BIAŁA KSIĘGA

NIS 2

Czerwiec 2024

Spis treści

1 Wprowadzenie

1.1 Czym jest dyrektywa NIS 2?

NIS 2 to dyrektywa Unii Europejskiej, która powinna zostać przyjęta w prawie krajowym każdego państwa członkowskiego UE do 17 października 2024 r. Dyrektywa NIS 2 ma na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej UE, co ma przyczynić się do bezpiecznego i skutecznego funkcjonowania gospodarki i społeczeństwa w regionie. Wymaga ona od podmiotów świadczących niezbędne i ważne usługi w kluczowych sektorach społeczeństwa budowania zdolności w zakresie cyberbezpieczeństwa, zmniejszenia zagrożeń w sieci IP i systemach informatycznych, zapewniania ciągłości usług w obliczu incydentów oraz zgłaszania incydentów bezpieczeństwa odpowiednim organom. Od państw członkowskich wymaga ona z kolei przyjęcia krajowych strategii cyberbezpieczeństwa i ustanowienia organów, w tym organów ds. zarządzania kryzysowego w zakresie cyberbezpieczeństwa i zespołów reagowania na incydenty związane z bezpieczeństwem komputerowym. Określono w niej środki zarządzania ryzykiem w zakresie cyberbezpieczeństwa, a także środki egzekwowania przepisów. Konsekwencje nieprzestrzegania przepisów przez niezbędne i ważne podmioty mogą obejmować wysokie grzywny i konsekwencje prawne dla zespołów zarządzających.

Więcej informacji na stronie:
eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1713340785613

1.2 Kogo dotyczy dyrektywa NIS 2?

Dyrektywa NIS 2 dotyczy wszystkich podmiotów, które świadczą **niezbędne** lub **ważne** usługi na rzecz europejskiej gospodarki i społeczeństwa, w tym firm i dostawców.

1.2.1 Wpływ bezpośredni

Niezbędne podmioty – Energetyka, transport, bankowość i finanse, służba zdrowia, wodociągi, kanalizacja, infrastruktura cyfrowa, administracja publiczna

Ważne podmioty – Usługi pocztowe, wywóz odpadów, chemia, żywność, produkcja (np. urządzenia medyczne, elektryczne, sprzęt transportowy), dostawcy usług cyfrowych (np. rynki internetowe, wyszukiwarki, sieci społecznościowe), organizacje badawcze

Właściwe organy krajowe – Właściwe organy krajowe są wyznaczane przez państwa członkowskie UE do nadzorowania wdrażania i egzekwowania wymagań dyrektywy NIS 2 w swoich krajach.

1.2.2 Wpływ pośredni

Sprzedawcy i dostawcy – Dyrektywa NIS 2 pośrednio wpływa na sprzedawców, dostawców i usługodawców zewnętrznych, którzy świadczą niezbędne usługi lub usługi cyfrowe na rzecz ważnych podmiotów. Firmy te muszą zapewnić bezpieczeństwo swoich produktów i usług i mogą podlegać umownym wymogom w zakresie cyberbezpieczeństwa ze strony swoich klientów.

Użytkownicy niezbędnych usług i usług cyfrowych – Choć dyrektywa NIS 2 nie reguluje bezpośrednio kwestii cyberbezpieczeństwa, użytkownicy niezbędnych usług i usług cyfrowych korzystają z ulepszonych praktyk w zakresie cyberbezpieczeństwa i możliwości reagowania na incydenty wymaganych przez dyrektywę. Pośrednio zwiększa to bezpieczeństwo i niezawodność wykorzystywanych usług.

2 Wymagania dyrektywy NIS 2

2.1 Niezbędne i ważne podmioty

Środki bezpieczeństwa – Wdrożenie odpowiednich środków bezpieczeństwa w celu zarządzania ryzykiem i zapewnienia bezpieczeństwa sieci IP i systemów informatycznych. Środki te powinny opierać się na ocenie ryzyka i najlepszych praktykach.

