny rozruch, integrację oraz ochronę wrażliwych danych, takich jak klucze kryptograficzne, przed nieautoryzowanym dostępem.

Więcej informacji o Axis Edge Vault

Axis Security Development Model (ASDM)

ASDM to model rozwoju zabezpieczeń, czyli metodologia stosowana przez Axis w celu obniżenia ryzyka wydania produktów z lukami w zabezpieczeniach oprogramowania. Model ten sprawia, że kwestie bezpieczeństwa są integralnym elementem prac nad oprogramowaniem, oraz obejmuje między innymi ocenę ryzyka, modelowanie zagrożeń, analizę kodu, testy penetracyjne, program nagród za wykryte błędy oraz skanowanie luk i zarządzanie nimi. Dzięki szybkiemu wykrywaniu i rozwiązywaniu problemów na każdym etapie prac rozwojowych ASDM pomaga ograniczyć zagrożenia bezpieczeństwa u naszych klientów.

Więcej informacji o ASDM

AXIS OS

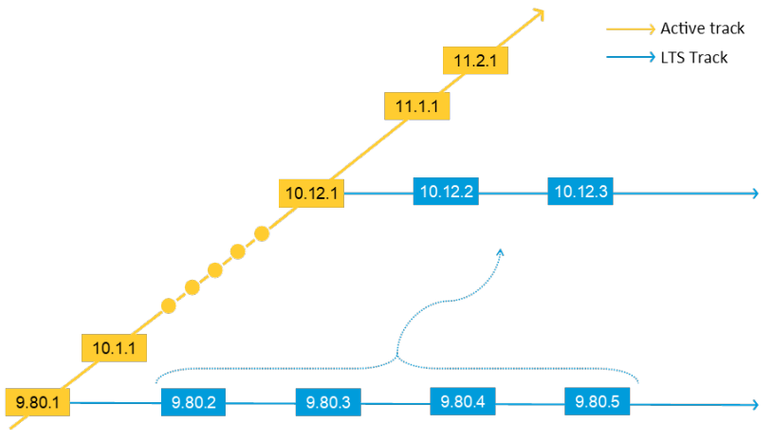
AXIS OS to nasz oparty na Linuxie system operacyjny dla urządzeń brzegowych. Ten wydajny system zbudowany na fundamencie otwartości, transparentności i cyberbezpieczeństwa udostępnia różne ścieżki wsparcia dla urządzeń Axis, dzięki czemu Axis może szybko wydawać funkcje i poprawki zabezpieczeń oprogramowania przeznaczone dla większej liczby produktów. AXIS OS został tak zaprojektowany, aby ułatwiać ograniczanie ryzyka oraz aktualizowanie i ochronę urządzeń i usług Axis. Na stronie internetowej Axis dla wielu produktów podane są daty zakończenia wsparcia technicznego, dzięki czemu klient może z wyprzedzeniem zaplanować wycofanie posiadanych produktów z eksploatacji i ich wymianę.

