사이버 보안 Q&A

사용자 설명서

다른 질문과 답변을 보려면 Axis *FAQ 데이터베이스*를 방문하십시오.

일반적인 질문들

사이버 보안이란?

사이버 보안은 사이버 위협으로부터 컴퓨터 시스템과 서비스를 보호하는 것입니다. 사이버 보안 관행에는 가용성, 무결성, 안전, 진정성, 기밀성 및 부인 방지를 보장하기 위해 컴퓨터, 전자 통신 시스템 및 서비스, 유선 및 전자 통신, 저장된 정보의 손상을 방지하고 복원하는 프로세스가 포함됩니다.

사이버 보안은 장기간에 걸쳐 위험을 관리하는 것입니다. 위험은 결코 제거할 수 없으며 완화될 뿐입니다.

일반적으로 사이버 보안 관리와 관련된 것은 무엇입니까?

사이버 보안은 제품, 사람, 기술 및 지속적인 프로세스에 관한 것입니다.

따라서 장치, 시스템, 소프트웨어 및 펌웨어 인벤토리 수행을 포함하여 조직의 다양한 측면을 **식별** 및 평가하고, 미션 크리티컬 목표 설정; 절차 및 보안 정책 문서화 위험 관리 전략을 적용하고 자산과 관련된 위험 평가를 지속적으로 수행합니다.

여기에는 사이버 공격에 대한 우선 순위로 식별한 데이터, 장치, 시스템 및 시설을 **보호**하기 위한 보안 제어 및 조치를 구현하는 것이 포함됩니다.

또한 적시에 조치를 취할 수 있도록 사이버 공격을 **감지**하는 데 도움이 되는 활동을 개발하고 구현하는 작업도 포함됩니다. 예를 들어, 여기에는 SIEM(Security Information and Event Management) 시스템이나 SOAR(Security Orchestration, Automation and Response) 시스템이 포함될 수 있습니다. 해당 데이터를 분석하여 실시간 알림을 제공합니다. Axis 장치는 SIEM 또는 SOAR 시스템의 기본 데이터 소스인 SYS 로그 및 원격 SYS 로그를 지원합니다.

사이버 보안 관리에는 사이버 보안 사고가 감지되면 **대응**하는 절차를 개발하고 구현하는 것도 포함됩니다. 현지 규정 및 내부 정책과 사이버 보안 사고 공개 요구 사항을 고려해야 합니다. Axis는 *AXIS OS Forensic Guide*를 제공하여 Axis 장치가 사이버 보안 공격 중에 손상되었는지 이해하는 데 도움을 줍니다.

복원력 계획을 유지하고 **복구**하거나 사이버 보안 사고로 인해 손상된 기능이나 서비스를 복원하기 위한 활동을 개발하고 구현하는 것 또한 중요합니다. 예를 들어 *Axis 장치 관리 애플리케이션*은 특정 시점의 시스템 구성이 저장된 "스냅샷"인 복원 지점을 지원하여 Axis 장치를 쉽게 복원할 수 있도록 합니다. 관련 복원 지점이 없는 경우 이 도구는 모든 장치를 기본 상태로 되돌리고 저장된 구성 템플릿을 네트워크를 통해 푸시하는 데 도움이 될 수 있습니다.

사이버 보안 위험은 무엇입니까?

사이버 보안 위험(RFC 4949 Internet Security Glossary에 정의됨)은 특정 위협이 특정한 유해 결과로 특정 취약점을 악용할 가능성으로 표현되는 예상 손실입니다.

장기적으로 적절한 위험 감소를 달성하려면 명확한 시스템 정책과 프로세스를 정의하는 것이 중요합니다. 권장되는 접근 방식은 ISO 27001, NIST 또는 이와 유사한 것과 같이 잘 정의된 IT 보호 프레임워크에 따라 작업하는 것입니다. 소규모 조직에는 이 작업이 부담스러울 수 있지만, 최소한의 정책 및 프로세스 문서를 작성하기만 해도 아무 것도 하지 않는 것보다 훨씬 도움이 될 것입니다.

위험을 평가하고 우선 순위를 지정하는 방법에 대한 정보는 *사이버 보안 참조 가이드*를 참조하세요.

위협은 무엇입니까?

