AXIS Camera Station Pro

사용자 설명서

서론

모든 보안 시스템과 사이트를 100% 사이버 보안으로 만들 수 있는 완벽한 기능입니다. 이 말은 매력적이기는 하지만 이러한 기능은 존재하지 않습니다. 또는 곧 존재할 가능성이 높습니다. 대신, 조직 고유의 위협과 취약성으로 인해 발생할 수 있는 위험을 조사하고 위험이 용납할 수 없는 것으로 판단되면 해당 위험을 완화하기 위한 제어 기능을 구현해야 합니다. 잘 정의된 정책과 절차는 조직 전반에 걸쳐 이러한 제어 수단의 일관된 의사 소통과 적용을 보장하고 성숙한 사이버 보안 프로그램의 기초를 형성합니다.

권장되는 액세스 방식은 ISO 27001, NIST CSF 등과 같은 표준화된 IT 보안 위험 관리 프레임워크에 따라 작업하는 것입니다. 소규모 조직에서는 이 작업이 어려울 수 있지만 기본적인 정보 보안 정책과 지원 프로세스를 정의하는 것이 전혀 없는 것보다 훨씬 낫습니다. 조직에서 사이버 성숙도 향상을 위한 여정을 시작하고 있으며 사용 가능한 리소스가 제한적인 경우 *인터넷 안전 센터(CIS) 중요 보안 제어 버전 8(Center for Internet Safety (CIS) Critical Security Controls Version 8)*을 검토하는 것이 좋습니다. CIS는 조직이 사이버 보안 프로그램을 개발하고 발전시키는 데 도움이 되도록 세 가지 구현 그룹으로 구성된 18가지 보안 제어 활동 목록을 제공합니다.

많은 조직에서 보안 침해가 발생하는 이유는 회사가 직원의 사용 및 접근 권한을 관리하는 명확한 정책, 룰 및 절차를 확립하지 않았기 때문입니다. 귀하의 조직은 영상 관리 작업을 위한 정책 및 프로세스를 사용하고 있나요? 그렇지 않은 경우 정의를 시작해야 합니다.

목적

이 문서에서는 AXIS Camera Station Pro 시스템의 보안 배포 및 유지보수를 지원하는 데 유용한 다양한 사이버 보안 정책 및 절차에 대해 설명합니다. 사이버 보안 프레임워크에 직접 매핑되지는 않지만 주로 다음 제어 활동에 중점을 두고 CIS 보안 제어 v8을 활용합니다.

- *컨트롤 1: 엔터프라이즈 자산의 재고 및 제어*
- *컨트롤 2: 소프트웨어 자산의 재고 및 제어*
- *컨트롤 3: 데이터 보호*
- *컨트롤 4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성*
- *컨트롤 5: 계정 관리*
- *컨트롤 6: 접근 제어 관리*
- *컨트롤 7: 지속적인 취약점 관리*
- *컨트롤 10: 멀웨어 방어*

권장 사항은 설치 관리자, 통합자 및 최종 사용자가 AXIS Camera Station Pro 시스템을 배포하고 관리할 때 일반적인 위험을 완화하도록 지원하는 데 중점을 둡니다.

전제 조건

*AXIS OS 강화 가이드*에 정의 및 설명된 권장 사항과 절차를 이해하고 준수한다고 가정합니다. 또한 이 문서에서는 영상 시스템과 상호 작용하는 몇 가지 일반적인 사용자 역할을 설명합니다. 이러한 사용자 역할을 자신의 사용자 및 역할 분류에 맞게 매핑하십시오. 개별 사용자는 조직에 따라 여러 역할을 가질 수 있습니다.

정의된 역할:

- **시스템 설치자**: 시스템을 설치, 설정, 수리, 업그레이드 및 다운그레이드합니다.
- **네트워크 관리자**: 네트워크 인프라, 엔드 노드 연결, 네트워크 서버 및 리소스, 네트워크 보호를 유지합니다.
- **비디오 시스템 관리자**: 영상 시스템의 사용, 성능, 사용자 권한을 보호하기 위해 영상 시스템을 정의하고 관리합니다.
- **비디오 시스템 유지관리자**: 영상 시스템 관리자를 대신하여 시스템 성능을 보호하기 위해 구성 요소를 모니터링, 조정 및 문제 해결합니다.

