Cybersecurity reference guide

Podręcznik użytkownika

Cybersecurity reference guide

Spis treści

Cybersecurity reference guide

Wprowadzenie

Wprowadzenie

Ten przewodnik został przygotowany po to, aby zapewnić jednolitą podstawę i punkt odniesienia dla materiałów związanych z cyberbezpieczeństwem opracowanych przez Axis. Są to uproszczone opisy, modele i struktury oparte na konferencjach NIST, SANS, ISO i RSA, a także materiały różnych organizacji zaliczających się do społeczności cyberbezpieczeństwa.

Łącza do innych materiałów Axis:

- *axis.com/about-axis/cybersecurity*
- *help.axis.com/cybersecurity-qna*
- *axis.com/support/cybersecurity/resources*
- *help.axis.com/axis-security-development-model*
- *axis.com/support/cybersecurity/vulnerability-management*

Definicja cyberbezpieczeństwa

Częściowo na podstawie definicji z NIST:

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

Typy organizacji

Organizacje różnią się posiadanymi aktywami, zasobami, ekspozycją i dojrzałością cybernetyczną. Zgodnie z zalecaną praktyką dokument *CIS Controls (wcześniej Critical Security Controls)* definiuje trzy profile organizacji.

- **Grupa implementacji SANS 1 (IG1)**

  Przedsiębiorstwo IG1 jest zwykle małą lub średnią firmą z niewielkim działem IT i ograniczoną ekspertyzą cyberbezpieczeństwa; może więc chronić zasoby IT i pracowników tylko w ograniczonym stopniu.

- **Grupa implementacji SANS 2 (IG2)**

  Przedsiębiorstwo IG2 zwykle zatrudnia osoby odpowiedzialne za zarządzanie infrastrukturą IT i jej ochronę. Firmy te zwykle mają wiele działów z różnymi profilami ryzyka na podstawie ich funkcji i misji. Małe jednostki biznesowe mogą mieć trudności z zapewnienie zgodności z przepisami.

- **Grupa implementacji SANS 3 (IG3)**

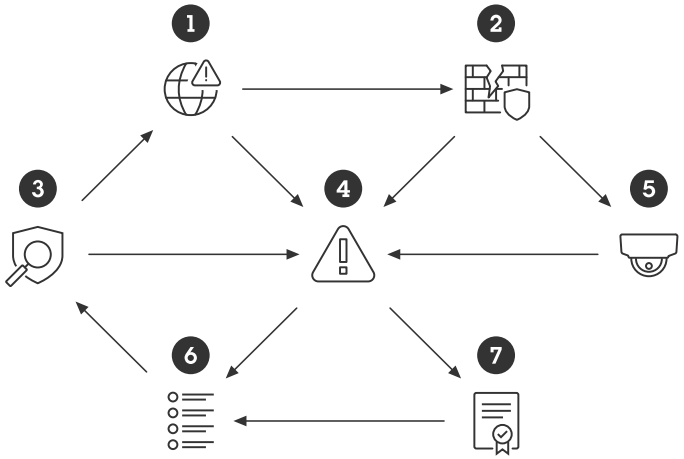
  Przedsiębiorstwo IG3 zwykle zatrudnia specjalistów ds. bezpieczeństwa wyspecjalizowanych w różnych aspektach cyberbezpieczeństwa (np. zarządzaniu ryzykiem, testowaniu penetracji, bezpieczeństwie aplikacji). Aktywa i dane IG3 zawierają poufne informacje lub funkcje, które podlegają nadzorowi regulacyjnemu i nadzorowi zgodności.

Terminologia

Terminologia

Terminologia

Mapa terminologii dobrze obrazuje relacje między najważniejszymi terminami z kategorii cyberbezpieczeństwa omówionymi w tym dokumencie.