위협은 자산이나 리소스를 손상시키거나 해를 입힐 수 있는 모든 것으로 정의할 수 있습니다. 일반적으로 사람들은 사이버 위협을 악의적인 해커 및 맬웨어와 연관시키는 경향이 있습니다. 실제로 사고, 의도하지 않은 오용 또는 하드웨어 오류로 인해 부정적인 영향이 자주 발생합니다. 공격은 기회주의적 공격 또는 표적 공격으로 분류할 수 있습니다. 오늘날 대부분의 공격은 기회주의적 공격입니다. 즉, 공격할 기회가 생겼기 때문에 발생하는 공격입니다. 이러한 공격은 피싱 및 프로빙과 같은 저비용 공격 벡터를 사용합니다. 표준 보호 수준을 적용하면 기회주의적 공격과 관련된 대부분의 위험을 완화합니다.

특정 목표를 가진 특정 시스템을 대상으로 하는 공격자로부터 보호하기가 더 어렵습니다. 표적 공격은 기회주의적 공격자와 동일한 저비용 공격 벡터를 사용합니다. 그러나 초기 공격이 실패하면 목표를 달성하기 위해 보다 정교한 방법을 사용하기 위해 보다 단호하고 시간과 리소스를 기꺼이 사용합니다. 그들에게 중요한 것은 얼마나 많은 가치가 걸려 있는지에 관한 것입니다.

가장 일반적인 위협은 무엇이며 어떻게 해결할 수 있습니까?

의도적이거나 우발적인 시스템 오용

시스템에 합법적으로 액세스할 수 있는 사람은 모든 시스템에 대한 가장 일반적인 위협 중 하나입니다. 권한이 없는 서비스에 액세스할 수 있습니다. 그들은 시스템을 훔치거나 의도적으로 손상시킬 수 있습니다. 사람도 실수할 수 있습니다. 문제를 해결하려고 하면 실수로 시스템 성능이 저하될 수 있습니다. 개인은 또한 사회 공학, 즉, 합법적인 사용자가 중요한 정보를 누설하도록 만드는 트릭에 취약합니다. 개인은 중요한 구성 요소(출입 카드, 전화, 노트북, 문서 등)를 분실하거나 다른 곳으로 옮길 수 있습니다. 사람들의 컴퓨터가 손상되어 의도치 않게 맬웨어로 시스템을 감염시킬 수 있습니다.

권장되는 보호에는 정의된 사용자 계정 정책 및 프로세스 보유, 충분한 액세스 인증 체계 보유, 시간이 지남에 따라 사용자 계정 및 권한을 관리하는 도구 보유, 노출 감소 및 사이버 인식 교육이 포함됩니다.

Axis는 *보안 강화 가이드*와 장치 및 *비디오 매니지먼트 소프트웨어*를 통해 이러한 위협에 대응하도록 지원합니다.

물리적 변조 및 방해 행위

물리적으로 노출된 장비는 변조, 도난, 분리, 방향 변경 또는 절단될 수 있습니다.

권장되는 보호 조치로는 잠긴 구역에 네트워크 장비(예: 서버 및 스위치) 배치, 손이 닿기 어려운 곳에 카메라 장착, 물리적으로 노출될 때 보호 케이스 사용, 벽이나 도관에서 케이블 보호 등이 있습니다.

Axis는 장치용 *보호 하우징*, 변조 방지 나사, SD 카드를 암호화하는 기능이 있는 카메라, 카메라 뷰 변조 감지 및 열린 포장 감지 기능을 통해 이러한 위협에 대처하는 데 도움이 됩니다.

소프트웨어 취약점 악용

모든 소프트웨어 기반 제품에는 악용될 수 있는 취약점(알려지거나 알려지지 않은)이 있습니다. 대부분의 취약점은 위험이 낮습니다. 즉, 악용하기가 매우 어렵거나 부정적인 영향이 제한적입니다. 때로는 심각한 부정적 영향을 미치는 악용 가능한 취약점이 발견될 수 있습니다. MITRE는 다른 사람들이 리스크를 완화할 수 있도록 방대한 CVE(공통 취약점 및 노출) 데이터베이스를 운영합니다.

권장되는 보호에는 시스템의 알려진 취약점 수를 최소화하는 데 도움이 되는 지속적인 패치 적용 프로세스, 알려진 취약점을 조사하고 악용하기 어렵게 하기 위해 네트워크 노출 최소화, 정책 및 프로세스에 따라 작업하는 신뢰할 수 있는 하도급 공급업체와의 협력이 포함됩니다. 결함을 최소화하고 패치를 제공하며 발견된 치명적인 취약점에 대해 투명하게 공개합니다.