- **사용자**: AXIS Camera Station Pro 클라이언트를 사용하여 실시간 및 녹화된 영상에 접근하고 일반적으로 조직의 물리적 보호를 담당하는 개인입니다.

시스템 보안 정책

물리적 보안

물리적 보호 정책

서버, 장치, 네트워크 장비 및 케이블은 방해를 받거나 파괴되거나 도난을 당할 수 있는 물리적 객체입니다. AXIS Camera Station Pro 서버 소프트웨어와 중요한 네트워크 장비(라우터, 스위치 등)를 실행하는 호스트는 물리적 및 논리적으로 접근이 제한된 환경에 배치되어야 합니다. 카메라 및 기타 연결된 장치는 접근하기 어려운 곳에 장착해야 하며 파손 방지 모델 또는 케이스를 갖추고 있어야 합니다. 벽이나 전선관의 케이블은 변조 및 파괴될 위험이 높으므로 이를 보호하는 데 주의를 기울여야 합니다.

권장 정책 및 절차
VMS 서버, 네트워크 하드웨어, 연결된 장치 및 케이블 연결에 대한 물리적 보호를 정의된 간격에 시각적으로 감사할 책임이 있는 개인 또는 조직 단위를 정의합니다. 위치를 포함한 모든 서버 및 장치의 정확한 인벤토리를 유지하는 것이 필수적입니다.

소프트웨어 관리

타사 애플리케이션 소프트웨어 정책

AXIS Camera Station Pro는 표준 Windows 환경에 설치되므로 영상 관리와 관련되지 않은 소프트웨어 애플리케이션에 해당 환경을 활용하고 싶은 유혹을 느낄 수 있습니다. 다른 타사 애플리케이션을 설치하면 환경에 맬웨어가 유입되어 시스템 가동 중지 시간이 발생하거나 공격자가 조직의 네트워크에 침입할 수 있는 백도어를 제공할 가능성이 열립니다.

권장 정책 및 절차
호스트 하드웨어에서 AXIS Camera Station Pro 서버 소프트웨어 및 신뢰할 수 있는 타사 통합 이외의 다른 것을 실행하지 마십시오. 물리적 하드웨어를 다른 목적으로 활용해야 하는 경우 여러 가상 서버 인스턴스를 사용하고 한 가상 머신에서는 AXIS Camera Station Pro 서버 소프트웨어를 실행하고 다른 가상 머신에서는 타사 비 VMS 관련 소프트웨어를 실행하는 것이 좋습니다. 가상 환경에서 AXIS Camera Station Pro를 실행하는 방법에 대한 정보는 *여기*에서 확인할 수 있습니다.

AXIS Camera Station Pro 서버에 연결되는 모든 서버와 컴퓨터에 바이러스 백신 소프트웨어를 배포하는 것이 좋습니다. 모바일 장치를 배포하는 경우 장치에 최신 운영 체제와 패치(직접적인 바이러스 백신은 아님)가 설치되어 있는지 확인하는 작업이 포함됩니다. 바이러스 검사를 수행할 때 녹화 데이터베이스가 포함된 디렉터리 및 하위 디렉터리를 검사하지 마십시오. 이러한 디렉터리에서 바이러스를 검사하면 시스템 성능에 영향을 줄 수 있습니다.

계정 관리

일반 계정 정책

편의를 위해 일반 사용자에게 관리자 수준 권한을 부여하는 경우도 있습니다. 많은 조직에서는 계정 권한을 검토하고 직원의 시스템 액세스를 모니터링하는 책임이 누구에게 있는지 명확하지 않습니다.