- **(1) Zagrożenia** wykorzystują **(2) luki w zabezpieczeniach**, narażając **(5) zasoby** i zwiększając **(4) ryzyko**.
- **(4) Ryzyko** wpływa na **(7) zasady** i określa **(6) wymagania**
- **(6) Wymagania** są uwzględniane w **(3) zabezpieczeniach**, które ciągle stawiają czoła **(1) zagrożeniom**, jednocześnie ograniczając **(4) ryzyko**

Ryzyko

Cyberbezpieczeństwo polega na zarządzaniu ryzykiem w czasie. Ryzyka nigdy nie da się wyeliminować, można je jedynie ograniczyć. Czasami myli się pojęcia, takie jak: ryzyko, zasoby, zagrożenie, luki czy szkody

Ryzyko (zgodnie z definicją w słowniku bezpieczeństwa w internecie RFC 4949 Internet Security Glossary) to oczekiwanie straty wyrażone jako prawdopodobieństwo wykorzystania luki przez dane zagrożenie z określoną szkodą.

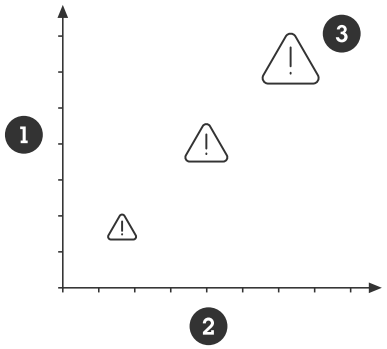
Najczęściej używaną wersją skróconą jest **Ryzyko = Prawdopodobieństwo x Negatywne skutki**

Ta formuła służy do ustalania priorytetów ryzyka. W definicji RFC jest zawarty termin „szczególne" odnoszący się do zagrożeń, luk w zabezpieczeniach i szkodliwych skutków. Wszystkie zagrożenia muszą być rozpatrywane osobno, zaczynając od tego, które jest najbardziej prawdopodobne i może mieć najgorsze negatywne skutki.

Podczas rozważania ryzyka sporym wyzwaniem jest czynnik prawdopodobieństwa. Coś może się wydarzyć, ale nie musi. Prawdopodobieństwo wykorzystania luki przez przeciwnika jest często określane na podstawie łatwości jej wykorzystania (ekspozycji) i potencjalnych korzyści dla przeciwnika.

Ryzyko można rozpatrywać na tych dwóch wymiarach: jedną osią jest prawdopodobieństwo wystąpienia ryzyka, a drugą — jego skutki, w razie gdyby wystąpiło. Pozwala to uzyskać jasny obraz potencjalnego znaczenia i priorytetu, jaki należy nadać każdemu ryzyku.

Terminologia



1 ***Prawdopodobieństwo*** *od niskiego do wysokiego*
2 ***Negatywny wpływ*** *od niskiego do wysokiego*
3 ***Poziomy ryzyka*** *od niskiego do wysokiego*

Wartość ataku = Korzyści z ataku – Koszty ataku

Im lepsze zabezpieczenia, tym większe koszty ataku, a tym samym jego mniejsze prawdopodobieństwo. Koszt ataku to czas, zasoby, umiejętności i motywacja wymagane do jego pomyślnego przeprowadzenia. Do kosztów ataku zalicza się też ryzyko ujęcia, wykrycia oraz inne negatywne konsekwencje.

Ocena ryzyka, a więc proces jego analizy w cyberprzestrzeni, wygląda tak samo, jak w przypadku zabezpieczeń fizycznych. W tym kontekście trzeba zadać sobie następujące pytania:

1. Co chcemy chronić?
2. Przed kim chcemy to chronić?
3. Jakie jest prawdopodobieństwo negatywnych skutków?
4. Na ile dotkliwe będą konsekwencje, gdy coś nie pójdzie zgodnie z planem?
5. Jakie strategie trzeba wdrożyć w celu ograniczenia ryzyka?

Wszystkie środki ochrony i kontroli bezpieczeństwa kosztują. A wszystkie organizacje mają ograniczone budżety. Nie znając ryzyka, trudno określić budżet potrzebny do odpowiedniego zabezpieczenia zasobów. Nie da się całkowicie wyeliminować zagrożeń, ale to, do jakiego stopnia jesteśmy w stanie je akceptować, musi być świadomą decyzją popartą analizą ryzyka.

