백서

NIS 2

6월 2024

목차

1 서론

1.1 NIS 2란 무엇입니까?

NIS 2는 2024년 10월 17일까지 각 EU 회원국의 국내법에 반영되어야 하는 EU 지침입니다. NIS 2는 지역 안보와 경제 및 사회의 효과적인 기능에 기여하기 위해 EU 전체에서 높은 공통 수준의 사이버 보안을 달성하는 것을 목표로 합니다. 이를 달성하기 위해서는 사회의 주요 영역에서 필수적이고 중요한 서비스를 제공하는 조직이 사이버 보안 능력을 구축하고, 네트워크 및 정보 시스템에 대한 위협을 완화하고, 사고 발생 시 서비스의 연속성을 보장하며, 보안 사고를 관련 당국에 보고해야 합니다. 이를 위해 회원국은 국가 사이버 보안 전략을 채택하고, 사이버 위기 관리 당국 및 컴퓨터 보안 사고 대응 팀을 포함한 관할 기관을 설립해야 합니다. NIS 2에는 사이버 보안 위험 관리 조치와 시행 조치가 간략하게 설명되어 있습니다. 필수 조직 및 중요 조직의 규정을 준수하지 않아 발생하는 결과에는 경영진에 대한 무거운 벌금과 법적 처벌이 포함될 수 있습니다.

자세한 내용은 다음 웹사이트에서 확인하십시오.
eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1713340785613

1.2 NIS 2는 누구에게 영향을 줍니까?

NIS 2는 유럽 경제와 사회에 **필수적** 또는 **중요한** 서비스를 제공하는 모든 대상 주체에 영향을 미치며, 여기에는 기업 및 공급업체도 포함됩니다.

1.2.1 직접적으로 영향을 받는 대상

필수 대상 주체 - 에너지, 운송, 은행/금융, 건강, 식수, 폐수, 디지털 인프라, 공공 행정, 우주

중요 대상 주체 - 우편 서비스, 폐기물 관리, 화학, 식품, 제조(예: 의료 기기, 전기, 운송 장비), 디지털 제공업체(예: 온라인 마켓플레이스, 검색 엔진, 소셜 네트워크), 연구 기관

국가 관할 기관 - EU 회원국은 각자의 국가에서 NIS 2의 이행 및 시행을 감독하기 위해 국가 관할 기관을 지정합니다.

1.2.2 간접적으로 영향을 받는 대상

벤더 및 공급업체 - NIS 2는 필수 서비스 또는 디지털 서비스를 필수 및 중요 대상 주체에 제공하는 벤더, 공급업체 및 타사 서비스 제공업체에 간접적으로 영향을 미칩니다. 이러한 회사는 제품과 서비스의 보안을 보장해야 하며 고객의 계약상 사이버 보안 요구 사항이 적용될 수 있습니다.

필수 서비스 및 디지털 서비스의 사용자 - 필수 서비스 및 디지털 서비스의 사용자는 NIS 2의 직접적 규제를 받지는 않지만 지침에서 요구하는 개선된 사이버 보안 관행 및 사고 대응 능력의 혜택을 받습니다. 이를 통해 그들이 의존하는 서비스의 보안 및 신뢰성이 간접적으로 향상됩니다.

2 NIS 2 요구 사항

2.1 필수적이고 중요한 대상 주체의 경우

보안 조치 - 위험을 관리하고 네트워크 및 정보 시스템의 보안을 보장하기 위해 적절한 보안 조치를 시행합니다. 이러한 조치는 위험 평가와 모범 사례에 기반해야 합니다.

사고 보고 - 네트워크 및 정보 시스템의 보안에 중대한 영향을 미칠 수 있는 중대한 사고를 관할 당국에 보고합니다. 적시에 보고하는 것은 대응을 조율하고 잠재적 피해를 완화하는 데 필수적입니다.

위험 관리 - 위험 평가를 수행하여 잠재적인 위협과 취약점을 식별하고, 이러한 위험을 완화하기 위한 조치를 취합니다.

관할 당국과의 협력 - EU 회원국이 지정한 관할 당국과 협력합니다. 여기에는 규제 감독 및 사고 대응 목적을 위해 필요한 정보와 시스템에 대한 접근 권한 제공이 포함됩니다.