권장 정책 및 절차
조직에서는 시스템 계정을 정의할 때 최소 권한의 원칙을 따르는 것이 좋습니다. 즉, 사용자 접근 권한은 특정 작업 수행에 필요한 리소스로만 제한됩니다. 또한 "권한 변동"을 방지하기 위해 시스템 사용자의 계정 권한을 정기적으로 감사하는 것이 좋습니다.

AXIS Camera Station Pro 관리자 계정 정책

Windows 환경에서 AXIS Camera Station Pro를 배포할 때 흔히 저지르는 실수는 Windows 호스트에 대해 단일 관리자 계정이 정의된다는 것입니다. 시간이 지남에 따라 조직 내에서 패스워드가 공유될 수 있으며 권한이 없는 개인이 Windows 환경에 대한 관리자 권한을 얻을 위험이 있습니다. 이로 인해 해당 서버에 원치 않는 수많은 사용자 애플리케이션이나 맬웨어가 쉽게 설치될 수 있습니다.

권장 정책 및 절차

AXIS Camera Station Pro 서버를 호스팅하는 Windows 시스템에는 관리자 권한 계정과 사용자 권한 계정이 각각 하나씩 있어야 합니다. 이 두 계정 모두 Windows의 기본 관리자 계정과 동일하지 않아야 합니다. 관리자 및 사용자 권한 계정을 생성한 후에는 기본 관리자 계정을 비활성화해야 합니다. 배포 후 관리자 계정 패스워드는 **네트워크 관리자**만 알고 사용해야 합니다. 사용자 권한 계정은 **영상 시스템 관리자**가 AXIS Camera Station Pro 서버에 로그인해야 하는 경우 사용해야 합니다. 위의 두 가지 역할을 동일한 개인이 수행하더라도 감사 목적으로 별도의 네트워크 및 영상 시스템 관리자 계정을 보유하는 것이 여전히 권장됩니다. 이전에 정의된 다른 역할을 지원하려면 시스템에 로그인할 각 개별 **사용자**에 대해 권한이 없는 사용자 계정을 추가로 생성해야 합니다.

AXIS Camera Station Pro를 실행하는 호스트가 Windows Active Directory 도메인 환경에 배치된 경우 도메인 컨텍스트에서 관리자 및 사용자 계정을 생성하거나 직원의 기존 도메인 계정을 사용하여 AXIS Camera Station Pro 호스트를 인증할 수 있습니다. 이를 통해 추가 계정을 생성하고 유지할 필요가 없으므로 계정 관리가 단순화될 수 있습니다. 이는 또한 그룹 정책 관리를 사용하여 패스워드 복잡성, 인증서 배포 및 도메인 환경에서 사용할 수 있는 기타 보안 기능을 적용할 수 있습니다.

AXIS Camera Station Pro 사용자 계정 정책

사용자 계정은 AXIS Camera Station Pro의 특정 역할에 할당되며, 이에 따라 각 사용자가 시스템에서 갖는 특정 권한(예: 접근 권한이 있는 보기 및 영상)이 결정됩니다. 여러 개인이 단일 사용자 계정을 공유하는 경우 조직 내 다른 사람과 패스워드가 공유될 위험이 높아집니다. 계정을 공유하면 누가 언제 어떤 카메라/영상에 접근했는지 감사하는 것이 사실상 불가능해집니다.

권장 정책 및 절차

Kerberos를 사용하여 AXIS Camera Station Pro 클라이언트 사용자를 인증하는 것이 좋습니다. 항목을 참조하십시오.

가능하다면 쉬운 사용자 및 그룹 관리를 위해 Microsoft Active Directory를 사용하십시오. 또한 시스템을 설정하기 전에 모든 사용자 역할에 대해 관련 보안 그룹이 정의되었는지 확인하는 것이 좋습니다.

Active Directory는 또한 다음을 제공합니다.

