Pytania i odpowiedzi dotyczące cyberbezpieczeństwa

Podręcznik użytkownika

Pytania i odpowiedzi dotyczące cyberbezpieczeństwa

Aby uzyskać odpowiedzi na inne pytania, przejedź do *bazy najczęściej zadawanych pytań* Axis.

Pytania i odpowiedzi dotyczące cyberbezpieczeństwa

Pytania ogólne

Pytania ogólne

Czym jest cyberbezpieczeństwo?

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.

Cyberbezpieczeństwo polega na zarządzaniu ryzykiem w dłuższym okresie czasu. Ryzyka nigdy nie da się wyeliminować, można je jedynie ograniczyć.

Co ogólnie wiąże się z zarządzaniem cyberbezpieczeństwem?

Cyberbezpieczeństwo to produkty, ludzie, technologia i bieżące procesy.

Dlatego wymaga **identyfikacji** i oceny różnych aspektów organizacji, w tym przeprowadzenia inwentaryzacji urządzeń, systemów i oprogramowania (układowego); ustalenia celów o znaczeniu krytycznym; udokumentowania procedur i zasad bezpieczeństwa; wdrożenia strategii zarządzania ryzykiem oraz ciągłego weryfikowania stanu ryzyka związanego z aktywami.

Obejmuje to wdrożenie kontroli bezpieczeństwa i środków **ochrony** przed cyberatakami danych, urządzeń, systemów i obiektów, które zidentyfikowano jako priorytetowe.

Wymaga to także opracowania i wdrożenia działań, które pomogą **wykrywać** cyberataki, by ułatwić podejmowanie działań w porę. Mogą to być na przykłady systemy Security Information and Event Management (SIEM) lub Security Orchestration, Automation and Response (SOAR) obsługujące dane z urządzeń sieciowych i oprogramowania zarządzającego, zbierające dane o nieprawidłowym zachowaniu lub potencjalnych cyberatakach i analizujące te dane, by zapewnić ostrzeżenia w czasie rzeczywistym. Urządzenia Axis obsługują dzienniki SYS Logs i Remote SYS Logs, będące podstawowym źródłem danych dla systemów SIEM lub SOAR.

Zarządzanie cyberbezpieczeństwem obejmuje również opracowanie i wdrożenie procedur **reagowania** na wykryte incydenty cyberbezpieczeństwa. Należy uwzględnić przy tym lokalne przepisy oraz zasady wewnętrzne, a także wymagania dotyczące ujawniania incydentów cyberbezpieczeństwa. Axis oferuje przewodnik *AXIS OS Forensic Guide*, który pomaga ustalić, czy dane urządzenie Axis zostało narażone na szwank podczas cyberataku.

Istotne będzie również opracowanie i wdrożenie działań mających na celu utrzymanie planów odporności, **odzyskiwania** danych i przywracania sprawności funkcji i usług, które mogły ucierpieć w wyniku incydentu cyberbezpieczeństwa. Na przykład *AXIS Device Manager* ułatwia przywracanie sprawności urządzeń Axis dzięki obsłudze punktów przywracania, które są zapisanymi „migawkami" konfiguracji systemu w danym momencie. W przypadku braku odpowiedniego punktu przywracania narzędzie może pomóc w przywróceniu wszystkich urządzeń do ich domyślnych stanów i rozesłać przez sieć zapisane szablony konfiguracji.

Czym jest ryzyko cyberbezpieczeństwa?

Ryzyko cyberbezpieczeństwa (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.*

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.

Informacje o tym, jak oceniać ryzyko i jego stopień, można znaleźć w *Przewodniku po cyberbezpieczeństwie*.

Czym jest zagrożenie?