Więcej informacji o AXIS OS

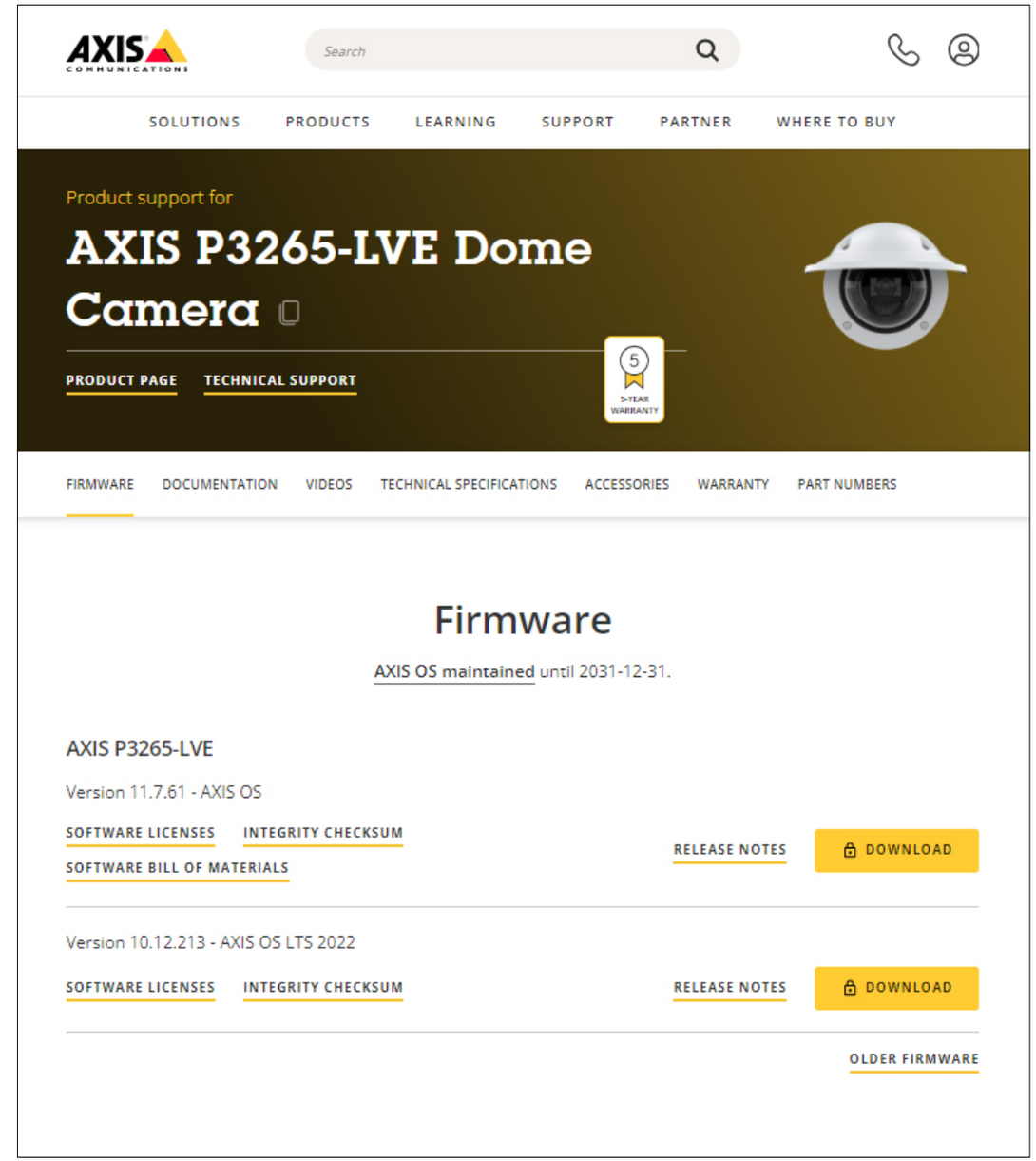
Programowy wykaz materiałów

Ponadto publikujemy programowy wykaz materiałów dotyczący systemu AXIS OS, kładąc szczególny nacisk na cyberbezpieczeństwo i transparentność z perspektywy klientów, badaczy zabezpieczeń i władz. Programowy wykaz materiałów to obszerna, szczegółowa lista komponentów użytych w systemie operacyjnym urządzeń Axis. Umożliwia on poznanie najlepszych praktyk z obszaru cyberbezpieczeństwa stosowanych przez dostawców oraz zawiera cenne informacje dla podmiotów zewnętrznych specjalizujących się w ocenie luk, analizie zagrożeń i planowaniu działań zaradczych.

Więcej informacji o programowym wykazie materiałów



Ścieżki systemu AXIS OS.



Zarządzanie nowo wykrytymi lukami

Jako członek organu Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA) Axis publikuje informacje o wykrytych lukach i powiadamia o nich zainteresowane podmioty, umożliwiając klientom terminowe podjęcie odpowiednich działań. Współpracując z badaczami zewnętrznymi, Axis ujawnia luki oraz słabe punkty w ramach transparentnego, odpowiedzialnego i skoordynowanego procesu. Udostępniamy poprawki przeznaczone dla dotkniętych urządzeń, aplikacji i usług oraz publikujemy wszystkie niezbędne informacje na **swojej stronie internetowej** i w ogólnodostępnej bazie luk programu CVE. Ponadto udostępniamy usługę powiadomień dotyczących bezpieczeństwa, w której można się zarejestrować, aby otrzymywać informacje na temat luk i innych kwestii związanych z bezpieczeństwem. Axis podkreśla, jak ważne jest aktualizowanie systemu operacyjnego zainstalowanych produktów, dzięki któremu wdrażane są najnowsze poprawki zabezpieczeń.

Więcej informacji o zasadach zarządzania lukami przez Axis

Program nagród za wykryte błędy

W ramach strategii transparentnego zarządzania lukami w zabezpieczeniach wprowadziliśmy program nagród za wykryte błędy. Jest on prowadzony we współpracy z serwisem Bugcrowd, liderem cyberzabezpieczeń w modelu crowdsourcingu. Dążymy do rozwijania profesjonalnej współpracy z zewnętrznymi badaczami zabezpieczeń i etycznymi hakerami. W ramach programu badaczom, którzy wykryją luki w produktach z systemem AXIS OS, przysługuje nagroda w formie gotówkowej. Następnie zgodnie z zasadą transparentności Axis upublicznia te i inne wykryte luki oraz udostępnia poprawki do dotkniętych nimi produktów.


PRODUKCJA


DYSTRYBUCJA

Ograniczanie ryzyka komponentów sprzętowych i programowych z naruszonymi zabezpieczeniami

Bezpieczeństwo łańcucha dostaw

Produkty z zakresu bezpieczeństwa fizycznego, podobnie jak wszystkie inne, powinny działać w sposób bezpieczny i zgodny z przeznaczeniem. Wymaga to skutecznej ochrony produktu — a więc jego komponentów sprzętowych i systemu operacyjnego — przed nieautoryzowanymi zmianami i próbami manipulacji na każdym etapie łańcucha dostaw.

Kontrola jakości

Firma Axis, wraz ze swoimi dostawcami i partnerami produkcyjnymi, wykorzystuje szereg mechanizmów kontroli jakości utrzymujących i chroniących integralność oferowanych produktów. Komponenty są zawsze pozyskiwane od podmiotów z listy zatwierdzonych dostawców, zgodnie z wykazem materiałów wyszczególnionym przez Axis. Bez zgody udzielonej przez Axis dostawcy nie wolno wprowadzać żadnych zmian w specyfikacji, instrukcjach roboczych ani dokumentach kontroli jakości. Wszelkie zatwierdzone zmiany należy udokumentować i zarejestrować.