- 패스워드 정책 - 사용자가 정기적으로 패스워드를 변경하도록 요구함
- 무차별 대입 보호 - 조직 패스워드 정책에 따라 여러 번의 인증 시도를 실패한 후에는 Windows AD 계정을 차단함
- 역할 기반 권한 - 도메인 전반에 걸쳐 접근 제어를 적용할 수 있음

로컬 Windows 계정을 사용해야 하는 경우 시스템의 각 사용자에 대해 고유한 계정을 생성하고 해당 사용자에게 책임을 수행하는 데 필요한 시스템 내 엔터티에만 접근할 수 있는 권한을 부여하는 것이 좋습니다. 사용자 그룹을 활용하면 동일한 권한을 가진 사용자가 여러 명 있는 경우 권한 할당을 단순화하는 데 도움이 될 수 있습니다.

Kerberos를 사용하여 인증하기

AXIS Camera Station Pro는 통합 Windows 인증을 사용하여 AXIS Camera Station Pro 클라이언트의 사용자를 인증합니다. AXIS Camera Station Pro는 SPNEGO(Microsoft Negotiate 프로토콜)를 사용하며, 이는 Kerberos가 선호되는 기본 인증 프로토콜임을 의미합니다. Negotiate 프로토콜은 Kerberos 사용을 시도하고 NTLM을 대체 수단으로 사용합니다.

Kerberos를 사용하려면 다음 명령을 사용하여 Active Directory에 SPN(Service Principal Name)을 등록해야 합니다.

```
setspn -s ACSService/{HOST} {ACCOUNT_NAME}
```

HOST - AXIS Camera Station Pro 서버를 실행하는 서버의 호스트 이름입니다.

ACCOUNT_NAME - AXIS Camera Station Pro 서버를 실행하는 컴퓨터(컴퓨터 계정)의 이름입니다.

Kerberos가 제대로 작동하려면 대상 AXIS Camera Station Pro 서버에 대해 짧은 호스트 이름과 FQDN을 모두 등록하는 것이 좋습니다.

예:

```
setspn -s ACSService/CompanyServer CompanyServerAccount setspn -s ACSService/CompanyServer.
domain.local CompanyServerAccount
```

자세한 내용은 *microsoft.com의 Setspn*을 참조하십시오.

장치 계정 정책

Axis 장치의 계정은 주로 컴퓨터/클라이언트 계정입니다. **사용자**가 장치에 직접 접근하도록 허용해서는 안 됩니다. 정상 작동 중에 장치에 접근해야 하는 유일한 클라이언트는 AXIS Camera Station Pro 서버입니다. 일반적인 전략은 모든 장치가 동일한 패스워드를 갖는 것입니다. 이로 인해 추가적인 위험이 발생하지만 패스워드 관리가 단순화되므로 자체 위험 허용 범위를 평가해야 합니다. AXIS Camera Station Pro는 관리 인터페이스를 통해 각 장치에 고유한 패스워드를 할당할 수 있도록 지원합니다.

흔히 저지르는 실수는 여러 역할이 공유하는 단일 계정으로 장치가 AXIS Camera Station Pro에 추가된다는 것입니다. 어느 시점에서 **영상 시스템 유지보수 관리자**가 브라우저를 사용하여 무언가를 조정해야 할 때 장치의 마스터 계정(root) 패스워드가 공개됩니다. 몇 달 안에 조직의 대부분의 사람들은 모든 장치의 패스워드를 알게 되고 시스템에 대한 관리자 권한을 갖게 됩니다.

권장 정책 및 절차
장치에는 장치 관리자용으로 생성된 고유 계정과 AXIS Camera Station Pro 서버에 장치를 추가하기 위한 기본 root 계정 등 최소 두 개의 관리자 계정이 있어야 합니다. **영상 시스템 유지보수 관리자**가 웹 브라우저를 사용하여 장치에 접근하는 경우와 같은 임시 접근 권한은 임시 계정을 사용하여 관리해야 합니다.

AXIS Device Manager는 장치 계정 및 패스워드를 관리하기 위한 기본 도구로 사용해야 합니다. AXIS Device Manager 버전은 AXIS Camera Station Pro에 직접 내장되어 있으며 관리 탭에서 사용할 수 있습니다. 장치의 root 패스워드는 AXIS Device Manager 및 AXIS Camera Station Pro에서만 사용해야 하며 AXIS Device Manager 또는 AXIS Camera Station Pro를 장치 관리 도구로 사용하는 사용자에게만 알려야 합니다.