Zagrożeniem może być wszystko, co może zagrozić lub zaszkodzić aktywom lub zasobom użytkownika. Generalnie cyberzagrożenia kojarzymy zwykle ze złośliwymi hakerami i złośliwym oprogramowaniem. Jednak w rzeczywistości za szkody często odpowiadają wypadki, niezamierzone użycie lub awarie sprzętu. Ataki można podzielić na oportunistyczne lub celowe. Większość dzisiejszych ataków to ataki oportunistyczne: tj. takie, które mają miejsce, ponieważ nadarza się do tego okazja. Takie ataki wykorzystują

Pytania ogólne

niskokosztowe wektory ataku, takie jak phishing i sondowanie. Zastosowanie standardowego poziomu ochrony pozwala ograniczyć większość zagrożeń związanych z atakami oportunistycznymi.

Trudniej jest chronić się przed napastnikami, 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.

Jakie są najczęstsze zagrożenia i jak można sobie z nimi radzić?

Celowe lub przypadkowe nieprawidłowe używanie systemu

Jednym z najczęstszych zagrożeń dla systemu są osoby uprawnione do korzystania z niego. Osoby te mogą uzyskiwać dostęp do usług, do korzystania z których nie są uprawnione. Osoby takie mogą ukraść sprzęt/dane lub celowo uszkodzić system. Ponadto ludzie mogą popełniać błędy. Próbując naprawiać problemy, mogą nieumyślnie pogarszać wydajność systemu. Ludzie są też podatni na manipulację, czyli sztuczki, które sprawiają, że uprawnieni użytkownicy zdradzają poufne informacje. 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.

Zaleca się stosowanie środków zabezpieczających, takich jak opracowanie i wdrożenie zasad oraz procesu tworzenia kont użytkowników, posiadanie odpowiednich procedur uwierzytelniania dostępu, posiadanie narzędzi do zarządzania kontami użytkowników i uprawnieniami na przestrzeni czasu, ograniczanie ekspozycji na zagrożenia oraz przeprowadzanie szkoleń podnoszących świadomość w zakresie zagrożeń dla bezpieczeństwa cybernetycznego.

Firma Axis pomaga zapobiegać tym zagrożeniom, oferując *instrukcje wzmacniania zabezpieczeń* oraz narzędzia, takie jak *AXIS Device Manager* i *AXIS Device Manager Extend*.

Uszkodzenia fizyczne i sabotaż

W przypadku sprzętu narażonego na zagrożenia fizyczne może dojść do sabotażu, kradzieży, odłączenia, przekierowania lub odcięcia.

Zalecane zabezpieczenia obejmują umieszczanie sprzętu sieciowego (na przykład serwerów i przełączników) w zamkniętych pomieszczeniach, montowanie kamer w taki sposób, aby były trudno dostępne, stosowanie chronionych/wzmacnianych obudów, gdy są mogą być one narażone na fizyczne uszkodzenie, a także zabezpieczanie kabli w ścianach lub kanałach.

Axis pomaga temu przeciwdziałać temu dzięki *ochronnym obudowom* urządzeń, śrubom zabezpieczającym przed sabotażem, kamerom z możliwością szyfrowania kart SD, detekcji sabotażu obrazu z kamery oraz detekcji otwarcia obudowy.

Wykorzystywanie luk w oprogramowaniu

Wszystkie produkty oparte na oprogramowaniu mają (znane lub nieznane) luki, które mogą zostać wykorzystane. Większość z nich nie niesie ze sobą dużego ryzyka, więc ich ewentualne odkrycie i wykorzystanie ma ograniczony negatywny wpływ. Jednak czasami mogą występować luki, których ewentualne wykorzystanie może mieć bardzo negatywny efekt. MITRE prowadzi dużą bazę danych CVE (Common Vulnerabilities & Exposures), by pomagać w redukowaniu tego ryzyka.

Zalecane zabezpieczenia obejmują wdrożenie ciągłego procesu implementacji poprawek, który pomaga ograniczyć liczbę znanych luk w systemie, zmniejszyć ekspozycję sieci, by utrudnić sondowanie i wykorzystanie znanych luk, i nawiązać współpracę z zaufanymi poddostawcami, którzy stosują zasady i procesy minimalizujące błędy, dostarczają poprawki i mają przejrzysty proces w odniesieniu do odkrytych luk o znaczeniu krytycznym.

