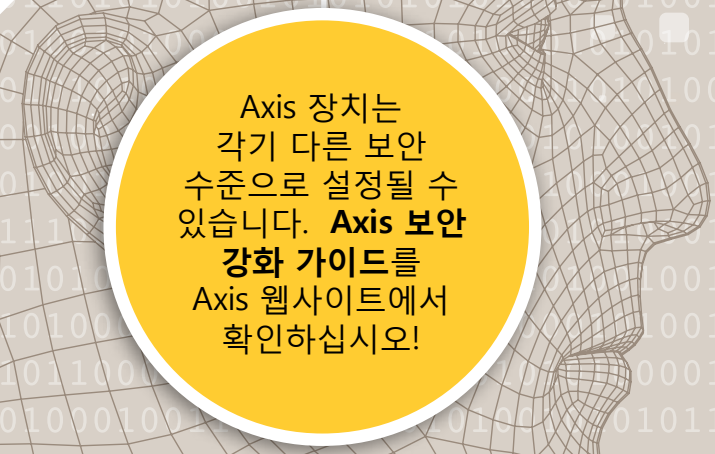
Axis Communications & 사이버 보안

네트워크 카메라를 비롯하여 모든 네트워크 장치는 위협의 대상입니다. 네트워크 카메라는 항상 네트워크가 백본인 대규모 시스템의 일부입니다. 시스템이든 개별 장치이든, 모든 부분은 취약하며 전체 시스템은 보호가 필요합니다.



Axis 장치는 각기 다른 보안 수준으로 설정될 수 있습니다. **Axis 보안 강화 가이드**를 Axis 웹사이트에서 확인하십시오!

귀사의 보안 수준은 **가장 약한 부분만큼만** 강할 뿐입니다.

사이버 위협에 대한 더 높은 수준의 보호를 제공하는 것은 적절한 위험 분석과 결합된 조직의 IT 및 사이버 정책에 달려 있습니다. IP 기반 장치는 추가적인 가치와 인텔리전스를 제공합니다. 노출 영역을 줄이고 위험을 완화하여 시스템을 더 안전하게 보호할 수 있습니다. 공격을 예방할 수는 없지만, Axis 취약성 정책(웹 사이트에서 이용 가능)은 파트너와 최종 사용자가 Axis에 기대할 수 있는 사항을 설명하고 있습니다.

Axis의 사이버 보안 미션:

> 보안 산업에 대한 인식 향상
> 사고 리더십(thought leadership) 제공
> 이해 당사자가 운영 및 요건을 기반으로 카메라/영상 시스템에 대해 적정한 보호 수준을 달성할 수 있도록 지원

www.axis.com/support/product-security

AXIS COMMUNICATIONS

Axis Communications 이 제시하는 Top 10 사이버 보안 권장 사항

1. 잠재적인 위협과 시스템이 공격받을 경우 발생 가능한 피해/비용에 대한 위험 분석을 수행하십시오.

2. 시스템 보호 및 가능한 위협에 대한 지식을 확보하십시오. 리셀러, 시스템 통합업체, 컨설턴트, 제품 벤더와 밀접하게 협업하십시오. 인터넷에서 많은 관련 정보를 찾을 수 있습니다.

3. 네트워크를 보호하십시오. 네트워크 보안이 침해되는 경우, 민감한 정보에 대한 스누핑 위험과 개별 서버 및 네트워크 장치에 대한 공격이 증가합니다.

4. 강력하고 독특한 패스워드를 사용하고, 정기적으로 변경하십시오.

5. 네트워크 장치의 공장 출하 시 기본 설정에 의존하지 마십시오.
> 기본 패스워드를 변경하십시오.
> 장치 보호 서비스를 활성화하고 설정하십시오.
> 사용하지 않는 서비스를 비활성화하십시오.

6. 로컬 네트워크일 경우에도, 가능한 경우 암호화된 연결을 사용하십시오.

7. 노출을 줄이기 위해, 비디오 클라이언트는 시스템/솔루션에서 필요로 하지 않는 한 카메라에 직접 액세스할 수 없어야 합니다.
클라이언트는 VMS(영상 관리 시스템) 또는 미디어 프록시를 통해서만 영상에 액세스해야 합니다.

8. 인가되지 않은 액세스 시도를 감지하기 위해 액세스 로그를 정기적으로 확인하십시오.

9. 정기적으로 장치를 모니터링하십시오. 시스템 알림이 적용 가능하거나 지원되는 경우, 이를 활성화하십시오.

10. 적용 가능한 최신의 펌웨어를 사용하십시오. 보안 패치에 포함되어 있을 수 있습니다.

www.axis.com/support/product-security

AXIS COMMUNICATIONS