Identyfikowalność

Podczas obsługi materiałów zawsze sprawdzany jest ich status, co pozwala wykryć wszelkie odstępstwa mogące obniżać jakość. Dostawcy i partnerzy produkcyjni mają obowiązek prowadzenia systemu identyfikacji, który umożliwia śledzenie produkowanych partii od etapu przyjęcia materiału po dostawę gotowego komponentu. W czasie produkcji komponenty fizyczne przechodzą szereg testów, które sprawdzają ich zgodność z wymogami i ujawniają ewentualne odstępstwa.

Wykrywanie podrabianych komponentów

Automatyczna inspekcja optyczna pomaga sprawdzać, czy nie zostały zamontowane żadne nieoryginalne komponenty. Axis samodzielnie projektuje i wytwarza kluczowe urządzenia produkcyjne, a także system testowania komponentów, modułów i produktów na różnych etapach produkcji. W ten sposób ogranicza ryzyko sabotażu. Dodatkowo wszystkie dane z testów są na bieżąco przekazywane do Axis, co pozwala natychmiast wykrywać niedozwolone modyfikacje.

Więcej informacji o bezpieczeństwie łańcucha dostaw w Axis

Przeciwdziałanie zagrożeniom podczas dystrybucji

Wbudowane cyberzabezpieczenia urządzeń Axis w połączeniu z procedurą wczytywania fabrycznych ustawień domyślnych zapewniają ochronę przed nieautoryzowanymi modyfikacjami oprogramowania podczas transportu. Funkcje udostępniane przez platformę Axis Edge Vault (opisaną na następnej stronie) zabezpieczają wrażliwe informacje znajdujące się w urządzeniach i dają pewność, że urządzenia korzystają wyłącznie z oryginalnego systemu operacyjnego Axis.

Wiedza na temat bezpieczeństwa łańcucha dostaw jest niezbędna, jeśli organizacja przeprowadza ocenę ryzyka mającą ustalić, czy dany dostawca wprowadził mechanizmy ograniczające zagrożenia dla organizacji.

Wbudowane cyberzabezpieczenia

Urządzenia Axis są wyposażone we wbudowane zabezpieczenia, które umożliwiają ich bezpieczny rozruch i dodanie do systemu oraz zapewniają ochronę wrażliwych informacji.

Platforma cyberbezpieczeństwa Axis Edge Vault

Nasza sprzętowa platforma cyberbezpieczeństwa to solidny fundament, dzięki któremu można mieć pewność, że dane urządzenie Axis będzie zaufanym i niezawodnym elementem sieci. Axis Edge Vault obejmuje następujące funkcje*:

> **Bezpieczny magazyn kluczy**, który obejmuje kryptograficzne moduły obliczeniowe umożliwiające bezpieczne przechowywanie kluczy kryptograficznych. Chroni on identyfikator urządzenia i inne wrażliwe informacje przed nieautoryzowanym dostępem — nawet w przypadku naruszenia zabezpieczeń urządzenia. Kryptograficznym modułem obliczeniowym może być środowisko TEE (Trusted Execution Environment) wbudowane w procesor system-on-chip (SoC) Axis, ewentualnie bezpieczny element lub moduł TPM (Trusted Platform Module), czyli odrębny układ na płycie głównej. W urządzeniach Axis stosowany jest jeden lub dowolne połączenie tych trzech modułów.

> **Podpisane oprogramowanie sprzętowe** i **bezpieczny start**, które dają pewność, że urządzenie pobiera i uruchamia wyłącznie oryginalny system operacyjny Axis (AXIS OS).

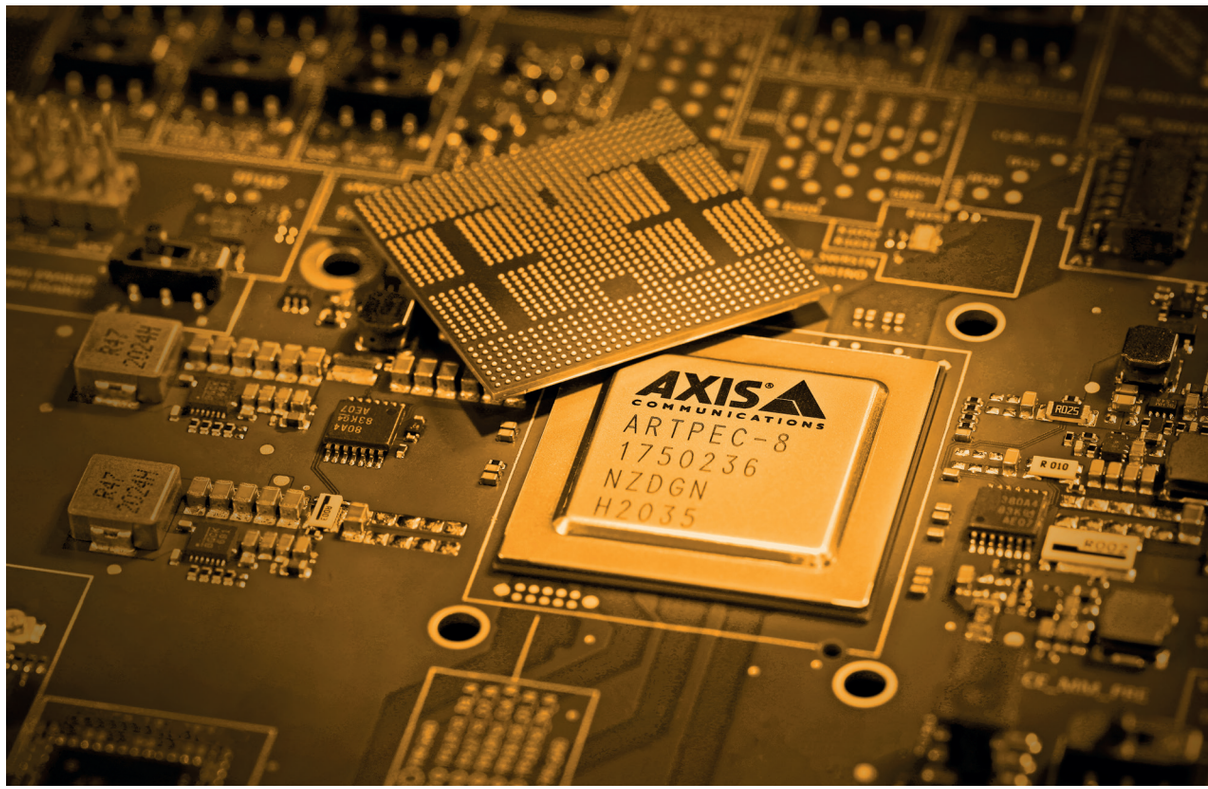
> **Identyfikator urządzenia Axis**, czyli funkcja zgodna ze standardem IEEE 802.1AR, która umożliwia bezpieczną identyfikację i dodawanie urządzeń do sieci.