유지보수 관리자 역할을 맡은 사람이 문제 해결이나 유지보수를 위해 웹 브라우저를 사용하여 장치에 접근해야 하는 경우 AXIS Camera Station Pro를 사용하여 임시 계정을 프로비저닝합니다. 장치를 선택하고 유지보수 관리자가 사용할 수 있는 운영자 권한이 있는 새 계정을 생성합니다. 작업이 완료되면 임시 계정을 제거합니다.

시스템 유지보수

AXIS Camera Station Pro Windows 호스트 패치 적용 정책

AXIS Camera Station Pro 서버와 클라이언트는 Windows 환경 위에서 실행됩니다. AXIS Camera Station Pro 소프트웨어를 호스팅하는 시스템에 영상 관리 시스템에 대한 무단 액세스를 얻기 위해 악용될 수 있는 공개 취약성이 없는지 확인하기 위해 이러한 시스템을 최신 상태로 유지하는 것이 중요합니다.

권장 정책 및 절차
Axis NVR 또는 사용자 정의 하드웨어에서 실행되는 모든 AXIS Camera Station Pro 시스템의 경우 자동 업데이트를 끄는 것이 좋습니다. 과거에는 Windows 업데이트로 인해 기본 Windows OS가 불안정해졌으므로 사용 가능한 업데이트를 AXIS Camera Station Pro를 실행하는 모든 호스트 시스템에 푸시하기 전에 일부 시스템에서 테스트하여 시스템의 안정성을 확인하는 것이 좋습니다. 그러나 Windows 시스템을 패치하지 않은 상태로 너무 오랫동안 방치하면 전체 환경에 위험이 발생할 수 있으므로 보안과 안정성 간의 균형을 유지해야 합니다. 외부 위협에 대한 고객 시스템의 노출 수준에 따라 시스템이 최신 업데이트를 받을 수 있도록 보장하는 기간을 패치 적용 정책에 명시해야 합니다.

AXIS Camera Station Pro 소프트웨어 업데이트 정책

대부분의 경우 AXIS Camera Station Pro용 최신 소프트웨어 릴리스를 사용하면 새로 발견된 모든 취약성에 대해 보안 패치를 활용할 수 있습니다. 시스템을 패치하지 않은 상태로 장기간 방치하면 공격자가 취약성을 악용하여 시스템, 애플리케이션 또는 장치를 손상시킬 위험이 높아집니다.

권장 정책 및 절차

AXIS Camera Station Pro을(를) 최신 상태로 유지하기 위해서 배포된 소프트웨어 버전을 정기적으로 평가하여 패치 적용 정책을 정의하는 것이 중요합니다. 또한 패치 적용 정책은 서버 및 클라이언트 소프트웨어 업데이트와 관련된 작업을 관리할 책임이 있는 사람을 식별해야 합니다. AXIS Camera Station Pro의 최신 릴리스는 *www.axis.com*에서 확인할 수 있습니다. AXIS Camera Station Pro에는 최신 .NET 라이브러리가 필요하므로 Windows 패치 정책을 AXIS Camera Station Pro 정책에 맞게 조정해야 합니다.

장치 펌웨어 업데이트 정책

최신 펌웨어 버전으로 장치를 실행하면 가장 일반적인 위험이 완화됩니다. 최신 펌웨어 버전에는 공격자가 악용하려고 시도할 수 있는 알려진 취약성에 대한 패치가 포함되어 있기 때문입니다. Axis는 보안 패치 및 버그 수정이 포함된 장치 펌웨어에 대한 LTS(장기 지원) 릴리스를 제공하지만 플랫폼의 장기적인 안정성을 보장하기 위해 기능 추가가 제한됩니다. 펌웨어 개발에 관한 Axis 전략에 대한 자세한 내용 *Axis 펌웨어 관리* 백서를 참조하십시오.