Axis는 Axis 소프트웨어에서 악용 가능한 취약점을 최소화하는 것을 목표로 하는 *Axis 보안 개발 모델*과, 고객이 적절한 조치를 취하기 위해 인지해야 할 취약점을 식별, 수정 및 공지하는 *Axis 취약점 관리 정책*을 통해 위협에 대처합니다. (2021년 4월부로 *Axis는 Axis 제품에 대한 CVE 번호 부여 기관*이 되어 MITRE Corporation의 업계 표준 프로세스에 맞게 프로세스를 조정할 수 있게 되었습니다.) 또한 Axis는 노출을 줄이고 악용 위험을 낮추기 위한 제어 기능을 추가하는 방법에 대한 권장 사항이 포함된 *보안 강화 가이드*를 제공합니다. Axis는 사용자에게 *다양한 장치 소프트웨어 트랙*을 제공하여 Axis 장치의 운영 체제를 최신 상태로 유지하도록 지원합니다. 주요 두 가지 트랙은 다음과 같습니다.

1. 활성 트랙은 새로운 기능과 성능을 지원하는 장치 소프트웨어 업데이트뿐만 아니라 버그 수정 및 보안 패치도 제공합니다.
2. 장기 지원(LTS) 트랙은 버그 수정 및 보안 패치를 지원하는 동시에 타사 시스템과의 비호환성 문제 위험을 최소화하는 장치 소프트웨어 업데이트를 제공합니다.

공급망 공격

공급망 공격은 공급망에서 덜 안전한 요소를 대상으로 조직을 손상시키려는 사이버 공격입니다. 공격은 소프트웨어/운영 체제/제품을 손상시키고 관리자가 이를 시스템에 설치하도록 유인하여 이루어집니다. 시스템 소유자에게 배송하는 동안 제품이 손상될 수 있습니다.

권장되는 보호에는 신뢰할 수 있고 검증된 소스의 소프트웨어만 설치하는 정책, 설치 전에 소프트웨어 체크섬(다이제스트)을 공급업체의 체크섬과 비교하여 소프트웨어 무결성 확인, 변조 징후가 있는지 제품 배송 확인이 포함됩니다.

Axis는 다양한 방법으로 이러한 위협에 대응합니다. Axis는 관리자가 소프트웨어를 설치하기 전에 무결성을 검증할 수 있도록 체크섬이 포함된 소프트웨어를 게시합니다. 새로운 장치 운영 체제(OS)를 불러올 때 Axis 네트워크 장치는 Axis가 서명한 장치 소프트웨어만 수용합니다. Axis 네트워크 장치의 *보안 부팅*은 또한 Axis 서명 OS만 장치를 실행하도록 합니다. 또한 각 장치에는 고유한 Axis 장치 ID가 있어 시스템에서 해당 장치가 정품 Axis 제품인지 확인할 수 있는 방법을 제공합니다. 이러한 사이버 보안 기능에 대한 자세한 내용은 백서 *Axis Edge Vault*에서 확인할 수 있습니다.

위협에 대한 자세한 내용은 Axis의 *사이버 보안 참조 가이드*를 참조하십시오.

취약점이란 무엇입니까?

취약점은 공격자가 시스템을 공격하거나 시스템에 액세스할 수 있는 기회를 제공합니다. 결함, 기능 또는 인적 오류로 인해 발생할 수 있습니다. 악의적인 공격자는 알려진 취약점을 악용하려고 할 수 있으며 종종 하나 이상을 결합합니다. 성공적인 위반 사례의 대부분은 인적 오류, 잘못 구성된 시스템 및 제대로 유지 관리되지 않은 시스템으로 인해 발생합니다. 종종 적절한 정책 부족, 정의되지 않은 책임 및 낮은 조직 인식으로 인해 발생합니다.

소프트웨어 취약점은 무엇입니까?

장치 API(Application Programming Interface) 및 소프트웨어 서비스에는 공격에 악용될 수 있는 결함이나 기능이 있을 수 있습니다. 어떤 공급업체도 제품에 결함이 없다고 보장할 수 없습니다. 결함이 알려진 경우 보안 제어 조치를 통해 위험을 완화할 수 있습니다. 반면에 공격자가 알려지지 않은 새로운 결함을 발견하면 피해자가 시스템을 보호할 시간이 없기 때문에 위험이 증가합니다.