> **Zaszyfrowany system plików**, który chroni dane systemu plików przed ekstrakcją i ingerencją, gdy urządzenie nie jest używane, na przykład podczas transportu od integratora systemu do klienta.

> **Podpisany materiał wizyjny**, czyli funkcja umożliwiająca weryfikację autentyczności zarejestrowanego materiału wizyjnego i daje pewność, że nie został on zmanipulowany.

**Uwaga: nie wszystkie modele urządzeń obsługują pełen zestaw funkcji platformy Axis Edge Vault. Aby sprawdzić funkcje obsługiwane przez określony produkt, należy się zapoznać z kartą jego danych technicznych lub skorzystać z selektora produktów Axis.*

Więcej informacji o Axis Edge Vault



Ustawienia domyślne

Oprócz funkcji zabezpieczających urządzenia Axis są dostarczane z fabrycznie zdefiniowanymi domyślnymi ustawieniami ochrony.

Poświadczenia i protokoły sieciowe

Urządzenie Axis nie będzie działać do czasu skonfigurowania kont obejmujących nazwę użytkownika i hasło. Po ich skonfigurowaniu dostęp do funkcji administracyjnych i/lub strumieni wideo jest możliwy tylko w przypadku użycia tych właśnie poświadczeń.

Ponadto w urządzeniach Axis domyślnie włączona jest jedynie minimalna liczba protokołów i usług sieciowych, na przykład HTTP i HTTPS na potrzeby dostępu do interfejsów urządzenia, RTSP i RTP do celów strumieniowego przesyłania materiału wizyjnego i dźwięku oraz takie protokoły jak UPnP i Bonjour, które umożliwiają wykrywanie urządzeń Axis przez aplikacje zewnętrzne.

Do sieci „zero trust" klientów

W odpowiedzi na wymagania związane z sieciami „zero trust" Axis wytwarza produkty z unikatowymi identyfikatorami urządzenia oraz obsługą protokołu HTTPS i standardu IEEE 802.1X, a także standardu IEEE 802.1AR na potrzeby uwierzytelniania urządzeń oraz IEEE 802.1AE MACsec do celów automatycznego szyfrowania danych.

Protokół HTTPS jest domyślnie włączony, umożliwiając bezpieczne konfigurowanie haseł urządzeń. Ponadto sprawia on, że oprogramowanie do zarządzania materiałem wizyjnym korzystające z HTTPS może zweryfikować certyfikat SSL podpisany przez zaufany urząd certyfikacji, który jest obsługiwany przez identyfikator urządzenia Axis w nowszych produktach.

Obsługa standardów IEEE 802.1X, IEEE 802.1AR i IEEE 802.1AE — domyślnie włączona w produktach Axis — umożliwia automatyczne dodawanie i uwierzytelnianie urządzeń oraz kompleksowe szyfrowanie. Dzięki temu specjaliści IT zyskują standardowe mechanizmy umożliwiające sprawne i bezpieczne integrowanie urządzeń Axis z siecią firmową zgodnie ze standardem IEEE 802.1X. Klienci korzystający z urządzeń Axis w sieci Aruba mogą pobrać przewodnik po integracji, w którym przedstawiono oparte na najlepszych praktykach procedury bezpiecznego dodawania urządzeń Axis i zarządzania nimi.

Więcej informacji o rozwiązaniach Axis dla korporacyjnych środowisk IT

WDROŻENIE

Cyberbezpieczeństwo podczas wdrożenia

Urządzenie Axis jest jednym z wielu sieciowych punktów końcowych — podobnie jak inne urządzenia, na przykład laptopy, komputery stacjonarne czy urządzenia mobilne. Jednak w odróżnieniu od laptopa na urządzeniu Axis użytkownik nie wejdzie na potencjalnie niebezpieczną stronę internetową, nie otworzy złośliwego załącznika do e-maila ani nie zainstaluje niezaufanej aplikacji. Nie zmienia to faktu, że sieciowy produkt umożliwiający przekazywanie materiału wizyjnego lub dźwięku albo kontrolowanie dostępu to urządzenie wyposażone w interfejs mogący narazić na niebezpieczeństwo system, do którego to urządzenie jest podłączone.