Zgłaszanie incydentów – Zgłaszanie właściwym organom istotnych incydentów, które mogą mieć znaczący wpływ na bezpieczeństwo sieci IP i systemów informatycznych. Terminowe zgłaszanie jest niezbędne do koordynowania reakcji i zmniejszenia potencjalnych szkód.

Zarządzanie ryzykiem – Przeprowadzenie oceny ryzyka w celu zidentyfikowania potencjalnych zagrożeń i luk w zabezpieczeniach oraz podjęcie środków w celu ich ograniczenia.

Współpraca z właściwymi organami – Współpraca z właściwymi organami wyznaczonymi przez państwa członkowskie UE. Obejmuje zapewnienie niezbędnych informacji i dostępu do systemów w celu nadzoru regulatora i reagowania na incydenty.

Planowanie reakcji na incydenty – Opracowywanie i utrzymywanie planów reagowania na incydenty w celu skutecznego reagowania na incydenty związane z cyberbezpieczeństwem. Plany te powinny określać procedury wykrywania, zgłaszania i zmniejszenia skutków incydentów.

Bezpieczeństwo łańcuchów dostaw – Zabezpieczenie łańcuchów dostaw, w tym zewnętrznych sprzedawców i dostawców, w celu zapewnienia ogólnej odporności sieci IP i systemów informatycznych.

Ciągłe monitorowanie – Wdrożenie ciągłego monitorowania i kontroli sieci IP oraz systemów informatycznych w celu wykrywania i reagowania na zagrożenia i luki w zabezpieczeniach w czasie rzeczywistym.

3 Wpływ na dostawców

Dostawcy wspierają wymagania dyrektywy NIS 2, spełniając następujące wymagania:

Bezpieczeństwo w fazie projektowania – Producenci urządzeń IoT powinni włączać funkcje bezpieczeństwa do swoich urządzeń od fazy projektowania, co zapewnia, że bezpieczeństwo jest integralną częścią produktu.

Regularne aktualizacje i poprawki programowe – Producenci powinni regularnie dostarczać aktualizacje zabezpieczeń i poprawki usuwające luki w zabezpieczeniach urządzeń IoT.

Uwierzytelnienie i autoryzacja – Urządzenia IoT powinny wykorzystywać silne mechanizmy uwierzytelniania i odpowiednią kontrolę dostępu celem zapobieżenia nieautoryzowanemu dostępowi.

Szyfrowanie danych – Transmisja i magazyn danych w urządzeniu IoT powinny być szyfrowane, by chronić wrażliwe informacje przed przechwyceniem lub dostępem do nich przez osoby nieupoważnione.

Zgłaszanie incydentów – Producenci powinni zgłaszać wszelkie istotne incydenty lub naruszenia bezpieczeństwa związane z ich urządzeniami IoT odpowiednim organom i potencjalnym konsumentom lub klientom.

Kwestie powiązane z ochroną prywatności – Urządzenia IoT, które przetwarzają dane osobowe, oprócz zgodności z dyrektywą NIS 2, powinny być zgodne z przepisami dotyczącymi ochrony danych osobowych takimi jak RODO (Rozporządzenie o Ochronie Danych Osobowych).

Bezpieczeństwo łańcucha dostaw – Powinno być wymagane zapewnienie bezpieczeństwa całego łańcucha dostaw, od dostawców komponentów po klientów, by zapobiec występowaniu luk w zabezpieczeniach na każdym etapie procesu produkcyjnego.