사고 대응 계획 - 사이버 보안 사고에 효과적으로 대응할 수 있도록 사고 대응 계획을 수립하고 유지합니다. 이러한 계획에는 사고를 감지, 보고 및 완화하는 절차가 포함되어야 합니다.

공급망 보안 - 타사 벤더 및 공급업체를 포함한 공급망을 보호하여 네트워크 및 정보 시스템의 전반적인 복원력을 보장합니다.

지속적인 모니터링 - 실시간으로 위협 및 취약점을 감지하고 대응하기 위해 네트워크 및 정보 시스템의 지속적인 모니터링 및 감사를 실행합니다.

3 공급업체에 미치는 영향

공급업체는 다음 요구 사항을 충족하여 NIS 2 대상 주체를 지원할 수 있습니다.

보안 내재화 설계 - IoT 장치 제조업체는 보안 기능을 제품 설계 단계에서부터 장치에 통합하여 보안이 제품의 필수 요소가 되도록 해야 합니다.

정기적 업데이트 및 패치 적용 - 제조업체는 IoT 장치의 취약점을 해결하기 위해 정기적인 보안 업데이트 및 패치를 제공해야 합니다.

인증 및 권한 부여 - IoT 장치는 무단 액세스를 방지하기 위해 강력한 인증 메커니즘 및 적절한 권한 통제를 사용해야 합니다.

데이터 암호화 - IoT 장치에 의한 데이터 전송 및 저장을 암호화하여 승인되지 않은 당사자가 민감한 정보를 가로채거나 무단으로 접근하는 것을 방지해야 합니다.

사고 보고 - 제조업체는 IoT 장치와 관련된 중요한 보안 사고 또는 침해를 관련 당국에 보고하고, 가능하면 소비자 또는 고객에게도 보고해야 합니다.

개인정보 보호 고려 사항 - 개인정보를 처리하는 IoT 장치는 NIS 2 외에도 GDPR(일반 데이터 보호 규정)과 같은 데이터 보호 규정을 준수해야 합니다.

공급망 보안 - 부품 공급업체부터 고객에 이르기까지 전체 공급망의 보안을 보장하여 생산 과정의 어느 지점에서든 보안 취약점이 발생하지 않도록 해야 합니다.

4 Axis의 대응

다음은 공급업체로서 Axis가 NIS 2 대상 주체의 요구 사항을 충족하는 방법입니다.

4.1 보안 내재화 설계

보안 내재화 설계는 제품 설계 및 개발의 필수적인 부분으로서 보안 고려 사항과 활동을 수행하고, 취약점의 위험을 줄이고, 제품에 견고한 보안 구성이 기본적으로 설정되도록 하기 위해 적용되는 접근 방식입니다. Axis의 보안 내재화 설계 원칙은 소프트웨어와 하드웨어에 적용되며, 다음과 같은 주요 요소로 구성됩니다.

- *ASDM(Axis 보안 개발 모델)*: ASDM은 보안 고려 사항이 소프트웨어 개발의 필수적인 부분이 되도록 하는 정의된 프로세스 및 도구로 구성된 프레임워크입니다. 활동에는 위험 평가, 위협 모델링, 침투 테스트, 취약점 스캔, 사고 관리, 버그 바운티 프로그램 등이 포함됩니다. Axis 소프트웨어 개발자는 ASDM을 사용하여 보안이 소프트웨어 개발에 내장되도록 하여, 취약점이 포함된 소프트웨어를 배포할 위험을 줄입니다.
- *버그 바운티 프로그램*: Axis는 대부분의 Axis 제품을 구동하는 Linux 기반 운영 체제인 AXIS OS의 취약점을 사전에 식별, 패치 및 공개하려는 회사의 노력을 강화하는 전용 버그 바운티 프로그램을 지원합니다. 버그 바운티 프로그램은 외부 보안 연구자 및 윤리적 해커와 전문적인 관계를 구축하기 위한 Axis의 노력을 강화합니다.
- *소프트웨어 구성품 명세서(SBOM)*: Axis는 대부분의 Axis 장치에 사용되는 Linux 기반 운영 체제인 AXIS OS를 위한 SBOM을 제공합니다. SBOM은 보안 연구자, 당국 및 고객에게 AXIS OS를 구성하는 소프트웨어 구성 요소에 대한 인사이트를 제공합니다. SBOM은 취약성 평가 및 위협 분석을 전문으로 하는 사람들에게 특히 유용하며, 사이버 보안의 투명성을 위한 Axis의 노력을 보여줍니다.
- *AXIS OS 기본 보안 설정*: 최신 AXIS OS 버전을 실행하는 장치는 기본 비밀번호 없음, HTTP 및 HTTPS 활성화, 보안 온보딩 및 IEEE 802.1X/802.1AR/802.1AE가 기본적으로 활성화된 통신, 덜 안전한 프로토콜 비활성화 등의 공장 기본 설정 상태로 사전 구성됩니다. 기본 보호 컨트롤에 대한 자세한 내용은 *여기*에서 확인할 수 있습니다.
- *Axis Edge Vault*: Axis 장치에 내장된 Axis Edge Vault는 하드웨어 기반 보안 플랫폼으로, Axis 네트워크 제품의 무결성을 보호하고 암호화 키를 기반으로 보안 작업을 실행할 수 있는 기능을 포함하고 있습니다. Axis Edge Vault는 Secure Boot 및 Signed OS를 통한 공급망 보호, 장치의 출처를 증명하기 위해 내장된 고유 Axis 장치 ID를 통한 신뢰할 수 있는 장치 ID, 암호화 정보의 변조 방지 저장을 위한 보안 키 스토리지, Signed Video(서명된 영상)를 통한 비디오 변조 감지를 제공합니다.