Do produktów Axis są dostępne poradniki dotyczące wzmacniania zabezpieczeń, które zawierają zalecenia pomagające ograniczyć ryzyko cyberataków. Poniżej przedstawiono kilka podstawowych zaleceń. Przykładowo zalecamy, aby przed przystąpieniem do konfiguracji urządzenia przywrócić w nim fabryczne ustawienia domyślne, co da pewność, że urządzenie jest wolne od niechcianego oprogramowania ani konfiguracji. Trzeba też sprawdzić, czy urządzenie korzysta z najnowszego systemu AXIS OS, który może zawierać najnowsze aktualizacje zabezpieczeń i poprawki błędów przeznaczone dla tego właśnie urządzenia.

Zalecamy ustawienie silnych haseł, ograniczenie bezpośredniego dostępu do interfejsu WWW urządzenia, skonfigurowanie urządzenia do korzystania wyłącznie z protokołu HTTPS (który szyfruje dane przesyłane między klientem i urządzeniem) oraz wyłączenie nieużywanych usług i funkcji w celu ograniczenia zbędnego ryzyka. Ważne jest także ustawienie w urządzeniu poprawnej daty i godziny, ponieważ umożliwia ono tworzenie dokładnych dzienników systemowych oraz zapewnia prawidłową weryfikację certyfikatów cyfrowych, z których korzystają takie funkcje jak HTTPS i IEEE 802.1X.

Narzędziem Axis umożliwiającym sprawne konfigurowanie urządzeń Axis i zarządzanie nimi na poziomie lokalnym jest AXIS Device Manager. Umożliwia ono zbiorcze wykonywanie zadań z zakresu instalacji i ochrony bezpieczeństwa, takich jak zarządzanie poświadczeniami urządzeń, wdrażanie certyfikatów cyfrowych, wyłączanie nieużywanych usług i uaktualnianie systemu AXIS OS. Więcej informacji na temat oprogramowania do zarządzania urządzeniami znajduje się na następnej stronie.

Aby uzyskać pełne, szczegółowe zalecenia z zakresu wzmacniania zabezpieczeń urządzeń z systemem AXIS OS, skorzystaj z Przewodnika po zabezpieczeniach systemu AXIS OS. Aby znaleźć przewodniki po zabezpieczeniach oprogramowania Axis do zarządzania materiałem wizyjnym i przełączników sieciowych, odwiedź stronę zasobów związanych z cyberbezpieczeństwem. Natomiast w celu uzyskania informacji o tym, jak urządzenia Axis można płynnie integrować z infrastrukturą i sieciami IT w dużych przedsiębiorstwach, zobacz rozwiązania Axis dla korporacyjnych środowisk IT.

Axis udostępnia narzędzia, dokumentację i szkolenia, które ułatwiają ograniczanie ryzyka oraz aktualizowanie i ochronę stosowanych produktów i usług Axis. **Zapoznaj się z naszymi zasobami dotyczącymi cyberbezpieczeństwa.**

EKSPLOATACJA

Cyberbezpieczeństwo urządzeń podczas eksploatacji

Podczas eksploatacji urządzenia jednym z najważniejszych sposobów dbania o jego cyberbezpieczeństwo jest regularne aktualizowanie jego oprogramowania sprzętowego lub systemu operacyjnego AXIS OS. Daje to pewność, że urządzenie korzysta z najnowszych aktualizacji zabezpieczeń i poprawek błędów. Takie funkcje urządzeń Axis jak podpisane oprogramowanie sprzętowe i bezpieczny start dają gwarancję, że można w nich zainstalować i uruchomić wyłącznie oryginalny system AXIS OS. Wersje systemu AXIS OS, udostępniane bezpłatnie, są objęte ścieżką aktywną lub ścieżką wsparcia długoterminowego. Wersje AXIS OS na ścieżce aktywnej obsługują nowe funkcje, natomiast wersje objęte ścieżką wsparcia długoterminowego ich nie obsługują, co minimalizuje ryzyko wystąpienia problemów ze zgodnością. Jednak obie ścieżki obejmują aktualizacje zabezpieczeń i poprawki błędów. Dobrym sposobem na monitorowanie nowo wykrytych luk w zabezpieczeniach jest zarejestrowanie się w usłudze powiadamiania o zabezpieczeniach Axis. Opublikowanym lukom towarzyszą instrukcje wyjaśniające, jak należy je usunąć w dotkniętych urządzeniach przy użyciu nowego oprogramowania.

Aby ułatwić i usprawnić aktualizowanie sytemu operacyjnego w dużej liczbie urządzeń, Axis oferuje oprogramowanie do zarządzania urządzeniami, w tym AXIS Device Manager i AXIS Device Manager Extend.

Jak działa oprogramowanie do zarządzania urządzeniami?

Oprogramowanie do zarządzania urządzeniami pozwala szybko i w czasie rzeczywistym zbierać dane o wszystkich kamerach, enkoderach, rozwiązaniach do kontroli dostępu, urządzeniach audio i innych sprzętach połączonych z siecią. Oprogramowanie skanuje całą sieć, a gdy wykryje nowe lub zaktualizowane urządzenie, rejestruje najważniejsze informacje na jego temat, takie jak numer modelu, adresy IP i MAC, wersję oprogramowania i status certyfikatu.