Oszacowanie potencjalnych szkód dla poszczególnych typów zasobów jest trudne i skomplikowane. Często te szacunki są subiektywne, a ewentualne szkody są niedoszacowane. Korzystanie z modelu skutków ISO 27000 i typów oznaczeń: Ograniczony, Znaczący, Poważny lub Katastrofalny pomaga kategoryzować zagrożenia i odpowiednio nadawać im priorytety. W ten dość prosty sposób można ustalić dokładniejszą wartość na podstawie tego, ile czasu wymaga przywrócenie sprawności, gdy dojdzie do skutecznego ataku:

- **Ograniczone** = od kilku godzin do kilku dni
- **Poważne** = od kilku dni do kilku tygodni
- **Ciężkie** = od kilku tygodni do kilku miesięcy
- **Katastrofalne** = od kilku miesięcy do kilku lat

Aktywa

Podczas gdy ochrona fizyczna koncentruje się na ochronie osób i obiektów fizycznych, ochrona cyberbezpieczeństwa koncentruje się na ochronie aktywów danych i komputerowych. Można tu wyróżnić trzy główne obszary:

- **Poufność**: ujawnianie informacji lub zasobów

Terminologia

- **Nienaruszalność**: niszczenie lub modyfikowanie informacji lub zasobów
- **Dostępność**: dostęp do informacji i zasobów

Te cele bezpieczeństwa komputerowego zwane są też triadą CIA. Osoby odpowiedzialne za technologie operacyjne (OT) często nadają priorytet użyteczności systemu, natomiast IT koncentruje się na bezpieczeństwie. Często znalezienie złotego środka między poufnością, nienaruszalnością i dostępnością jest bardzo trudne.

Aktywa i zasoby powinny być odpowiednio klasyfikowane, aby można było przypisać do nich odpowiednie poziomy zabezpieczeń. Naruszenia bezpieczeństwa niektórych danych aktywów i zasobów komputerowych może być gorsze w skutkach niż atak na inne zasoby i dane. Zasoby te dzieli się często na następujące kategorie:

- **Publiczne**: zasób jest przeznaczony dla opinii publicznej lub jest to taki zasób, którego publiczne ujawnienie wiąże się z niewielkimi negatywnymi skutkami.
- **Prywatne**: zasoby przeznaczone dla konkretnej/wybranej grupy odbiorców. Zazwyczaj szkody związane z ujawnieniem takich zasobów są ograniczone do konkretnej organizacji lub np. rodziny.
- **Z ograniczonym dostępem**: zasoby te są przeznaczone tylko dla wybranych osób w organizacji.

Obraz wideo na żywo w systemie wideo można sklasyfikować jako publiczny, co odnosi się zarówno do ogółu społeczeństwa, jak członków organizacji. W większości przypadków obraz wideo na żywo jest jednak uznawany za dane prywatne, co oznacza, że jest on dostępny i przeznaczony tylko dla określonej jednostki organizacyjnej. Natomiast nagranie wideo w większości przypadków jest klasyfikowane jako dane z ograniczonym dostępem ze względu na to, że może ono zawierać sceny uznawane za bardzo wrażliwe. Do danych z ograniczonym dostępem powinny być zaliczane także poświadczenia i konfiguracje.

Zagrożenia

Zagrożeniem może być wszystko, co może zagrozić lub zaszkodzić aktywom lub zasobom użytkownika. Generalnie cyberzagrożenia kojarzymy zwykle ze złośliwymi hakerami i złośliwym oprogramowaniem. Jednak przyczyną szkód często są również wypadki, niezamierzone użycie lub awarie sprzętu.

Ataki nie biorą się znikąd. Cyberprzestępcy zawsze mają jakąś motywację, by włamać się do systemu i jego aktywów. Ataki można podzielić na oportunistyczne lub celowe. W branży cyberbezpieczeństwa atakujących uznaje się też za przeciwników, którzy mogą mieć złośliwe zamiary.

Większość dzisiejszych ataków to ataki oportunistyczne: tj. takie, które mają miejsce, ponieważ nadarza się do tego okazja. Często osoba przeprowadzająca atak oportunistyczny nawet nie wie, kim jest ofiara. Tacy atakujący wykorzystują niskokosztowe wektory ataku, takie jak phishing i sondowanie. Nie mają oni motywacji, żeby poświęcać czas ani zasoby na nieudany atak, dlatego szybko przechodzą do kolejnej próby. Standardowy poziom ochrony pozwala ograniczyć większość zagrożeń związanych z atakami oportunistycznymi. Trudniej jest chronić się przed atakami kierowanymi przeprowadzanymi przez napastników, którzy obierają za cel konkretny system. Ataki celowe wykorzystują te same niskokosztowe wektory ataku, jednak jeżeli początkowe ataki zakończą się niepowodzeniem, intruzi są bardziej zdeterminowani i skłonni poświęcić czas i zasoby, by zastosować bardziej wyrafinowane metody do osiągnięcia swoich celów. To zależy w dużej mierze od wartości celu ataku.