4.2 정기적 업데이트 및 패치

Axis는 Axis 하드웨어 및 소프트웨어 제품에서 새롭게 발견된 보안 취약점을 비롯한 다양한 문제를 해결하도록 소프트웨어 업데이트를 제공합니다. Axis는 고객이 더 쉽게 Axis 장치 소프트웨어를 최신 상태로 유지할 수 있도록 돕기 위해 장치 관리 도구도 제공합니다. 연결된 장치를 위한 새로운 AXIS OS 릴리스는 AXIS Companion, AXIS Camera Station, 그리고 Milestone

XProtect® 및 Genetec™ Security Center와 같은 파트너 영상 관리 소프트웨어 및 Axis 장치 관리 도구에서 확인할 수 있습니다. 이외에도, Axis는 누구나 구독할 수 있는 보안 알림 서비스를 제공합니다. 자세한 내용은 아래에서 확인할 수 있습니다.

- *AXIS OS*: Axis는 장치 소프트웨어를 최신 상태로 유지하기 위한 두 가지 주요 대안, 즉 액티브 트랙과 LTS(Long Term Support) 트랙을 제공합니다. 액티브 트랙은 버그 수정 및 보안 패치뿐만 아니라 최신 첨단 기능에 대한 액세스를 제공합니다. LTS(Long Term Support) 트랙의 소프트웨어는 버그 수정 및 보안 패치만 제공하여 안정성을 극대화합니다. 잘 통합된 타사 시스템을 유지하는 데 중점을 두고 있기 때문입니다.
- 장치 관리 도구: *AXIS Device Manager* 및 *AXIS Device Manager Extend는* 고객이 Axis 장치 소프트웨어를 최신 보안 패치 및 버그 수정으로 더 쉽게 최신 상태로 유지할 수 있도록 도와주는 도구입니다.

  로컬에서 Axis 장치를 효율적으로 구성하고 관리하려는 경우, AXIS Device Manager를 사용하면 장치 자격 증명 관리, 인증서 배포, 사용하지 않는 서비스 비활성화, AXIS OS 업그레이드와 같은 보안 작업을 일괄 처리할 수 있습니다.

  AXIS Device Manager Extend는 사용하기 쉬운 단일 애플리케이션에서 모든 장치와 사이트에 대한 정보를 수집하는 통합 대시보드를 제공합니다. 장치 소프트웨어 업그레이드가 가능할 때마다 알림을 받게 되며, 대규모 업그레이드 및 기타 작업을 일괄적으로 수행할 수 있습니다. 교체 제품에 대한 추천도 받게 됩니다. 활동을 완전히 추적할 수 있으며, 보고 또는 감사 목적으로 모든 시스템 장치 정보를 내보낼 수 있습니다.
- *Axis 보안 알림 서비스*: Axis가 가입을 권장하는 이 서비스는 가입자에게 보안 사고 및 취약점에 대한 알림을 적시에 제공합니다.

4.3 인증 및 권한 부여

무단 접근을 방지하고 전반적인 Axis 장치 보안을 강화하기 위해 Axis는 다음과 같은 지원을 제공합니다.