4 Odpowiedź firmy Axis

W niniejszym rozdziale opisano sposób, w jaki Axis jako dostawca spełnia wymagania dyrektywy NIS 2:

4.1 Bezpieczeństwo w fazie projektowania

Bezpieczeństwo w fazie projektowania (Security by design) to podejście mające na celu zapewnienie, że kwestie i działania związane z bezpieczeństwem są podejmowane jako integralna część projektowania i rozwoju produktu w celu zmniejszenia ryzyka wystąpienia luk w zabezpieczeniach i zapewnienia, że domyślnie ustawione są w produktach wypróbowane konfiguracje bezpieczeństwa. Zasada „Security by design" w firmie Axis ma zastosowanie do oprogramowania oraz sprzętu i obejmuje następujące główne elementy:

- *Model rozwoju bezpieczeństwa Axis (Axis Security Development Model - ASDM)*: ASDM oznacza ramy zdefiniowanych procesów i narzędzi, które zapewniają, że kwestie bezpieczeństwa są integralną częścią tworzenia i rozwoju oprogramowania. Działania obejmują przeprowadzanie ocen ryzyka, modelowanie zagrożeń, testy penetracyjne, kontrolę podatności, zarządzanie incydentami, a także program nagród za wykryte błędy. Twórcy oprogramowania Axis stosują ASDM do zapewnienia bezpieczeństwa w rozwoju oprogramowania w celu zmniejszenia ryzyka wydania oprogramowania zawierającego luki w zabezpieczeniach.
- *Program nagród za wykryte błędy*: Axis promuje prywatny program nagród za wykryte błędy, który wspiera działania firmy w zakresie proaktywnego identyfikowania, usuwania i ujawniania luk w AXIS OS, systemie operacyjnym opartym na Linuksie, który znajduje się w większości produktów Axis. Wzmacnia to zaangażowanie Axis w budowanie zawodowych relacji z zewnętrznymi badaczami bezpieczeństwa i etycznymi hakerami.
- *Zestawienie komponentów oprogramowania (Software bill of materials - SBOM)*: Axis dostarcza SBOM dla AXIS OS, systemu operacyjnego opartego na Linuksie stosowanego w większości urządzeń Axis. Zapewnia ono badaczom bezpieczeństwa, władzom i klientom wgląd w komponenty oprogramowania, które składają się na AXIS OS. Jest to szczególnie pomocne dla osób specjalizujących się w ocenie podatności i analizie zagrożeń, i jest przejawem zaangażowania Axis w transparentność w kwestii cyberbezpieczeństwa.
- *Domyślne ustawienia zabezpieczeń systemu operacyjnego AXIS OS*: Urządzenia z najnowszymi wersjami systemu operacyjnego AXIS OS są domyślnie skonfigurowane fabrycznie z następującymi ustawieniami: brak domyślnego hasła, włączone protokoły HTTP i HTTPS, domyślnie włączone bezpieczne uruchomienie i komunikacja z protokołami IEEE 802.1X / 802.1AR / 802.1AE, wyłączone mniej bezpieczne protokoły. Więcej informacji na temat domyślnych mechanizmów ochrony zawiera *następująca strona*.
- *Axis Edge Vault*: Wbudowana w urządzenia Axis funkcja Axis Edge Vault to sprzętowa platforma bezpieczeństwa, która zawiera funkcje chroniące integralność produktów sieciowych Axis i umożliwia wykonywanie bezpiecznych operacji opartych na kluczach kryptograficznych. Zapewnia ochronę łańcucha dostaw dzięki bezpiecznemu uruchamianiu i podpisanemu systemowi operacyjnemu, zaufaną identyfikację urządzenia dzięki wbudowanemu unikalnemu identyfikatorowi urządzenia Axis w celu udokumentowania pochodzenia urządzenia, bezpieczne przechowywanie kluczy na potrzeby zabezpieczonego przed sabotażem magazynu informacji kryptograficznych oraz detekcję sabotażu obrazu za pomocą podpisanego strumienia wizyjnego.

4.2 Regularne aktualizacje i poprawki programowe

Axis udostępnia aktualizacje oprogramowania w celu wyeliminowania, między innymi, nowych luk w zabezpieczeniach sprzętu i oprogramowania. Axis zapewnia również narzędzia do zarządzania urządzeniami celem ułatwienia aktualizacji oprogramowania układowego urządzeń Axis Nowe wersje systemu operacyjnego AXIS OS dołączonych urządzeń są sygnalizowane w oprogramowaniu AXIS Companion, AXIS Camera Station i oprogramowaniu do zarządzania obrazem partnerów takich jak Milestone XProtect® i Genetec™ Security Center, a także w narzędziach do zarządzania urządzeniami Axis. Axis zapewnia ponadto usługę powiadomień bezpieczeństwa, którą może subskrybować każdy użytkownik. Szczegółowe informacje znajdują się poniżej.