Najczęstsi przeciwnicy (cyberprzestępcy)

- **Fałszywi przyjaciele**: osoby próbujące zdobyć zaufanie, by zdobyć Twoje dane prywatne
- **Pracownicy**: lub osoby, które legalnie uzyskały dostęp do systemu, przez przypadek lub umyślne nadużycie
- **Żartownisie:** osoby czerpiące osobistą satysfakcję z atakowania systemów
- **Haktywiści**: osoby atakujące organizacje z powodów politycznych lub ideologicznych
- **Cyberprzestępcy**: osoby zainteresowane zarabianiem pieniędzy na oszustwach lub sprzedawaniu wartościowych informacji
- **Konkurencja z branży**: osoby chcące uzyskać korzyści lub przewagę dla swoich firm lub organizacji
- **Cyberterroryści**: osoby lub podmioty, które przeprowadzają atak celem wywołanie alarmu lub paniki; ich motywy są często ideologiczne lub polityczne

Terminologia

- **Państwa narodowe**: agenci obcych służb wywiadowczych działający w celu uzyskania korzyści ekonomicznych i politycznych lub wyrządzenia szkód krytycznym systemom informatycznym
- **Cyberprzestępcy indywidualni**: konkretne osoby lub grupy działające na własną rękę, których motywacja może być inna od wymienionych powyżej. Mogą to być dziennikarze śledczy, tzw. hakerzy w białych kapeluszach itp. Hakerzy w białych kapeluszach (znani też jako etyczni hakerzy) mogą stanowić zagrożenie, jeśli właścicielowi systemu bardziej zależy na ukryciu luk niż ich naprawieniu.

Luka

Wszystkie systemy mają luki. Przez te luki w zabezpieczeniach intruzi mogą zaatakować system lub uzyskać do niego dostęp. Mogą one wynikać z wad, ekspozycji, cech systemu lub błędów ludzkich. Osoby atakujące systemy mogą wykorzystywać wszelkie znane luki, często kilka równocześnie. Większość udanych ataków jest skutkiem błędów ludzkich, niewłaściwie skonfigurowanych i źle konserwowanych systemów. Często wynika to z braku odpowiednich zasad, nieprecyzyjnego określenia obowiązków i niskiej świadomości zagrożeń wśród pracowników organizacji.

Luki w oprogramowaniu

Interfejs API urządzenia (Application Programming Interface) i usługi oprogramowania mogą mieć wady lub funkcje, które można wykorzystać do ataku na system. Żaden dostawca nie może zagwarantować, że jego produkt nie ma luk. Jeśli są one znane, ryzyko można złagodzić za pomocą kompensujących środków kontroli bezpieczeństwa. Z drugiej strony, gdy atakujący odkrywa nową, nieznaną lukę, wzrasta ryzyko powodzenia exploitów zero-day, ponieważ nie ma wtedy czasu na zabezpieczenie systemu.

Common Vulnerability Scoring System (CVSS) to standard branżowy służący do oceny stopnia zagrożenia bezpieczeństwa oprogramowania. Jest to wzór, za pomocą którego można sprawdzić, jak łatwo da się wykorzystać system i jakie mogą być tego negatywne skutki. Wynik jest wartością od 0 do 10, gdzie 10 oznacza największe zagrożenie. Numer CVSS można często znaleźć w opublikowanych raportach Common Vulnerabilities and Exposures (CVE).

Axis wykorzystuje CVSS jako jedną z miar określających, na ile poważne zagrożenie może powodować luka wykryta w oprogramowaniu/produkcie.

Zasada

Ważne jest, aby zdefiniować jasne zasady i procesy systemowe w celu zapewnienia odpowiedniego ograniczenia ryzyka w długiej perspektywie. Zalecaną strategią jest podejściem jest precyzyjne zdefiniowanie schematu ochrony IT, np. zgodnie z normami ISO 27001, NIST itp. Mimo że zadanie to może wydawać się przytłaczające dla mniejszych organizacji, to posiadanie nawet minimalnej dokumentacji zasad i procesów jest o wiele lepsze niż nieposiadanie niczego.