Pełny obraz

Szczegółowe informacje o całym ekosystemie sieciowym ułatwiają wdrażanie spójnych zasad i procedur zarządzania cyklem istnienia wszystkich urządzeń oraz pomagają w bezpiecznym nadzorowaniu wszystkich istotnych zadań związanych z instalacją, wdrażaniem, konfigurowaniem, zabezpieczaniem i konserwacją.

Zasady i najlepsze praktyki cyberbezpieczeństwa z zakresu zarządzania urządzeniami muszą odpowiadać na pytania dotyczące takich kwestii jak siła haseł i wymagana częstotliwość ich zmiany; które nie używane urządzenia należy wyłączać, aby ograniczyć obszar potencjalnych ataków; jak często urządzenia należy skanować na obecność luk w zabezpieczeniach oraz jakie procedury wdrożono z myślą o ocenie stopnia ryzyka w przypadku, gdy producent opublikuje informacje o wykrytych atakach wykorzystujących luki.

Oszczędność czasu i energii

Oprogramowanie do zarządzania urządzeniami pomaga organizacjom zaoszczędzić czas i energię w obszarze przeciwdziałania zagrożeniom cyberbezpieczeństwa.

Dzięki niemu można:

- Dostarczać zmiany systemowe, aktualizacje oprogramowania urządzeń i nowe certyfikaty cyfrowe do wszystkich właściwych urządzeń jednocześnie.
- Łatwo tworzyć i modyfikować ustawienia zabezpieczeń oraz stosować je w obrębie całej sieci, tak by wszystkie urządzenia były zgodne z najnowszymi zasadami i procedurami z zakresu bezpieczeństwa.
- Sprawdzać, czy wszystkie urządzenia korzystają z najnowszej i najbezpieczniejszej wersji oprogramowania.
- Zarządzać poziomem uprawnień użytkowników w sieci i konfigurować ich modyfikacje.

Wgląd w czasie rzeczywistym

Dzięki narzędziom do zarządzania urządzeniami organizacja zyskuje bieżący wgląd w stan ekosystemu. Przykładowo użytkownik widzi, które urządzenia trzeba zaktualizować za pomocą najnowszych aktualizacji oprogramowania i certyfikatów, oraz otrzymuje informacje o wycofywanych produktach i zakończeniu wsparcia technicznego, co ułatwia planowanie terminów wymiany urządzeń.

Narzędzia Axis do zarządzania urządzeniami

Nasze oprogramowanie do zarządzania urządzeniami, czyli narzędzia AXIS Device Manager i AXIS Device Manager Extend, pomaga w wydajnym zarządzaniu urządzeniami Axis. AXIS Device Manager i AXIS Device Manager Extend wzajemnie się uzupełniają.

AXIS Device Manager

AXIS Device Manager pomaga w szybkim i łatwym instalowaniu i konfigurowaniu nowych urządzeń. Jest to narzędzie lokalne, które pozwala wykonywać wszystkie istotne zadania z zakresu instalacji, bezpieczeństwa i eksploatacji, w tym instalować uaktualnienia oprogramowania i aplikacje. Umożliwia ono konfigurowanie ustawień kopii zapasowej i przywracania urządzeń Axis oraz sprawdzanie stanu gwarancji. Użytkownik może także stosować mechanizmy kontroli cyberbezpieczeństwa, na przykład certyfikaty HTTPS i IEEE 802.1X.

Więcej informacji o narzędziu AXIS Device Manager

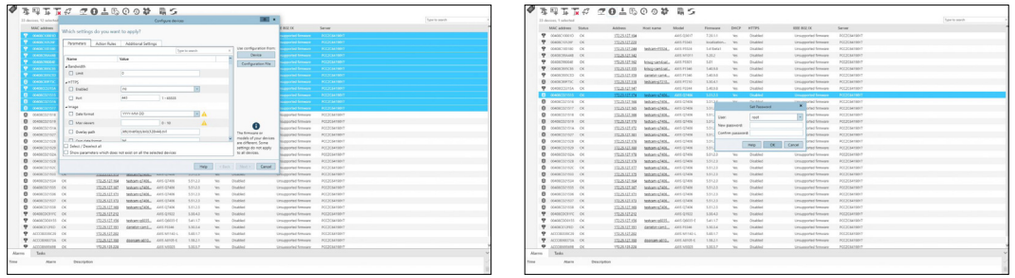
AXIS Device Manager Extend

AXIS Device Manager Extend to idealne narzędzie do sieci obejmujących wiele lokalizacji, które pomaga w zarządzaniu wszystkimi tworzącymi je zasobami. Za pomocą tej łatwej w obsłudze aplikacji można na dużą skalę wykonywać ważne zadania konserwacyjne, takie jak uaktualnianie systemu AXIS OS, definiowanie, stosowanie i egzekwowanie zasad bezpieczeństwa oraz zarządzanie aplikacjami. Aktualizowany na żywo pulpit przyspiesza rozwiązywanie problemów dzięki bieżącemu sygnalizowaniu możliwych „punktów zapalnych" w systemie, takich jak urządzenia znajdujące się w trybie offline lub nieobjęte gwarancją. Ponadto narzędzie przedstawia zalecane ustawienia urządzeń, które sprzyjają minimalizacji zagrożeń bezpieczeństwa i neutralizacji luk w zabezpieczeniach. Użytkownik może definiować, stosować i egzekwować zasady bezpieczeństwa we wszystkich urządzeniach Axis jednocześnie.