권장 정책 및 절차
하드웨어 장치의 경우 모든 펌웨어가 최신 상태로 유지되도록 정책에 명시해야 합니다. 프로세스는 AXIS Camera Station Pro 또는 AXIS Device Manager Extend에 내장된 펌웨어 업데이트 기능을 활용하여 Axis 장치에 사용할 수 있는 새 펌웨어 버전이 있는지 확인할 수 있습니다. 모든 카메라의 모든 펌웨어 업그레이드를 배포하기 위한 예정 시간(일반적으로 업무 시간 외)을 정의해야 합니다. AXIS Camera Station Pro / AXIS Device Manager Extend도 펌웨어 업데이트가 수락되었는지 확인할 수 있습니다. 시스템에 업데이트의 영향을 받을 수 있는 특정 통합이 있는 경우 LTS 펌웨어 트랙의 표준화하는 것을 고려하십시오.

네트워크 보안

원격 액세스 정책

인터넷에 노출된 장치 및 서비스는 외부 공격자가 알려진 취약성을 조사하거나 악용할 위험을 높입니다. 예를 들어, 원격 비디오 액세스가 필요한 소규모 조직에서 인터넷에 노출된 카메라는 취약한 패스워드가 사용되거나 새로운 치명적인 취약성이 발견되면 쉽게 피해자가 됩니다. Windows 환경에 대한 원격 액세스는 엄격하게 제어하거나 가능한 한 피해야 합니다. Windows 환경에는 시스템 업데이트의 편의를 위해 인터넷 연결이 가능할 수 있지만 Windows 원격 데스크톱, TeamViewer 및 AnyDesk와 같은 원격 데스크톱 서비스를 활용하면 올바르게 관리되지 않을 경우 시스템에 액세스할 수 있는 경로가 제공됩니다.

권장 정책 및 절차
카메라의 IP 주소/포트를 인터넷에서 직접 액세스할 수 있는 방식으로 노출하지 마십시오. 원격 비디오 액세스가 필요한 경우 AXIS Secure Remote Access를 사용합니다. AXIS Camera Station Pro는 클라우드 기반 원격 액세스 서버를 사용하여 AXIS Camera Station Pro 클라이언트 또는 AXIS Camera Station 모바일 애플리케이션을 통해 시스템에 대한 암호화된 원격 액세스를 용이하게 합니다. 원격 액세스 서버는 원격 및 모바일 사용자의 연결 관리를 담당하는 것 외에도 원격 사용자가 사용할 때 무결성을 보호하는 데 중요한 역할을 합니다. AXIS Secure Remote Access에 대한 자세한 내용은 *여기*에서 확인할 수 있습니다. Axis는 Android 및 Apple iOS 모두에 대해 공식 브랜드 모바일 애플리케이션을 제공합니다. AXIS Camera Station 모바일 앱은 공식 출처인 Google Play 스토어와 Apple App 스토어에서만 다운로드해야 합니다.

Windows 환경에 대한 원격 데스크톱 액세스의 경우 AXIS Camera Station Pro를 실행하는 시스템에 이러한 유형의 액세스를 제공하는 것은 권장되지 않습니다. 그러나 필요한 경우 선택한 원격 데스크톱 애플리케이션의 보안을 보장하고 접근 권한을 필요로 하는 개인에게만 제공되도록 세심한 주의를 기울여야 합니다. 다단계 인증(MFA)과 같은 추가 제어 계층을 구현하는 것이 좋습니다. 원격 연결 시도에 대한 로깅 및 후속 감사를 위해 누가, 언제 Windows 환경에 원격으로 액세스하는지 추적할 것을 강력히 권장합니다.

로컬 네트워크 노출 정책

로컬 네트워크 노출을 줄이면 공격 표면을 줄여 많은 일반적인 위협을 완화하는 데 도움이 될 수 있습니다. 네트워크 노출을 줄이는 방법에는 물리적 네트워크 분할(별도의 네트워크 하드웨어 및 케이블), 가상 LAN(VLAN)을 통한 논리적 네트워크 분할, IP 필터링 등이 있습니다. Axis 카메라는 장치가 명시적으로 허용된 IP 주소에서 이루어진 연결 요청에만 응답하도록 IP 필터(IP 테이블)를 지원합니다.