Funkcje zabezpieczeń

Funkcje zabezpieczeń to zabezpieczenia lub środki zapobiegawcze stosowane w celu unikania, wykrywania lub minimalizowania zagrożeń dla mienia fizycznego, informacji, systemów komputerowych lub innych aktywów. Wdrażanie zabezpieczeń często jest nazywane zabezpieczaniem.

Zabezpieczenia uzupełniające to alternatywne zabezpieczenia, które mogą być stosowane, gdy zastosowanie preferowanej formy zabezpieczeń jest niemożliwe, jest ona niedostępna lub zbyt kosztowna.

Funkcje zabezpieczeń wymagają stałego monitorowania i aktualizowania w miarę zmieniających się zagrożeń, wartości chronionych zasobów, luk w zabezpieczeniach i ekspozycji na niebezpieczeństwo. To z kolei wymaga określenia i przestrzegania zasad oraz procesów.

SANS Institute opublikował *listę zabezpieczeń CIS*, będącą zestawem zalecanych najlepszych rozwiązań w kategorii cyberbezpieczeństwa organizacji. Poniżej przedstawiamy pełną listę zabezpieczeń, aby pokazać ich różnorodność.

- Zabezpieczenie CIS nr 1: Inwentaryzacja i kontrola aktywów przedsiębiorstwa
- Zabezpieczenie CIS nr 2: Inwentaryzacja i kontrola zasobów oprogramowania
- Zabezpieczenie CIS nr 3: Ochrona danych

Terminologia

- Zabezpieczenie CIS nr 4: Bezpieczna konfiguracja zasobów i oprogramowania firmy
- Zabezpieczenia CIS nr 5: Zarządzanie kontami
- Zabezpieczenia CIS nr 6: Zarządzanie kontrolą dostępu
- Zabezpieczenia CIS nr 7: Stałe zarządzanie podatnością na ataki
- Zabezpieczenia CIS nr 8: Zarządzanie dziennikami audytów
- Zabezpieczenia CIS nr 9: Ochrona poczty elektronicznej i przeglądarek internetowych
- Zabezpieczenia CIS nr 10: Zabezpieczenia przed złośliwym oprogramowaniem
- Zabezpieczenia CIS nr 11: Odzyskiwanie danych
- Zabezpieczenia CIS nr 12: Zarządzanie infrastrukturą sieciową
- Zabezpieczenia CIS nr 13: Monitorowanie i ochrona sieci
- Zabezpieczenia CIS nr 14: Szkolenie w zakresie świadomości i umiejętności w zakresie bezpieczeństwa
- Zabezpieczenia CIS nr 15: Zarządzanie dostawcami usług
- Zabezpieczenia CIS nr 16: Bezpieczeństwo oprogramowania i aplikacji
- Zabezpieczenia CIS nr 17: Zarządzanie reagowaniem na incydenty
- Zabezpieczenia CIS nr 18: Testowanie penetracyjne

AXIS OS Hardening Guide (Przewodnik po zabezpieczeniach systemu operacyjnego AXIS) jest oparty na liście CIS.

Środki ochrony przed częstymi zagrożeniami

Środki ochrony przed częstymi zagrożeniami

Większość typów ryzyka można ograniczyć dzięki dobremu zrozumieniu częstych zagrożeń i przeciwdziałaniu im.

Celowe lub przypadkowe nieprawidłowe używanie systemu

Uzyskanie równowagi między użytecznością a bezpieczeństwem systemu jest trudne. W przypadku wielu systemów wzmocnienia są uwarunkowane komfortem a nie bezpieczeństwem. Stwarza to możliwości celowego lub przypadkowego niewłaściwego użycia. Najczęstszym zagrożeniem dla systemu są osoby uprawnione do korzystania z niego.