- 역할 기반 액세스 장치 관리 액세스 권한(관리자/운영자/보는 사람) 및 Axis 장치를 IT 표준화 ADFS(*Active Directory Federation Service*) 통합에 연결하여 인증/권한을 중앙 집중화할 수 있습니다. (ADFS는 Windows Server 운영 체제 사용자에게 싱글 사인 온(SSO) 인증 서비스를 제공하기 위해 Microsoft에서 개발한 소프트웨어 구성 요소입니다. ADFS는 사용자가 조직 경계를 넘어 Windows Server 운영 체제에서 애플리케이션에 단일 로그인 자격 증명을 사용하여 액세스할 수 있도록 합니다.)
- *제로 트러스트 네트워킹*을 더 쉬워지게 하는 기술. 최신 AXIS OS 릴리스에서 이러한 기술에는 IEEE 802.1X 네트워크에 장치를 자동으로 안전하게 온보딩하기 위한 IEEE 802.1AR 호환 Axis 장치 ID 및 데이터 통신의 자동 암호화를 위한 IEEE 802.1AE(MACsec)와 함께 IEEE 802.1X가 포함됩니다.

4.4 데이터 암호화

승인되지 않은 사람이 민감한 정보를 가로채거나 접근하는 것을 방지하기 위해 Axis 제품은 다음을 지원합니다.

- 모든 데이터 통신이 TLS 1.2 또는 최신 표준을 지원하는 HTTPS. AXIS Camera Station 영상 관리 소프트웨어 서버와 클라이언트 간의 비디오 스트림 연결은 AES-256으로 암호화됩니다.
- 자동 데이터 통신 암호화를 위한 *IEEE 802.1AE (MACsec)*.
- RTP를 통한 Secure Video 스트리밍. 이는 SRTP/RTSPS라고도 하며 AXIS OS 7.40부터 시작되었습니다. SRTP/RTSPS는 안전한 엔드 투 엔드 암호화 전송 방법을 사용하여 인증된 클라이언트만 Axis 장치의 비디오 스트림을 수신하도록 합니다.
- *에지 스토리지 암호화*(SD 카드)
- AXIS OS 10.10부터 *에지 녹화(SD 카드, 네트워크 공유)의 패스워드 암호화 내보내기*. 즉, 패스워드로 암호화된 녹화물을 내보낼 수 있어 내보낸 녹화물을 수동으로 암호화할 필요 없이 민감한 영상 데이터를 안전하게 공유할 수 있습니다.

4.5 사고 보고

Axis는 제품 및 서비스에서 발견된 보안 사고 또는 취약점에 대한 사고 보고를 제공합니다.

- Axis는 공통 취약점 및 노출(CVE) 번호 부여 기관(Common Vulnerability and Exposures (CVE) Numbering Authority)입니다. 즉, Axis는 고객의 노출 위험을 최소화하기 위해 업계 모범 사례를 따라 제품 및 서비스의 취약성을 발견하고 투명하게 관리합니다. Axis는 새로 발견된 취약점에 CVE 번호를 할당하고 이를 *www.cve.org* 웹 사이트에 보고할 수 있습니다. Axis *취약점 관리 정책*은 axis.com에 게시되어 있습니다.
- 누구나 *여기*에서 구독하여 Axis의 보안 알림을 받을 수 있습니다.
- 보안 패치 및 버그 수정은 새로운 AXIS OS 버전에 배포됩니다. 업데이트된 장치 소프트웨어의 사용 가능 여부는 AXIS Companion, AXIS Camera Station, AXIS Device Manager, AXIS Device Manager Extend 및 Milestone XProtect 및 Genetec Security Center와 같은 타사 VMS에서도 확인할 수 있습니다.
- Axis는 모든 회사 관련 사이버 공격에 대해 투명성을 유지하기 위해 노력하고 있으며, 관련 스웨덴 당국이 제공하는 지침에 따라 이러한 사고를 보고할 것입니다.

4.6 개인정보 보호 고려 사항

Axis는 *개인정보 취급방침* 및 처리방침을 온라인에 게시하며, 여기에는 수집되는 개인정보(예: My Axis의 온라인 계정에서 수집되는)와 그러한 개인정보의 사용 방식이 간략하게 설명되어 있습니다.

