백서

비디오 데이터로 증거 활용

AXIS Camera Station으로 비디오 데이터 무결성 보호

7월 2021

목차

1 요약

고품질의 신뢰할 수 있고 훼손되지 않은 비디오 데이터는 증거로 사용할 수 있습니다. AXIS Camera Station을 사용하여 비디오 데이터를 증거로 처리하는 모범 사례:

- 원하는 이미지, 녹화, 보안을 제공할 수 있도록 시스템을 적절하게 설계, 구성, 검증
- 정기적인 유지 관리 수행
- 설정된 절차에 따라 증거 처리

2 서론

감시 비디오는 법정에서 증거물로 사용할 수 있도록 사실상 맞춤 제작된 것입니다. 말하자면 "테이프에" 포착된 이벤트는 거부할 수 없습니다. 아니면 거부할 수 있습니까? 글쎄요, 판사는 아마도 고품질이고 신뢰할 수 있으며 훼손되지 않은 비디오 데이터를 받아들일 겁니다.

그러나 비디오의 증거 가치가 의도치 않게 낮아지는 경우도 있습니다. 예를 들어, 사람이나 차량이 갑자기 사라지거나 이미지에서 "점프"하는 등 시간 간격이 있는 감시 영상은 증거물로 사용하기에 충분히 신뢰할 수 없는 것으로 간주될 수 있습니다. 비디오의 메타데이터(타임스탬프 또는 카메라의 MAC 주소)가 맞지 않는지 여부도 질문될 수 있습니다. 비디오가 편집, 삭제 또는 훼손되었을 수 있다는 의심은 비디오 소유자의 신뢰성을 떨어뜨릴 수 있습니다.

이 백서에서는 증거로서 비디오를 관리하는 방법에 대해 조언합니다. 보다 구체적으로, 증거 사슬에서 영상 관리 소프트웨어(VMS) AXIS Camera Station의 역할과 비디오 소유자의 역할을 설명합니다.

Figure 1. 전략적 장소에서의 영상 감시는 올바르게 설정 및 관리된다면 귀중한 증거를 제공할 수 있습니다.

3 비디오 데이터를 증거로 처리하는 모범 사례

영상 감시를 사용하는 기업과 조직은 비디오 데이터의 처리 및 저장 방법을 결정하는 프로세스와 절차를 마련해야 합니다. 카메라 중 하나가 사건을 포착할 때 완벽하게 대비하려면, 비디오를 덮어쓰거나, 훼손하거나, 도난당하지 않도록 보호해야 합니다. 또한 안전하게 영상을 내보내 저장 공간을 보호하고 이를 법 집행 기관에 넘길 수 있어야 합니다.

그러나 고품질 비디오 증거 제작은 비디오 시스템의 의도적인 설계부터 시작하는 프로세스입니다. 또한 시스템을 최신 상태로 유지하고 불규칙성을 추적하는 것이 가장 중요합니다. 이 장에서는 이 프로세스의 단계와 AXIS Camera Station 및 그 도구 상자인 AXIS Camera Station Integrator Suite를 사용하여 수행할 수 있는 방법을 설명합니다.

시스템 설계, 시스템 유지 관리 및 사건 처리와 관련된 이러한 원칙에 따라 감시 영상을 제작하는 경우, 현행 사이버 보안 요건을 준수할 것이며, 대부분의 경우 필요하다면 증거로서의 가치를 제공할 것입니다.

Figure 2. AXIS Camera Station 소프트웨어는 영상 감시 시스템의 설정, 일상적인 운영 및 전략적 관리를 모두 용이하게 합니다.

3.1 적절한 시스템 설계...

영상 감시 시스템은 주의하여 설계해야 합니다. 필요에 따라 장비를 선택하고 원하는 이미지, 원하는 녹화 유형 및 보안을 제공하도록 설정해야 합니다. AXIS Site Designer는 이러한 목적을 위해 많은 지원을 제공합니다.

3.1.1 원하는 이미지를 제공하려면

이미지 품질은 카메라와 위치에 따라 다릅니다. 카메라 모델, 렌즈, 장면까지의 카메라 거리와 각도를 알고 있는 경우 이미지의 해상도, 보다 구체적으로는 이벤트 장면 전체의 픽셀 밀도를 계산할 수 있습니다. 장면에 있는 사람 얼굴 전체에 적절한 픽셀 밀도를 얻으려면 더 많은 카메라를 배치하거나 더 높은 해상도의 카메라를 사용해야 할 수 있습니다. 특정 사이트의 특정 카메라에 대한 시야각, 조명 요건 및 기타 매개변수를 조사해야 합니다. 이 모든 것은 AXIS Site Designer에서 원활하게 설계할 수 있습니다.