Przykłady typowych zagrożeń:

- Osoby fizyczne mogą uzyskać dostęp do usług (np. obrazu wizyjnego na żywo lub nagranych materiałów wideo), do których nie mają uprawnienia
- Ludzie popełniają błędy
- Użytkownicy mogą próbować naprawić problemy, prowadząc do zmniejszenia wydajności systemu
- Osoby sfrustrowane mogą ukraść sprzęt/dane lub celowo uszkodzić system
- Osoby są podatne na socjotechnikę
- Osoby mogą dopuszczać się kradzieży
- Poszczególne osoby mogą też zgubić lub przenosić w inne miejsce krytyczne elementy systemów (karty dostępu, telefony, laptopy, dokumentację i inne zasoby).
- Może także dojść do naruszenia bezpieczeństwa komputera użytkownika, a następnie nieświadomego zainfekowania systemu oprogramowaniem.

Często zaleca się stosowanie następujących środków bezpieczeństwa:

- Zdefiniowane zasady i proces dotyczące kont użytkowników
- Wystarczający schemat uwierzytelniania dostępu
- Narzędzia do zarządzania kontami i uprawnieniami użytkowników w czasie
- Zmniejszenie ekspozycji
- Budowanie świadomości cyberzagrożeń

W jaki sposób firma Axis pomaga w radzeniu sobie z tymi zagrożeniami:

- *Przewodnik po zabezpieczeniach systemu operacyjnego AXIS* opisuje typowe zabezpieczenia przed typowym ryzykiem dla urządzenia
- *Przewodnik po zabezpieczeniach programu AXIS Camera Station* opisuje typowe zabezpieczenia systemów wideo
- *AXIS Device Manager* i *AXIS Device Manager Extend* pomagają zarządzać typowymi zabezpieczeniami

Uszkodzenia fizyczne i sabotaż

Z punktu widzenia cyberbezpieczeństwa bardzo ważne jest fizyczne zabezpieczenie systemów IT.

Przykłady typowych zagrożeń:

- Sprzęt niezabezpieczony fizyczne może być użyty do sabotażu
- Sprzęt niezabezpieczony fizyczne może zostać skradziony

Środki ochrony przed częstymi zagrożeniami

- Kable niezabezpieczone fizyczne mogą zostać odłączone, przekierowane lub przecięte

Często zaleca się stosowanie następujących środków bezpieczeństwa:

- Umieścić sprzęt sieciowy (np. serwery i przełączniki) w zamkniętych pomieszczeniach
- Montować kamery w miejscach trudno dostępnych
- W przypadku fizycznego narażenia stosować obudowę ochronną
- Zabezpieczyć kable w ścianach lub przewodach

W jaki sposób firma Axis pomaga w radzeniu sobie z tymi zagrożeniami:

- Zaszyfrowana karta SD zapobiegająca odtwarzaniu wideo, jeśli użytkownik bez uprawnień może ją wysunąć
- Wykrywanie sabotażu widoku kamery
- Wykrywanie otwartej obudowy

Wykorzystywanie znanych luk w zabezpieczeniach oprogramowania

Wszystkie produkty oparte na oprogramowaniu mają luki w zabezpieczeniach, które mogą zostać wykorzystane. Luki w zabezpieczeniach można podzielić na znane i nieznane. Wszystkie obecnie nieznane luki w zabezpieczeniach stają się znane po jakimś czasie. Większość z nich nie niesie ze sobą dużego ryzyka, co oznacza, że ich ewentualne wykorzystanie może wyrządzić bardzo ograniczone szkody. Czasami jednak zdarzają się takie luki w zabezpieczeniach, których wykorzystanie może spowodować bardzo poważne problemy. MITRE prowadzi dużą bazę danych CVE (Common Vulnerabilities & Exposures), by pomagać w redukowaniu tego ryzyka.

Często zaleca się stosowanie następujących środków bezpieczeństwa:

- Stałe instalowanie łatek pomaga zminimalizować liczbę znanych luk w systemie.
- Warto też minimalizować ekspozycję urządzeń i danych w sieci, aby utrudnić cyberprzestępcom sondowanie i wykorzystywanie znanych luk w zabezpieczeniach.
- Kolejną praktyką wartą polecenia jest współpracowanie tylko z zaufanymi poddostawcami przestrzegającymi zasad i procesów, które minimalizują błędy, a także stosują procesy dostarczania poprawek i ujawniają informacje o wykryciu krytycznych luk w zabezpieczeniach.