Axis pomaga zażegnać to zagrożenie za pomocą *Axis Security Development Model*, którego celem jest zminimalizowanie możliwych do wykorzystania luk w oprogramowaniu Axis; a także za pomocą *Axis Vulnerability Management Policy*, która służy do identyfikowania, naprawy i ogłaszania luk w zabezpieczeniach, o których klienci muszą wiedzieć, by podjąć odpowiednie działania. (Od kwietnia 2021 roku *Axis jest organizacją odpowiedzialną za indeksowanie znanych luk (Common Vulnerability and Exposures Numbering Authority)* dla produktów Axis, co pozwala nam dostosować nasze procesy do standardowego procesu branżowego MITRE Corporation). Axis udostępnia również *przewodniki* z zaleceniami, jak zmniejszyć ekspozycję i zapewnić większy poziom kontroli w celu zmniejszenia ryzyka wykorzystania luk. Axis oferuje użytkownikom *dwie ścieżki aktualizacji oprogramowania urządzeń* w celu zachowania aktualności systemu operacyjnego Axis:

1. Ścieżka aktywna zapewnia aktualizacje oprogramowania urządzenia, które obsługują nowe funkcje, a także poprawki błędów i zabezpieczeń.

Pytania ogólne

2. Ścieżka długoterminowego wsparcia (LTS) zapewnia aktualizacje oprogramowania urządzenia z poprawkami błędów i zabezpieczeń, które jednocześnie minimalizują ryzyko wystąpienia problemów z niekompatybilnością z systemami innych firm.

Atak na łańcuch dostaw

Atak na łańcuch dostaw to cyberatak, którego celem jest wyrządzenie szkód organizacji za pośrednictwem gorzej zabezpieczonych elementów w łańcuchu dostaw. Atak jest przeprowadzany przez nakłonienie administratora do zainstalowania w systemie oprogramowania (systemu operacyjnego) lub produktu wprowadzającego w nim luki. Takie zmiany w produkcie mogą być wprowadzane na etapie wysyłki do właściciela systemu.

Aby bronić się przed tego rodzaju atakami, zalecane jest wdrożenie zasad instalowania tylko oprogramowania pochodzącego z zaufanych i zweryfikowanych źródeł, weryfikowania integralności oprogramowania poprzez porównanie sumy kontrolnej (skrótu) oprogramowania z sumą kontrolną dostawcy przed instalacją oraz sprawdzania dostaw produktów pod kątem oznak sabotażu.

Axis przeciwdziała tym zagrożeniom na kilka sposobów. Axis publikuje oprogramowanie z sumą kontrolną, aby administratorzy mogli sprawdzić jego integralność przed instalacją. Gdy ma zostać wczytany nowy system operacyjny urządzenia, urządzenia sieciowe Axis zaakceptują tylko oprogramowanie urządzenia podpisane przez Axis. *Bezpieczne uruchamianie* na urządzeniach sieciowych Axis zapewnia również, że urządzenie może być uruchomione tylko za pomocą systemu operacyjnego podpisanego przez Axis. Każde urządzenie ma unikalny identyfikator urządzenia Axis, za pomocą którego system może zweryfikować, czy urządzenie jest oryginalnym produktem Axis. Szczegóły dotyczące takich funkcji cyberbezpieczeństwa można znaleźć w oficjalnym dokumencie *Axis Edge Vault* (pdf).

Aby dowiedzieć się więcej o zagrożeniach, przeczytaj *Przewodnik po cyberbezpieczeństwie*.

Czym są luki?

Luki w zabezpieczeniach umożliwiają przeciwnikom zaatakowanie systemu lub uzyskanie do niego dostępu. Mogą one wynikać z wad, funkcji lub błędów ludzkich. Osoby atakujące systemy mogą wykorzystywać wszelkie znane luki, często łącząc jedną lub więcej. Większość skutecznych 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.

Czym są luki oprogramowaniu?