Axis는 ISO/IEC 27001 인증을 받은 Information Security Management System(정보 보안 관리 시스템)과 관련된 *사이버 보안 프레임워크 및 관행*을 발표했습니다. Axis ISO/IEC 27001 인증의 범위는 내부 IT 인프라 및 서비스의 개발과 운영을 포함합니다. ISO 27001은 효과적인 위험 관리를 통해 조직의 정보를 보호하고 관리하는 방법에 대한 지침을 제공하는 국제 공인 표준입니다.

ISO/IEC 27001 준수는 Axis가 고객과 파트너에게 서비스를 지원하고 제공하는 내부 정보 인프라와 시스템을 관리하기 위해 국제적으로 인정된 프로세스와 모범 사례를 사용하고 있음을 보여주는 것입니다.

이외에도, Axis는 고객이 비디오 및 오디오 캡처와 관련하여 보안 감시에서 개인정보 보호 문제를 해결할 수 있도록 지원합니다. 솔루션에는 다음이 포함됩니다.

- Axis 카메라의 정적 프라이버시 마스킹, 그리고 *AXIS Live Privacy Shield* 소프트웨어 애플리케이션을 사용한 동적 프라이버시 마스킹
- 통계적 수치 데이터만 캡처하고 저장하며 개인 식별 정보는 처리하지 않는 *AXIS People Counter* 애플리케이션 또는 *AXIS P8815-2 3D People Counter*와 같은 에지 기반 분석 애플리케이션
- *열상 카메라*
- *레이더 제품*
- 객체 또는 관심 없는 영역을 마스킹하기 위한 *AXIS Camera Station*의 비디오 편집 도구
- Axis 영상 감시 제품에서 *기본적으로 비활성화된 오디오 기능*

개인정보 보호 솔루션에 대한 자세한 내용은 *axis.com/solutions/privacy-in-surveillance에서* 확인할 수 있습니다.

4.7 공급망 보안

보안 취약점이 발생하는 것을 방지하려면 부품 공급업체에서 고객에 이르는 공급망을 보호하는 것이 중요합니다.

Axis는 사이버 보안을 다룰 때 제품 *수명주기 접근 방식*을 사용합니다. Axis는 부품 수준에서 완제품에 이르는 전체 공급망뿐만 아니라 유통 및 구현, 사용 및 폐기 단계에서도 위험을 완화하기 위해 최선을 다하고 있습니다.

다음은 Axis가 공급망 보안을 해결하는 몇 가지 방법입니다.

- Axis는 전략적 공급업체로부터 직접 핵심 구성 요소를 조달합니다. Axis는 제조 파트너와 긴밀하게 협력합니다. 생산 공정을 모니터링하고 데이터를 연중무휴로 공유하여 실시간 분석 및 투명성을 확보합니다. *Axis 공급망 보안*에 대해 자세히 알아보십시오.
- Axis Edge Vault를 통한 내장형 장치 보안은 다음과 같은 기능을 통해 Axis 장치의 무결성을 보호합니다.
  - **Signed OS**: 설치된 AXIS OS가 Axis의 정품임을 보장합니다. 또한 장치에 설치하려는 모든 새 AXIS OS도 Axis에서 서명했는지 확인합니다.
  - **Secure Boot**: 장치가 운영 체제에 Axis 서명이 있는지 확인할 수 있도록 합니다. OS가 승인되지 않았거나 변경된 경우, 부팅 프로세스가 중단되고 장치 실행이 중지됩니다. Signed OS, Secure Boot, 장치 공장 초기화를 조합하면 장치 배송 중 변조 시도를 방지할 수 있습니다.

- **Axis 장치 ID**는 IEEE 802.1AR을 준수하므로 네트워크에서 장치를 안전하게 식별하고 온보딩할 수 있습니다. Axis 장치 ID는 장치의 보안 키 저장소(Secure Element, TPM, TEE)에 저장됩니다.
- **암호화된 파일 시스템**은 장치가 시스템 통합업체에서 고객에게 배송 중인 경우와 같이, 장치를 사용하지 않는 동안에 파일 시스템에 저장된 고객별 구성 및 정보가 추출되거나 변조되는 것을 방지합니다.
- 이외에도, Axis는 **Signed Video(서명된 영상)**를 지원하므로, 보는 사람은 장치에서 내보낸 비디오가 변조되었는지 여부를 확인할 수 있습니다. 이는 수사 시 또는 기소 시 특히 중요합니다. 자세한 내용은 *axis.com/solutions/edge-vault*에서 확인할 수 있습니다.