W jaki sposób Axis może pomóc:

- *Model rozwoju zabezpieczeń AXIS* jest strukturą definiującą procesy i narzędzia wykorzystywane przez Axis, które mają na celu maksymalne ograniczanie ryzyka wprowadzenia na rynek produktów zawierających luki w oprogramowaniu.
- *Zasady zarządzania lukami w zabezpieczeniach rozwiązań Axis* obejmują identyfikowanie, usuwanie i ujawnianie luk w zabezpieczeniach, o których klienci muszą wiedzieć, aby móc adekwatnie reagować. Od kwietnia 2021 roku firma Axis jest akredytowaną organizacją odpowiedzialną za indeksowanie znanych luk w zabezpieczeniach (Common Vulnerability and Exposures Numbering Authority) dla produktów Axis, co pozwala nam dostosować nasze procesy do standardowego procesu branżowego MITRE Corporation). Dzięki temu możemy zapewnić lepszą pomoc naszym klientom.
- *Przewodniki Axis dotyczące zabezpieczeń*, takie jak *Przewodnik po zabezpieczeniach systemu operacyjnego AXIS*, zawierają zalecenia dotyczące sposobu minimalizowania ekspozycji i dodawania rozwiązań kompensacyjnych w celu maksymalnego ograniczania ryzyka wykorzystania błędów w oprogramowaniu.
- Wersje oprogramowania sprzętowego LTS (z długoterminowym wsparciem) umożliwiają klientom łatanie systemu operacyjnego urządzeń Axis przy jednoczesnym minimalizowaniu ryzyka niezgodności z systemami zarządzania materiałem wizyjnym innych firm.

Środki ochrony przed częstymi zagrożeniami

Atak na łańcuch dostaw

Atak na łańcuch dostaw to cyberatak, którego celem jest wyrządzenie szkód organizacji za pośrednictwem gorzej zabezpieczonych elementów w łańcuchu dostaw. Jest on stosowany głównie wtedy, gdy inne wektory ataku (np. socjotechnika, phishing i sondowanie interfejsu) zawodzą ze względu na wysoki poziom ochrony systemu. Atak jest przeprowadzany przez nakłonienie administratora do zainstalowania w systemie oprogramowania (układowego) lub produktu wprowadzającego w nim luki. Takie zmiany w produkcie mogą być wprowadzane na etapie wysyłki do właściciela systemu. Do skutecznego przeprowadzenia ataku na łańcuch dostaw potrzeba umiejętności, czasu i zasobów.

Często zaleca się stosowanie następujących środków bezpieczeństwa:

- Wprowadzenie zasady instalowania oprogramowania pochodzącego wyłącznie z zaufanych i zweryfikowanych źródeł.
- Sprawdzenie integralności oprogramowania poprzez porównanie sumy kontrolnej z sumą kontrolną dostawcy przed instalacją.
- Sprawdzenie pakietu produktu pod kątem oznak sabotażu.

W jaki sposób firma Axis pomaga w radzeniu sobie z tymi zagrożeniami:

- Axis publikuje oprogramowanie z sumą kontrolną, aby administratorzy mogli sprawdzić jego integralność przed instalacją.
- Podpisane oprogramowanie w urządzeniach Axis gwarantuje, że zainstalowany system operacyjny (AXIS OS) został udostępniony przez firmę Axis i że każde nowe oprogramowanie sprzętowe, które zostanie pobrane i zainstalowane na urządzeniu, również będzie podpisane przez firmę Axis.
- Funkcja bezpiecznego rozruchu w urządzeniach Axis umożliwia sprawdzenie, czy oprogramowanie sprzętowe jest podpisane przez firmę Axis. Jeśli oprogramowanie sprzętowe nie zostało autoryzowane lub było modyfikowane, proces rozruchu zostanie przerwany.
- Identyfikator urządzenia Axis zgodny ze standardem IEEE 802.1AR to niepowtarzalny certyfikat dostawcy, przypisany do urządzenia Axis, który umożliwia systemowi sprawdzenie, czy sprzęt zawarty w produkcie pochodzi od firmy Axis.
- Dzięki szyfrowaniu kart SD i systemu plików w razie kradzieży urządzenia lub karty nie jest możliwe wyodrębnienie przechowywanych na nich informacji.

Podręcznik użytkownika
Cybersecurity reference guide

Wer. M3.2
Data: Listopad 2023
Numer części T10201166