- *AXIS OS*: Axis oferuje dwie główne możliwości aktualizacji oprogramowania urządzeń: ścieżkę aktywną i ścieżkę wsparcia długoterminowego (LTS). Ścieżka aktywna zapewnia dostęp do najnowszych funkcji, w tym poprawek błędów i poprawek zabezpieczeń. Oprogramowanie na ścieżkach długoterminowego wsparcia (LTS) ma maksymalną stabilność poprzez dostarczanie tylko poprawek błędów i zabezpieczeń, ponieważ koncentruje się na utrzymaniu zintegrowanego systemu firm trzecich.
- Narzędzia do zarządzania urządzeniami: *AXIS Device Manager* i *AXIS Device Manager Extend* to narzędzia, które ułatwiają aktualizowanie oprogramowania urządzeń Axis o najnowsze poprawki zabezpieczeń i poprawki błędów.

  W celu lokalnego zapewnienia wydajnej konfiguracji i zarządzania urządzeniami Axis oprogramowanie AXIS Device Manager udostępnia przetwarzanie wsadowe zadań bezpieczeństwa takich jak zarządzanie uwierzytelnieniem urządzeń, wdrażanie certyfikatów, wyłączanie nieużywanych usług i aktualizacja systemu AXIS OS.

  AXIS Device Manager Extend zapewnia zagregowany pulpit nawigacyjny, który gromadzi informacje o wszystkich urządzeniach i lokalizacjach w jednej, łatwej w użyciu aplikacji. Użytkownik będzie informowany o dostępności aktualizacji oprogramowania urządzeń i możliwe będzie wykonanie zbiorczych aktualizacji i innych zadań. Przekazane zostaną również rekomendacje dotyczące produktów zastępczych. Zadania są w pełni identyfikowalne i możliwe jest wyeksportowanie wszystkich informacji o urządzeniach systemowych w celu raportowania lub kontroli.
- *Usługa powiadamiania o zabezpieczeniach Axis*: Usługa ta, do której rejestracji zachęca Axis, zapewnia subskrybentom terminowe powiadomienia o incydentach bezpieczeństwa i lukach w zabezpieczeniach.

4.3 Uwierzytelnienie i autoryzacja

Aby zapobiec nieautoryzowanemu dostępowi i zwiększyć ogólne bezpieczeństwo urządzeń Axis, obsługiwane są:

- Oparte na rolach uprawnienia dostępu do zarządzania urządzeniami (Administrator / Operator / Obserwator) oraz możliwości centralizacji uwierzytelniania / autoryzacji poprzez dołączenie urządzeń Axis do zgodnych ze standardami informatycznymi usług *Active Directory Federation Service* (ADFS) . (ADFS jest komponentem programowym opracowanym przez Microsoft w celu zapewnienia usługi autoryzacji Single Sign-On (SSO) na potrzeby użytkowników w systemach operacyjnych Windows Server. ADFS umożliwia użytkownikom ponad ograniczeniami organizacyjnymi dostęp do aplikacji w systemach operacyjnych Windows Server przy użyciu jednego zestawu uwierzytelnienia logowania).
- Technologie wykorzystujące podejście *zero-trust networking* . W najnowszych wersjach systemu operacyjnego AXIS OS technologie te obejmują protokół IEEE 802.1X wraz z identyfikatorami urządzeń Axis zgodnymi z IEEE 802.1AR do automatycznego i bezpiecznego dołączania urządzeń do sieci IEEE 802.1X oraz IEEE 802.1AE (MACsec) celem automatycznego szyfrowania komunikacji danych.