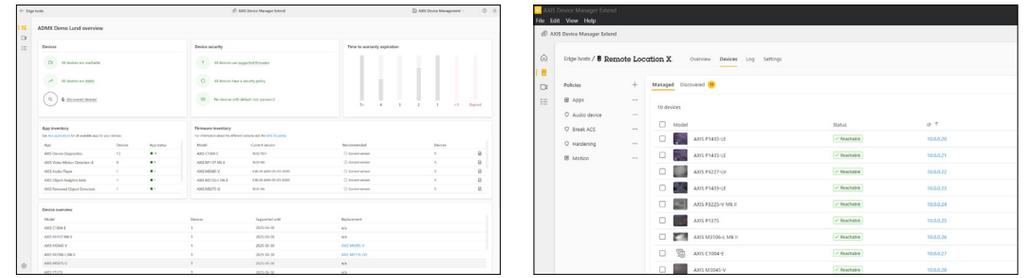
Więcej informacji o narzędziu AXIS Device Manager Extend

W razie naruszenia zabezpieczeń

Jeśli dojdzie do naruszenia zabezpieczeń sieci, Axis udostępnia Przewodnik po pracach wyjaśniających w systemie AXIS OS, który pomaga w przeprowadzeniu analiz dotyczących urządzeń sieciowych Axis.



Interfejs narzędzia AXIS Device Manager.



Interfejs narzędzia AXIS Device Manager Extend.

WYCOFANIE Z EKSPLOATACJI

Planowanie wycofania z eksploatacji

Aktualizacje i poprawki to najlepszy sposób na dbanie o cyberbezpieczeństwo produktu, ale w przypadku bardzo starych urządzeń często są niedostępne. Z perspektywy cyberbezpieczeństwa starsze, nieaktualizowane produkty stanowią duże zagrożenie. Każde przeoczone urządzenie może łatwo stać się miejscem, przez które hakerzy przenikną do systemu.

To ważne, aby planować terminy wycofania produktów z eksploatacji, ponieważ pozwala to uniknąć ryzyka posiadania urządzeń nieobjętych wsparciem technicznym, które mogą zawierać nieusunięte luki. Axis sygnalizuje datę zakończenia wsparcia systemu operacyjnego danego urządzenia, dzięki czemu można zawczasu zaplanować jego wycofanie z eksploatacji i wymianę. Ponadto w narzędziu AXIS Device Manager Extend informacje o gwarancji, wycofaniu i zakończeniu wsparcia można wyświetlić dla wszystkich urządzeń w systemie.

Kolejną ważną kwestią jest usunięcie danych z urządzenia wycofywanego z eksploatacji. Przywracając domyślne ustawienia fabryczne, można szybko skasować z urządzenia wszystkie ustawienia konfiguracyjne i dane. Szczegółowe informacje na temat wycofywania produktów z eksploatacji można znaleźć w portalu AXIS OS.

Zgodność z przepisami

Zapewnianie cyberbezpieczeństwa wymaga nieustannej czujności i dbałości.

Władze wprowadzają kolejne przepisy i regulacje związane z cyberbezpieczeństwem, których muszą przestrzegać firmy działające na danym obszarze. Również organizacje branżowe i innego rodzaju coraz częściej wymuszają zgodność z określonymi standardami, w tym certyfikację produktów i usług. Obowiązek zapewnienia zgodności z przepisami i regulacjami oraz wdrożenia wytycznych i specyfikacji odpowiednich dla stosowanych procesów biznesowych spoczywa na wszystkich zainteresowanych podmiotach.

Zgodność z przepisami jako punkt wyjścia

Zgodność z przepisami z zakresu cyberbezpieczeństwa oznacza przestrzeganie standardów i wymogów prawnych określonych przez władze. Jednak, choć nie sposób podważyć znaczenia standardów i certyfikacji, są one tylko pewnym elementem. Zawsze istnieje ryzyko, że zapewnianie zgodności ze standardami i certyfikatami stanie się swoistą zabawą w „odhaczanie pól".

Zgodność z przepisami dotyczącymi cyberbezpieczeństwa to obszar podlegający ciągłej ewolucji i to, co kiedyś było miłym dodatkiem, szybko staje się wymogiem.

Dlatego standardy i certyfikacje należy traktować jako punkt wyjścia, czyli pewien minimalny zestaw wymogów, a nie stan docelowy. Prawdziwym celem jest sytuacja, gdy dostawcy dostarczają produkty i usługi, z których można korzystać w możliwie najbezpieczniejszy sposób, a także zapewniają klientom wskazówki i przejrzyste informacje, które ułatwiają ciągłe dbanie o cyberbezpieczeństwo.

Regulacje

Regulacje związane z cyberbezpieczeństwem mają na celu skłonienie organizacji do ochrony systemów i informacji oraz zapewnienie pewnego minimalnego poziomu bezpieczeństwa dostarczanych przez nie produktów i usług. Poniżej omawiamy kilka ważnych zbiorów regulacji i sposób ich stosowania. W 2023 r. weszła w życie dyrektywa NIS2 i państwa członkowskie Unii Europejskiej muszą do października 2024 r. wprowadzić jej zapisy do prawa krajowego. Zgodnie z dyrektywą wszystkie unijne firmy działające w istotnych sektorach muszą wdrożyć wysoki wspólny poziom cyberbezpieczeństwa. Przewidziano kary za zaniedbania w obszarze cyberbezpieczeństwa, nawet jeśli wynikają one z niedociągnięć któregoś z dostawców.