권장 정책 및 절차

AXIS Camera Station S22 NVR은 듀얼 네트워크 포트가 있는 하드웨어 서버입니다. 포트 중 하나는 카메라를 위한 분할된 네트워크를 생성하고 다른 하나는 기본 네트워크(도메인)에 연결하여 비디오 클라이언트를 제공합니다. 서버는 카메라 네트워크에 대한 브리지 및 방화벽 역할을 하여 클라이언트가 카메라에 직접 액세스하는 것을 방지합니다. 이렇게 하면 기본 네트워크에서 공격자의 위협이 발생할 가능성이 줄어듭니다.

AXIS Camera Station Pro 서버와 카메라가 모두 기본 네트워크에 배치된 경우 카메라의 IP 필터를 구성하여 AXIS Camera Station Pro를 호스팅하는 서버, AXIS Device Manager 및 추가 유지보수 클라이언트에만 액세스하도록 제한하는 것이 좋습니다.

추가 애플리케이션 및 서비스

AXIS Camera Station Pro 서버에서 로컬 호스트(서버 자체)에 국한되도록 의도된 추가 애플리케이션을 호스팅하는 경우, 관리자가 클라이언트를 통해 원격으로 해당 애플리케이션에 액세스할 수도 있음을 유의하십시오. 이는 의도치 않게 해당 애플리케이션을 노출시킬 수 있습니다.

동일한 위험이 네트워크에서 실행 중인 다른 모든 서비스에도 적용됩니다. 위험을 줄이기 위해, AXIS Camera Station Pro 및 해당 카메라를 호스팅하는 네트워크와 관련 없는 애플리케이션이나 서비스를 호스팅하는 다른 네트워크 사이에 방화벽을 설치할 것을 권장합니다. 이러한 망 분리는 잠재적 침해 가능성을 억제하고 불필요한 액세스 경로를 제한하는 데 도움이 됩니다.

네트워크 암호화 정책

안전하지 않은 네트워크를 통해 전송되는 네트워크 트래픽은 항상 암호화되어야 합니다. 인터넷은 안전하지 않은 네트워크로 분류됩니다. 로컬 네트워크도 안전하지 않은 것으로 분류될 수 있으므로 네트워크 트래픽도 암호화되어야 합니다. 네트워크의 영상 트래픽에 적용할 정책은 영상이 분류되는 방식과 공격자가 네트워크에서 영상 시스템에 접근할 수 있는 위험에 따라 달라집니다. 네트워크는 이미 손상되었다고 가정하는 것이 좋습니다. 대규모 조직에는 일반적으로 네트워크 분류 방법을 정의하는 정책이 있습니다.

권장 정책 및 절차

비디오 클라이언트와 AXIS Camera Station Pro 서버 간의 트래픽은 암호화를 사용해야 합니다. AXIS Camera Station Pro 서버와 카메라 간의 트래픽은 인프라에 따라 암호화되어야 합니다. Axis 카메라에는 기본적으로 활성화된 자체 서명 인증서와 HTTPS가 함께 제공됩니다. 악의적인 컴퓨터가 카메라를 가장하려고 시도하는 경우와 같이 네트워크 스푸핑의 위험이 있는 경우 CA 서명 인증서가 있는 PKI(개인 키 인프라)를 사용해야 합니다. AXIS Camera Station Pro에는 Axis 장치의 서버 인증서 서명 및 배포를 비용 효율적으로 관리할 수 있는 로컬 CA(인증 기관)가 내장되어 있습니다.

TLS 버전

TLS 버전 1.1 및 1.0을 비활성화하는 것이 좋습니다. AXIS Camera Station 설치 프로그램은 설치 또는 업그레이드 중에 지원을 제공합니다.