4.4 Szyfrowanie danych

Aby chronić poufne informacje przed przechwyceniem lub dostępem osób nieupoważnionych, produkty Axis obsługują:

- Protokół HTTPS, w którym cała komunikacja danych obsługuje zabezpieczenia TLS 1.2 lub nowsze. Strumień wizyjny z serwera oprogramowania do zarządzania obrazem AXIS Camera Station do klienta jest szyfrowany algorytmem AES-256.
- Protokół *IEEE 802.1AE (MACsec)* do automatycznego szyfrowania komunikacji danych.
- Bezpieczne strumieniowanie wizyjne przez protokół RTP, określane również jako SRTP / RTSPS (począwszy od systemu AXIS OS 7.40). SRTP / RTSPS wykorzystuje bezpieczną, szyfrowaną metodę transportu end-to-end celem zapewnienia, że strumień wizyjny z urządzenia Axis otrzymują tylko autoryzowani klienci.
- *Szyfrowanie w urządzeniu brzegowym* (karta SD)
- *Eksport nagrań z urządzenia brzegowego chroniony hasłem* (karta SD, zasób sieciowy), począwszy od systemu AXIS OS 10.10. Oznacza możliwość eksportowania nagrań zabezpieczonych hasłem, włącznie z możliwością bezpiecznego udostępniania poufnych danych wizyjnych bez konieczności manualnego szyfrowania eksportowanych nagrań.

4.5 Zgłaszanie incydentów

Axis zapewnia zgłaszanie incydentów związanych z bezpieczeństwem lub luk w zabezpieczeniach wykrytych w naszych produktach i usługach.

- Axis ma status Common Vulnerabilities and Exposures (CVE) Numbering Authority. Oznacza to, że Axis przestrzega najlepszych praktyk branżowych w zakresie zarządzania i reagowania - z zachowaniem transparentności - na wykryte luki w naszych produktach i usługach, co ma na celu zminimalizowanie ryzyka narażenia klientów. Axis może również nadawać numery CVE nowo odkrytym lukom i zgłaszać je na stronie *www.cve.org*. *Polityka zarządzania lukami w zabezpieczeniach* Axis jest publikowana na stronie axis.com.
- Po zapisaniu się pod *tym adresem* każdy zainteresowany będzie otrzymywać od firmy Axis powiadomienia dot. bezpieczeństwa.
- Poprawki zabezpieczeń i poprawki błędów są wprowadzane w nowych wersjach systemu operacyjnego AXIS OS. Dostępność zaktualizowanego oprogramowania jest sygnalizowana w oprogramowaniu AXIS Companion, AXIS Camera Station, AXIS Device Manager, AXIS Device Manager Extend oraz w systemach zarządzania obrazem innych firm np. Milestone XProtect i Genetec Security Center.
- Axis zobowiązuje się do zachowania transparentności w odniesieniu do wszelkich cyberataków związanych z firmą i będzie zgłaszać takie incydenty zgodnie z wytycznymi dostarczonymi przez odpowiednie szwedzkie władze.

4.6 Kwestie powiązane z ochroną prywatności

Axis publikuje własną *politykę prywatności* i informacje na stronie internetowej, w których określa, jakie dane osobowe są gromadzone (na przykład z konta online w My Axis) i w jaki sposób są one przetwarzane.

Axis opublikował również własne *ramy i praktyki w zakresie cyberbezpieczeństwa* odnoszące się do Systemu Zarządzania Bezpieczeństwem Informacji posiadającym certyfikat ISO/IEC 27001. Zakres certyfikatu ISO/IEC

27001 Axis obejmuje rozwój i operacje wewnętrznej infrastruktury informatycznej i usług. ISO 27001 to uznana na całym świecie norma zawierająca wytyczne dotyczące ochrony i zarządzania informacjami organizacji poprzez skuteczne zarządzanie ryzykiem.

Zgodność z normą *ISO/IEC 27001* oznacza, że Axis stosuje uznawane na całym świecie procesy i najlepsze praktyki w celu zarządzania wewnętrzną infrastrukturą oraz systemami informatycznymi, które wspomagają świadczenie usług klientom i partnerom.