W tej sytuacji ocena dostawców i bezpieczeństwo łańcucha dostaw dodatkowo zyskają na znaczeniu. Dyrektywa pośrednio nałoży obowiązki na producentów, importerów i dystrybutorów, którzy będą musieli dochować należytej staranności w całym cyklu istnienia swoich produktów.

W grudniu 2023 r. Unia osiągnęła wstępne porozumienie w sprawie nowej regulacji pod nazwą Akt dotyczący cyberodporności, która definiuje wspólne standardy cyberbezpieczeństwa produktów sprzętowych i programowych z elementami cyfrowymi. Grupa ta obejmuje produkty bezpośrednio lub pośrednio połączone z innym urządzeniem lub siecią, na przykład urządzenia IoT. Proponowana regulacja ma zmniejszyć liczbę incydentów związanych z cyberbezpieczeństwem, a także zwiększyć transparentność i wzmocnić ochronę danych. W Wielkiej Brytanii przyjęto podobne przepisy pod nazwą UK Product Security and Telecommunications Infrastructure, które wchodzą w życie w kwietniu 2024 r.

Organizacje prowadzące interesy z organami administracji publicznej w USA mogą być zobowiązane do przestrzegania takich standardów jak Cybersecurity Maturity Model Certification, który wymaga audytu i certyfikacji wewnętrznych procedur zarządzania cyberbezpieczeństwem.

Standardy i certyfikacje

Większość standardów i certyfikacji koncentruje się na cechach, funkcjach, środkach zaradczych i procesach zapewniających traktowanie bezpieczeństwa jako integralnego składnika. Ich uzupełnieniem mogą być testy zewnętrzne, w tym testy penetracyjne i programy nagród za znalezione luki w oprogramowaniu.

Chociaż certyfikaty produktów działają uspokajająco na klientów i organy władz, warto zauważyć, że zazwyczaj są one ważne przez około rok, po czym produkt wymaga recertyfikacji. W sytuacji, gdy wciąż są opracowywane i wprowadzane nowe technologie i funkcje, certyfikacje mogą za nimi nie nadążać.

Warto także pamiętać, że o ile standardy pomagają we wzmacnianiu cyberzabezpieczeń, nie gwarantują wyeliminowania incydentów cybernetycznych. Organizacje muszą stale analizować i weryfikować zagrożenia oraz stosowane zasady bezpieczeństwa.

Dlaczego Axis?

Stymulowanie cyberbezpieczeństwa

Dla Axis cyberbezpieczeństwo jest nieodłącznym elementem działalności. Jest podstawą naszego wewnętrznego systemu bezpieczeństwa informacji, zarządzania łańcuchem dostaw, tworzenia i rozwijania produktów i usług oraz zarządzania lukami w oprogramowaniu. Traktujemy cyberbezpieczeństwo jako stały i wspólny obowiązek, w którym zasadnicze znaczenie ma transparentność. Chcemy, aby klienci mogli korzystać z naszych rozwiązań w jak najbezpieczniejszy sposób. Dlatego nasze produkty są projektowane i wytwarzane z wbudowanymi zabezpieczeniami i ochronnymi ustawieniami domyślnymi, a klientom oferujemy poradniki pomagające w zwiększaniu zabezpieczeń. Nieustannie monitorujemy zagrożenia i szukamy sposobów na poprawę bezpieczeństwa. Jako uczestnik programu CVE Numbering Authority, reagujemy na nowo wykryte luki, publikując informacje na ich temat i udostępniając poprawki, aby umożliwić klientom szybkie podjęcie niezbędnych działań. Oferujemy uaktualnienia oprogramowania, dzięki czemu po zainstalowaniu urządzeń Axis można na bieżąco wzmacniać ich zabezpieczenia. Natomiast za sprawą takich narzędzi jak AXIS Device Manager i AXIS Device Manager Extend ułatwiamy klientom zarządzanie urządzeniami Axis i ograniczanie zagrożeń cyberbezpieczeństwa w całym cyklu ich istnienia.

Inne powody, by wybrać Axis

> **Jakość we wszystkich aspektach:**

Wszystkie nasze produkty przechodzą szeroko zakrojone testy, aby klienci mogli być o nie spokojni.

> **Innowacyjne technologie:**

Łącząc technologię z możliwościami ludzkiej wyobraźni, zwiększamy wydajność i funkcjonalność produktów. Nasze rozwiązania opierają się na standardach branżowych, dlatego są elastyczne, skalowalne i łatwe w integracji.

> **Zrównoważony rozwój na każdym poziomie:**

Axis wyróżnia się trwałym i silnym zaangażowaniem w rozwój przyjazny dla środowiska oraz korzystaniem z ekologicznych materiałów. Około 90% kamer i enkoderów Axis wprowadzonych w 2022 r. nie zawierało PCW.

> **Globalna obecność i lokalne doświadczenie:**

Axis może się pochwalić największą na świecie liczbą zainstalowanych sieciowych produktów wizyjnych oraz kadrą pracowników w ponad 50 krajach. Dzielimy się wiedzą i doświadczeniem oraz śledzimy najnowsze wydarzenia w branży.

> **Potęga partnerstwa:**

Głębokie zaangażowanie w relacje z partnerami sprawia, że Axis jest najbardziej otwartą marką kamer dostępną na rynku.

O firmie Axis Communications

Axis wspiera rozwój inteligentnego oraz bezpiecznego świata przez tworzenie rozwiązań umożliwiających poprawę bezpieczeństwa i efektywności 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 4000 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.