HTTPS 암호

AXIS Camera Station Pro 는 TLS 암호화 제품군을 지원하고 사용하여 HTTPS 연결을 안전하게 암호화합니다. 특정 암호화 제품군은 AXIS Camera Station Pro에 연결하는 클라이언트 또는 연결된 서비스에 따라 다르며, AXIS Camera Station Pro는 TLS 프로토콜에 따라 이를 협상합니다. *RFC 7540에* 나열된 TLS 1.2 암호 제품군을 사용하지 않도록 Windows를 구성하는 것이 좋습니다. 암호 제품군 비활성화 기능은 AXIS Camera Station Pro와(과) 함께 사용되는 장치 및 카메라에 따라 다릅니다. 장치나 카메라에 특정 암호화 제품군이 필요한 경우 약한 암호화 제품군을 비활성화하지 못할 수도 있습니다.

데이터 관리

설치

AXIS Camera Station Pro는 표준 프로그램 파일 디렉토리 외부의 폴더에 설치할 수 있습니다. 하지만 이는 덜 엄격한 접근 제어를 초래하여 잠재적인 보안 위험을 초래할 수 있습니다. 기본 설치 경로를 사용하거나 선택한 폴더의 액세스 권한을 확인할 것을 권장합니다.

영상 분류

실시간 및 녹화된 영상으로 분류되어야 합니다. 영상은 공개, 비공개, 제한 또는 조직 정책에 정의된 기타 등급으로 분류될 수 있습니다. 대부분의 경우 영상은 내부 IT 정책은 물론 법률 및 지역 규정에 의해 규제되므로 영상 데이터에 적용되는 법률 및 규정을 숙지하는 것은 시스템 소유자의 책임입니다.

권장 정책 및 절차
조직의 데이터 분류 정책에 따라 실시간 영상, 녹화된 영상, 오디오를 분류합니다. 비디오 및 오디오 데이터의 민감도에 따라 사용자 접근 권한 및 시스템 강화를 구성합니다. 필요하지 않은 경우 장치 수준에서 오디오가 비활성화될 수 있습니다.

추가 보안 제어 기능

조직의 성숙도 수준과 위험 허용 범위에 따라 일상적인 운영에서 사이버 보안 위험을 줄이는 데 도움이 되도록 구현하는 것이 권장되는 CIS 제어 v8의 몇 가지 추가 보안 제어 기능이 있습니다.

추가 CIS 제어:

컨트롤 8: 감사 로그 관리
공격을 감지, 이해 또는 복구하는 데 도움이 될 수 있는 이벤트의 감사 로그를 수집, 경고, 검토 및 보관합니다.

컨트롤 14: 보안 인식 및 교육 프로그램 실시
직원들의 기술과 행동을 이해합니다. 다양한 형태의 공격을 식별하는 방법을 직원에게 교육합니다.

컨트롤 17: 사고 대응 및 관리
사고 처리/관리 단계와 직원 역할이 명확하게 정의된 서면 사고 대응 계획과 보안 사고를 관련 기관 및 제3자에게 보고하는 방법을 활용합니다.

데이터베이스 백업 보안

데이터베이스 백업 위치를 변경하는 경우 접근이 제한된 안전한 위치를 사용합니다. 접근 권한이 넓은 네트워크 공유는 보안이 취약합니다.

DbConsole

DbConsole은 AXIS Camera Station Pro가 실행되지 않는 동안 데이터베이스 백업 및 복원을 수행할 수 있는 명령줄 도구입니다. 자세한 내용은 *수동 백업* 및 *데이터베이스 복구*를 참조하십시오.

- 프로세스 목록 및 셸 기록에 표시될 수 있으므로 패스워드를 도구의 매개변수로 제공하지 마십시오. 대신 관리자 권한이 있는 사용자로 도구를 실행하거나 프롬프트가 표시될 때 패스워드를 제공합니다.
- 백업 명령을 실행할 때 출력물의 안전한 위치를 지정합니다.
- 복원 명령을 실행할 때 신뢰할 수 있는 소스의 백업 파일만 사용합니다. 악성 백업 파일을 복원하면 시스템 보안이 침해될 수 있습니다.

T10203603_ko

2025-11 (M3.2)

© 2024 – 2025 Axis Communications AB