Axis pomaga również klientom w rozwiązywaniu problemów związanych z prywatnością w systemach dozorowych w zakresie zapisu i prezentacji obrazu i dźwięku. Rozwiązania obejmują:

- Statyczne maskowanie prywatności w kamerach Axis i dynamiczne maskowanie prywatności w oprogramowaniu *AXIS Live Privacy Shield*.
- Narzędzia analityczne w urządzeniu brzegowym w rodzaju *AXIS People Counter* lub *AXIS P8815-2 3D People Counter* ujmujące i przechowujące jedynie statystyczne dane liczbowe – nie są przetwarzane żadne informacje umożliwiające identyfikację osób.
- *Kamery termowizyjne*
- *Urządzenia radarowe*
- Narzędzie wizyjne w oprogramowaniu *AXIS Camera Station* do maskowania obiektów lub obszarów zainteresowania.
- *Funkcje audio domyślnie wyłączone* w wizyjnych urządzeniach dozorowych Axis.

Więcej informacji na temat rozwiązań w zakresie prywatności znajduje się na stronie *axis.com/solutions/privacy-in-surveillance*

4.7 Bezpieczeństwo łańcucha dostaw

Zabezpieczenie łańcucha dostaw od dostawców komponentów do klientów ma służyć przeciwdziałaniu wprowadzanym lukom w zabezpieczeniach.

Axis podchodzi do kwestii cyberbezpieczeństwa zgodnie z *cyklem eksploatacji* produktu. Jesteśmy zaangażowani w ograniczanie ryzyka, nie tylko w całym łańcuchu dostaw, od poziomu komponentów do gotowego produktu, ale także podczas dystrybucji i wdrażania oraz w fazie serwisowania i wycofywania z eksploatacji.

Poniżej przedstawiono niektóre ze sposobów, w jakie Axis realizuje bezpieczeństwo łańcucha dostaw:

- Axis zaopatruje się w kluczowe komponenty bezpośrednio u strategicznych dostawców. Ściśle współpracujemy z producentami. Procesy produkcyjne są monitorowane, a dane są przekazywane Axis w trybie 24/7, co pozwala na ich analizę w czasie rzeczywistym i zapewnia transparentność. Dowiedz się więcej o *bezpieczeństwie łańcucha dostaw Axis*.
- Wbudowane zabezpieczenia urządzeń dzięki funkcji Axis Edge Vault chroniącej integralność urządzeń Axis za pomocą następujących czynników:
  - **Podpisane oprogramowanie układowe**: gwarantuje, że zainstalowany system operacyjny AXIS OS (oprogramowanie układowe) pochodzi od Axis. Zapewnia również, że każdy nowy system operacyjny AXIS OS przeznaczony do instalacji w urządzeniu jest również podpisany przez Axis.
  - **Bezpieczne uruchamianie**: włączenie w urządzeniu funkcji sprawdzania czy system operacyjny ma sygnaturę Axis. Jeżeli system nie jest autoryzowany lub został zmodyfikowany, uruchamianie

zostanie przerwane i urządzenie przestanie działać. Połączenie podpisanego systemu operacyjnego (oprogramowania układowego), bezpiecznego uruchamiania i przywracania ustawień fabrycznych urządzenia zapewnia ochronę przed próbami modyfikacji podczas transportu urządzenia.

- **Identyfikator urządzenia Axis** jest zgodny ze normą IEEE 802.1AR, co umożliwia bezpieczną identyfikację urządzenia i włączenie go do sieci IP. Identyfikator urządzenia Axis jest przechowywany w bezpiecznym magazynie kluczy urządzenia (bezpieczny element, TPM, TEE).
- **Zaszyfrowany system plików** chroniący konfiguracje własne 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.
- Co więcej, obsługa **podpisanego strumienia wizyjnego (obrazu)** Axis umożliwia sprawdzenie, czy materiał wizyjny wyeksportowany z urządzenia nie został poddany manipulacji. Jest to szczególnie ważne z perspektywy prac wyjaśniających lub postępowania sądowego. Więcej informacji znajduje się na stronie *axis.com/solutions/edge-vault*.