Interfejs API urządzenia (Application Programming Interface) i usługi oprogramowania mogą mieć luki lub funkcje, które można wykorzystać do ataku na system. Żaden sprzedawca nie może zagwarantować, że jego produkty nie mają luk. Jeśli luki są znane, ryzyko można ograniczyć za pomocą środków kontroli bezpieczeństwa. Z drugiej strony, gdy atakujący odkrywa nową, nieznaną lukę, ryzyko wzrasta, ponieważ nie ma wtedy czasu na zabezpieczenie systemu.

Czym jest Common Vulnerability Scoring System (CVSS)?

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 można wykorzystać system i jakie mogą być negatywne skutki. Wynik jest wartością od 0 do 10, gdzie 10 oznacza największe zagrożenie. Numer CVSS można często znaleźć w opublikowanych raportach Common Vulnerability and Exposure (CVE).

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

Pytania i odpowiedzi dotyczące cyberbezpieczeństwa

Pytania dotyczące rozwiązań Axis

Pytania dotyczące rozwiązań Axis

Z jakich szkoleń i przewodników można skorzystać, aby dowiedzieć się więcej o cyberbezpieczeństwie i zabezpieczaniu produktów oraz usług przed cyberatakami i innymi zagrożeniami?

Na stronie *Resources (Zasoby)* znajdują się instrukcje wzmacniania zabezpieczeń (np. *AXIS OS Hardening Guide*, *AXIS Camera Station System Hardening Guide* i *Axis Network Switches Hardening Guide*), dokumentacja zasad i inne materiały pomocnicze. Ponadto firma Axis oferuje *kursy e-learning* z zakresu cyberbezpieczeństwa.

Gdzie można znaleźć najnowszy system operacyjny do urządzenia?

Otwórz menu *device software (Oprogramowanie urządzenia)* i wyszukaj swój produkt.

Jak łatwo zaktualizować system operacyjny w urządzeniu?

Aby zaktualizować oprogramowanie urządzenia, można użyć oprogramowania do zarządzania zawartością wideo firmy Axis, takiego jak *AXIS Companion* lub *AXIS Camera Station*, albo narzędzi takich jak *AXIS Device Manager* czy *AXIS Device Manager Extend*.

Jak mogę dowiedzieć się o zakłóceniach w funkcjonowaniu usług Axis?

Odwiedź stronę *status.axis.com*.

Jak mogę otrzymać powiadomienie o odkrytej luce?

Możesz subskrybować *Usługę powiadomień o bezpieczeństwie Axis*.

Jak Axis zarządza lukami w zabezpieczeniach?

Zobacz: *Polityka AXIS zarządzania podatnością na ataki*.

Jak Axis minimalizuje luki w oprogramowaniu?

Przeczytaj artykuł *Integracja cyberbezpieczeństwa w procesie tworzenia oprogramowania Axis*.

Jak Axis wspomaga cyberbezpieczeństwo w całym cyklu życia urządzeń?

Przeczytaj informacje na stronie *A lifecycle approach to cybersecurity (Cyberbezpieczeństwo w całym cyklu życia)*.

Jakie funkcje cyberbezpieczeństwa są wbudowane w produkty Axis?

Więcej informacji:

- *Moduł Axis Edge*
- *AXIS OS*
- *Wspomaganie cyberbezpieczeństwa w całym cyklu życia urządzeń*

Pytania i odpowiedzi dotyczące cyberbezpieczeństwa

Pytania dotyczące rozwiązań Axis

Czy Axis posiada certyfikat ISO? Zgodność z jakimi innymi przepisami zapewnia Axis?

Odwiedź stronę internetową dotyczącą *Zgodności*.

W jaki sposób Axis ułatwia mojej firmie zachowanie zgodności z dyrektywą NIS 2?

Przeczytaj artykuł na temat dyrektywy *NIS 2* (pdf).

Podręcznik użytkownika
Pytania i odpowiedzi dotyczące cyberbezpieczeństwa

Wer. M4.2
Data: Lipiec 2024
Numer części T10189380