- 소프트웨어를 axis.com에서 다운로드할 때 체크섬이 제공됩니다. 체크섬을 통해 파일의 무결성을 확인할 수 있습니다.
- ETSI 인증: AXIS OS 11 이상을 실행하는 150개 이상의 Axis 제품이 *ETSI EN 303 645 사이버 보안 표준* 인증을 받았습니다. ETSI는 유럽전기통신표준협회(European Telecommunications Standards Institute)의 약자입니다. 이러한 요구사항은 장치 자체에 적용되며, 보안 키 저장소와 같은 하드웨어 기반 보안 기능과 HTTPS가 기본적으로 활성화되고 기본 패스워드가 없는 등의 기본 보안 기능에 대한 지원을 포함합니다. 또 다른 측면은 장치 보안 업데이트에 대한 정의된 지원 기간과 같은, 수명 주기 관리와 관련이 있습니다. 그 외에도 소프트웨어 개발 시 취약점 위험을 줄이기 위한 방법론을 마련하고, 투명한 취약점 관리 정책을 수립하며, 개인 데이터 처리 모범 사례를 지원하는 것 등이 있습니다. 이러한 요구사항은 인증 제품이 수명 주기 동안 최소한의 기본 보안 수준을 유지하는 데 도움이 되는 업계 모범 관행을 고려합니다. 이 표준은 EU 사이버 보안 복원력 법, EU 무선 장비 지침 및 전 세계의 기타 표준 및 법률과 긴밀히 연계되어 있습니다.

4.8 교육 및 안내

Axis는 직원, 파트너 및 고객에게 사이버 보안 모범 사례에 대한 정보 및 교육을 제공합니다. 여기에는 다음이 포함됩니다.

- 내부 보안 인식 및 교육: Axis는 조직에 대한 보안 위협을 방지하고 완화하기 위해 직원들을 지속적으로 교육하기 위한 보안 인식 프로그램을 개발했습니다. 이 인식 교육은 Axis 직원이라면 꼭 받아야 합니다. 개인의 조직 내 역할과 책임에 따라 개발자와 시스템 소유자를 대상으로 추가 보안 교육이 제공됩니다.
- *Axis Academy 교육*: 고객이 이용할 수 있는 교육 과정에는 사이버 보안에 대한 온라인 과정과 *사이버 보안 주제에 대한 Axis의 접근 방식*이 포함되어 있습니다.
- 다음에 대한 *보안 강화 가이드*가 온라인으로 제공됩니다.
  - *AXIS OS*
  - *AXIS Camera Station*
  - *Axis 네트워크 스위치*

- *AXIS OS Security Scanner Guide*: Axis 장치에 대한 보안 검사를 실행하여 Axis 장치가 취약점이나 잘못된 구성의 영향을 받는지 확인하는 것이 좋습니다. AXIS OS Security Scanner Guide는 특정 스캔 결과를 보정하는 방법에 대한 권장 사항을 제공하고 일반적인 "잘못된 경보"에 대해 간략하게 설명합니다.
- *AXIS OS Forensic Guide*: 이 가이드는 Axis 장치가 설치된 주변 네트워크 및 IT 인프라에 대한 사이버 보안 공격이 발생할 경우 Axis 장치의 포렌식 분석을 수행하는 모든 사람에게 기술적 조언을 제공합니다.

Axis 및 사이버 보안에 대한 자세한 내용은 *Axis 사이버 보안 포털*을 참조하십시오.

T10210486/KO/M3.3/2406

Axis Communications 정보

Axis는 보안 및 새로운 비즈니스 성과를 개선하기 위한 솔루션을 창조하여 더 스마트하고 안전한 세상을 가능하게 합니다. 네트워크 기술 회사이자 업계 리더인 Axis는 비디오 감시, 접근 제어, 인터콤, 오디오 시스템 솔루션을 제공합니다. 이러한 솔루션은 지능형 분석 애플리케이션으로 향상되고, 고품질 교육의 지원을 받습니다.

Axis에서는 50개 이상의 나라에 약 4,000명의 전담 직원이 있으며 전 세계 기술 및 시스템 통합 파트너와 협력하여 고객 솔루션을 제공합니다. Axis는 1984년에 설립되었으며 본사는 스웨덴 룬드에 있습니다