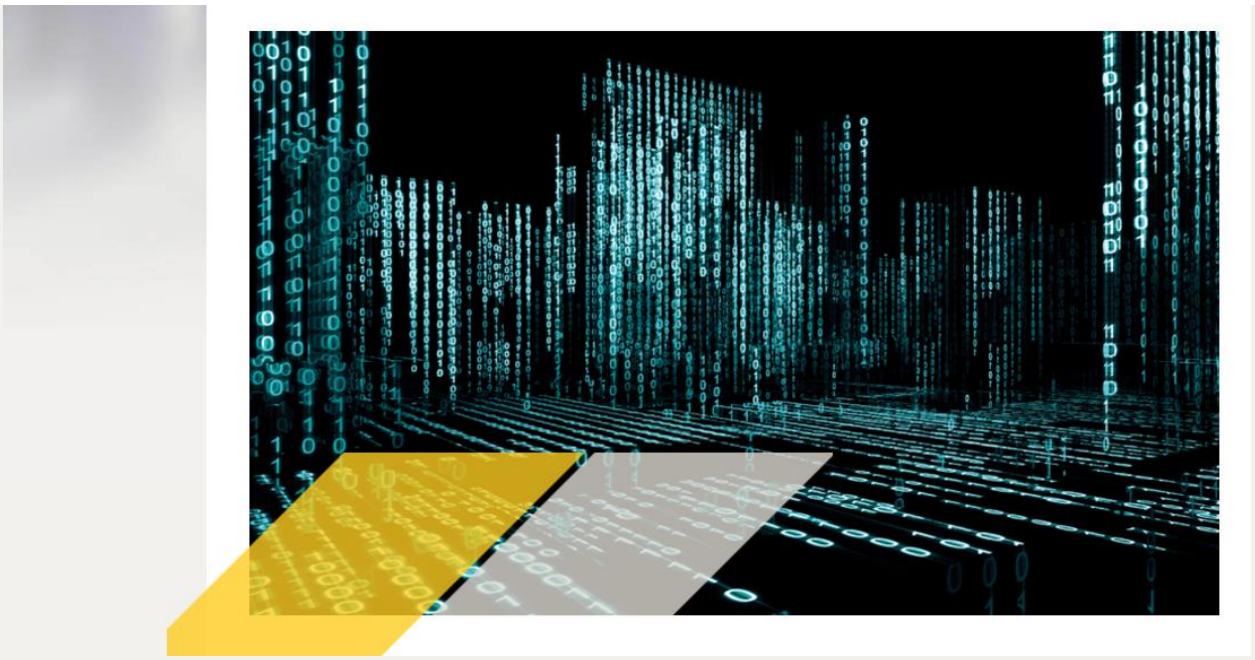

IP 카메라 - 네트워크 도어를 열어두지 마십시오.

IoT의 비전이 편리함과 및 능력, 연결된 장치의 방대한 네트워크가 제공하는 편리함과 기능, 그리고 유연성이라는 유혹에 빠져있는 동안, 네트워크 진입점 수의 극적인 증가에 따른 보안 위협과 위반 요소의 위험이 크게 늘어나는 추세입니다. 최근 Cisco가 진행한 설문조사에서 비즈니스 의사결정권자의 73%가 향후 2년 이상 심각하게 증가할 보안 위협을 야기할 원인으로 IoT를 언급했습니다. 더욱 우려되는 것은, IT 보안 전문가의 78%가 자신의 능력에 대해 확신하지 못하거나, 새로운 종류의 네트워크 연결 장치를 보호하는 데 필요한 안목과 관리가 부족하다고 믿는 것입니다.

네트워크 접근 가용성의 증가는 보안 위반으로 인한 위험을 증가시킵니다. 시스템 설계 시 철저한 시스템 위협/위험 분석이 고려되어야 합니다. 시스템에 추가되는 애플리케이션 같이, 새 구성요소가 추가됨에 따라 공격 노출 영역은 증가합니다. 비디오 시스템을 추가하면 노출 영역이 증가될 것입니다. 마치 Microsoft Office Suite를 모든

PC에 설치하면 추가적인 사이버 위험이 증가하는 것처럼 말입니다. 비디오 시스템 구성 요소는 다른 네트워크 리소스에 위험을 높일 수 있으며, 마찬가지로 네트워크에 더해지는 추가 리소스는 비디오 시스템에 위험을 가져옵니다. 공격 영역을 최소화하는 것은 일반적인 사이버 보호 조치입니다. **장치, 서비스 및 애플리케이션이 상호 작용할 필요가 없다면, 그 사이의 연결을 제한해야 합니다.** 기존 네트워크로부터 비디오 시스템을 격리하는 것은 일반적으로 양호한 보호 조치이며, 비디오 및 비즈니스 리소스가 부정적이거나 위험한 방법으로 서로에게 영향을 미치는 위험을 줄입니다.

노트북, 데스크톱, 또는 모바일 장치 같은 다른 네트워크 장치와 달리, 네트워크 카메라는 사용자가 잠재적으로 유해한 웹사이트를 방문하고 악의적인 이메일 첨부 파일을 열거나 신뢰할 수 없는 애플리케이션을 설치하는 등의 일반적인 위협에는 노출되지 않습니다. 그러나 인터페이스가 있는 네트워크 장치이므로, 카메라 또는 연결된 다른 물리적 보안 장치는 위험에 노출될 수도 있습니다. 그러므로 이러한 위험의 노출 영역을 줄이는 것이 중요합니다.

설치 담당자와 IT 직원이 비디오 보안 시스템을 보호하거나 보안 강화 과정을 이해하는 것이 갈수록 중요해지고 있습니다. 훌륭한 보안 강화 가이드는 특정 사용자 필요 조건에 맞는 구성 전략을 제공하여 증가하는 위협 환경에 대응합니다. Axis는 SANS Top 20위 핵심 보안 제어를 Axis 보안 강화 가이드에 대한 기준으로 삼습니다. 첫 번째 단계는 다양한 수준의 사용자 인증/승인, 패스워드 보호, SSL/TLS 암호화, 802.1X, IP 필터링 및 인증서 관리를 포함하는 산업 표준 보안 프로토콜을 이해하고 올바르게 사용하는 것입니다.

또한 Axis와 같은 카메라 공급자는 새로운 기능, 버그 수정 및 보안 패치를 적용한 카메라 펌웨어를 계속 업데이트하고 있습니다. 보안 시스템 사용자는 증가하는 위험과 다양성 및 규모가 큰 보안 위험을 처리하기 위해 카메라 공급자가 제공하는 업데이트를 자세히 알고 있어야 하며, 네트워크 카메라 기반 시스템을 통한 공격을 예방한 모범 사례에 주목해야 합니다.