- Suma kontrolna pliku oprogramowania pobieranego ze strony axis.com.
- Certyfikacja ETSI: ponad 150 produktów Axis z systemem AXIS OS 11 lub nowszym posiada certyfikat zgodności z *normą dot. cyberbezpieczeństwa ETSI EN 303 645*. ETSI to skrót od European Telecommunications Standards Institute (Europejski Instytut Norm Telekomunikacyjnych). Wymagania dotyczą samych urządzeń i obejmują takie kwestie jak obsługa sprzętowych funkcji zabezpieczeń, na przykład bezpiecznego przechowywania kluczy, oraz domyślne funkcje zabezpieczeń, takie jak obsługa protokołu HTTPS i brak haseł domyślnych. Kolejnym aspektem jest zarządzanie cyklem eksploatacji, na przykład zdefiniowany okres wsparcia technicznego obejmujący aktualizacje zabezpieczeń urządzeń. Jeszcze inne wymogi zakładają wprowadzenie metodologii ograniczania ryzyka luk podczas opracowywania oprogramowania, wdrożenie przejrzystych zasad zarządzania lukami oraz zgodność z najlepszymi praktykami z zakresu przetwarzania danych osobowych. Wymagania te uwzględniają najlepsze praktyki branżowe zapewniające, że certyfikowane produkty w całym okresie eksploatacji będą mieć pewien minimalny bazowy poziom zabezpieczeń. Norma ta jest ściśle zgodna z unijną ustawą o odporności na cyberzagrożenia, dyrektywą UE dot. urządzeń radiowych oraz innymi normami i przepisami z innych krajów.

4.8 Szkolenia i wskazówki

Axis zapewnia pracownikom, partnerom i klientom informacje i szkolenia dotyczące najlepszych praktyk w zakresie cyberbezpieczeństwa. Obejmują one następujące elementy:

- Świadomość i szkolenia w zakresie bezpieczeństwa wewnętrznego: Firma Axis opracowała program podnoszenia świadomości w zakresie bezpieczeństwa na potrzeby stałego szkolenia swoich pracowników w zakresie unikania i zmniejszania zagrożeń dotyczących bezpieczeństwa organizacji. Szkolenie to jest obowiązkowe dla wszystkich pracowników Axis. W zależności od roli w organizacji i obowiązków danej osoby, programiści i właściciele systemów przechodzą dodatkowe szkolenia z zakresu bezpieczeństwa.
- *Szkolenie w ramach Axis Academy*: Dostępne dla klientów szkolenia obejmują kurs online na temat cyberbezpieczeństwa i *polityki cyberbezpieczeństwa w Axis*.
- *Zalecenia dotyczące zwiększenia funkcjonalności i bezpieczeństwa sieciowego* dostępne online dla:
  - *systemu AXIS OS,*
  - *oprogramowania AXIS Camera Station,*
  - *przełączników sieciowych Axis.*

- *AXIS OS Security Scanner Guide*: Axis zaleca przeprowadzenie skanowania bezpieczeństwa urządzeń Axis w celu sprawdzenia, czy nie są one podatne na ataki lub czy nie mają nieprawidłowej konfiguracji. AXIS OS Security Scanner Guide zawiera zalecenia dotyczące obsługi niektórych wyników skanowania i opisuje najczęstsze fałszywe alarmy.
- *AXIS OS Forensic Guide*: Przewodnik ten zawiera porady techniczne dotyczące wykonywania analiz na potrzeby dowodowe związanych z urządzeniami Axis w razie cyberataku na sieć i infrastrukturę informatyczną, w której zainstalowane jest dane urządzenie Axis.

Aby uzyskać więcej informacji na temat firmy Axis i cyberbezpieczeństwa, zapraszamy na stronę *Portal cyberbezpieczeństwa Axis*.

T10210486/PL/M3.3/2406

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