CVSS(Common Vulnerability Scoring System)란 무엇입니까?

Common Vulnerability Scoring System(CVSS)은 소프트웨어 취약성의 심각도를 분류하는 한 가지 방법입니다. 악용이 얼마나 쉬운지, 부정적인 영향이 무엇인지 살펴보는 공식입니다. 점수는 0~10 사이의 값이며 10이 가장 큰 심각도를 나타냅니다. 게시된 CVE(Common Vulnerability and Exposure) 보고서에서 종종 CVSS 번호를 찾을 수 있습니다.

Axis는 CVSS를 소프트웨어/제품에서 식별된 취약성이 얼마나 중요한지 결정하는 측정 방법 중 하나로 사용합니다.

Axis 관련 질문

사이버 보안에 대한 이해를 높이고 사이버 사고로부터 제품 및 서비스를 더 효과적으로 보호하는 데 도움이 되는 교육 및 가이드에는 어떤 것이 있습니까?

리소스 웹 페이지에서 보안 강화 가이드(예: *AXIS OS 보안 강화 가이드*, *AXIS Camera Station Pro 시스템 보안 강화 가이드*, 및 *Axis 네트워크 스위치 보안 강화 가이드*), 정책 문서 등을 이용할 수 있습니다. Axis는 사이버 보안에 대한 *e-러닝* 과정도 제공합니다.

내 장치의 최신 운영 체제는 어디에서 찾을 수 있습니까?

*device software(장치 소프트웨어)*로 이동하여 제품을 검색합니다.

장치의 운영 체제를 어떻게 쉽게 업그레이드할 수 있습니까?

장치 소프트웨어를 업그레이드하려면 *Axis 비디오 또는 장치 관리 소프트웨어*를 사용할 수 있습니다.

Axis 서비스에 중단이 있는 경우 어떻게 알 수 있습니까?

*status.axis.com*를 방문하세요.

발견된 취약점에 대한 알림을 받으려면 어떻게 해야 합니까?

*Axis Security Notification Service*에 가입할 수 있습니다.

Axis는 취약점을 어떻게 관리합니까?

*Axis 취약점 관리*를 참조하십시오.

Axis는 어떻게 소프트웨어 취약성을 최소화합니까?

사이버 보안을 Axis 소프트웨어 개발에 통합 문서를 읽어보세요.

Axis는 장치 수명 주기 전반에 걸쳐 사이버 보안을 어떻게 지원합니까?

*A lifecycle approach to cybersecurity(사이버 보안에 대한 수명주기 접근 방식)*을 참조하십시오.

Axis 제품에 내장된 사이버 보안 기능은 무엇입니까?

자세히 알아보기:

- *Axis Edge Vault*
- *AXIS OS*
- *장치 수명 주기 전반에 걸쳐 사이버 보안 지원*

Axis는 ISO 인증을 받았습니까? 그 외에 어떤 사이버 보안 관련 규정을 준수합니까?

예, Axis는 *ISO/IEC 27001:2023* 인증을 받았습니다. 당사는 소프트웨어, 클라우드 서비스 및 IT 인프라의 개발 및 운영과 관련한 요구 사항을 충족하는 정보 보안 관리 시스템(ISMS)을 갖추고 있습니다.

Axis Communications UK Ltd.는 Cyber Essentials(인증서 번호: IASME-CE-017710) 및 Cyber Essentials Plus(IASME-CEP-004245) 인증을 받았습니다.

AXIS OS 11 이상을 실행하는 Axis 장치는 *ETSI EN 303 645* 사이버 보안 표준 인증을 받았습니다. AXIS OS 네트워크 제품은 독일 연방 정보 보안청(*BSI - Bundesamt für Sicherheit in der Informationstechnik*)의 IT 보안 라벨(IT-Sicherheitskennzeichen)도 획득했습니다.

Axis 사이버 보안 규정 준수 및 인증에 대한 최신 정보는 *Axis Trust Center*에서 자세히 확인하십시오.

Axis는 우리 회사가 NIS 2를 준수하도록 어떻게 지원합니까?

*NIS 2*에 대한 문서를 참조하십시오.

T10189380_ko

2025-09 (M5.2)