3.1.2 원하는 녹화를 제공하려면

비디오를 녹화하려면 리던던시 기능이 있는 검증된 고성능 하드웨어를 사용해야 합니다. 시스템 신뢰성을 높이기 위해 AXIS Camera Station은 네트워크 카메라 SD 카드에 이미지를 임시로 저장하여 페일오버 녹화를 지원합니다. VMD(비디오 모션 디텍션) 분석을 사용하는 경우 전체 사건을 검증하는 데 가

치를 제공할 수 있을 만큼 녹화 시간이 충분히 길어야 합니다. 최적으로 보정되지 않은 모션 디텍션 녹화는 시간 간격과 연결되지 않는 영상을 나타낼 수 있습니다. 많은 경우 지속 녹화가 더 나은 선택이 될 수 있지만, 충분한 대역폭의 지속적인 가용성과 훨씬 더 많은 저장 공간이 필요합니다.

3.1.3 원하는 보안을 제공하려면

무단 액세스를 방지하는 데 필요한 물리적 보안을 시스템에 제공해야 합니다. 카메라, 네트워크 장비 및 케이블, 서버, 데이터 스토리지, 전원 장치 및 케이블을 포함한 모든 하드웨어 요소를 보호해야 합니다. 보안 조치에는 서버 룸 액세스 제한 영역 유지, 서버 캐비닛 잠금, 캐비닛 내 서버 랙 설치, 서버의 물리적 포트 비활성화, 네트워크 케이블 노출 차단 등이 포함될 수 있습니다.

또한 데이터 남용, 데이터 훼손 시도, 악의적인 공격의 위험을 최소화하는 데 필요한 사이버 보안을 시스템에 제공하기 위해 노력해야 합니다. 소프트웨어 도구와 기술을 통해 시스템이 현행 보안 표준을 충족하도록 하는 이른바 강화 기능을 부분적으로 제공할 수 있습니다. 그러나 또한 강화는 시스템 소유자가 사이버 보안 사고방식을 적용하고 조직 내에 이를 전파하기 위해 적극적으로 노력해야 합니다. 예를 들어, 시스템의 모든 사용자는 추측하기 어려운 강력한 패스워드를 사용하는 것이 중요하다는 것을 알고 있어야 하며 패스워드가 노출되지 않도록 주의해야 합니다. 또한 최소 권한 사용자 계정 접근 방식을 사용하여 사용자 액세스와 사용자 권한도 최소화해야 합니다. 시스템 소유자는 직원에게 모범 사례를 교육하고 이러한 모범 사례가 성공적으로 구현되도록 보장할 책임이 있습니다. 공인 통합 업체가 시스템을 강화시킬 수 있지만, 일부 사이버 보안 대책은 시스템을 사용하는 사람들의 적극적인 협조가 있어야만 효과적일 수 있습니다.

전반적인 사이버 보안 강화를 위한 한 가지 중요한 방법은 암호화된 데이터 전송을 사용하여 비디오를 보호하는 것입니다. 클라이언트와 서버 간의 데이터 전송을 위해 AXIS Camera Station은 비디오, 오디오 및 메타데이터에 AES 암호화를 사용하고 다른 데이터에는 TLS 1.2 암호화를 사용합니다. AXIS Camera Station은 HTTPS를 통해 카메라와 서버 간의 데이터 스트림을 암호화하도록 구성할 수도 있습니다. 소프트웨어 보호를 위한 다른 모범 사례로는 사용되지 않는 서비스 비활성화, IP/MAC 주소 필터링 사용, IEEE 802.1X 수용, SNMP 모니터링 수용, 신뢰할 수 있는 NTP 서버와 함께 올바른 날짜 및 시간 설정(비디오 메타데이터의 타임스탬프 정확성 보장), 원격 연결 시 Axis Secure Remote Access만 사용(포트 포워딩 또는 원격 데스크톱 대신) 등이 있습니다. 자세한 사이버 보안 조치 및 권장 사항은 Axis 사이버 보안 강화 가이드를 참조하십시오.

3.1.4 시스템 구성 및 검증

AXIS Site Designer를 사용하여 설계할 때 이미 시스템의 주요 부분을 특정 카메라 이름, 해상도 및 보존 시간으로 구성할 수 있습니다. 시스템이 설계 및 설치되면 AXIS Site Designer에서 설정한 구성을 AXIS Camera Station으로 자동으로 가져올 수 있으며, 여기서 원하는 경우 설정을 계속 변경하고 조정할 수 있습니다.

실제 설치가 완료된 후 AXIS Camera Station Integrator Suite의 일부인 AXIS Installation Verifier를 사용하여 시스템을 검증할 수 있습니다. Installation Verifier는 야간 모드와 일반 모드에서 시스템을 테스트하여 노이즈 수준이 높고 더 많은 대역폭이 필요한 저조도 작동 시 충분한 대역폭이 있는지 확인합니다. 그런 다음 AXIS Installation Verifier는 첫 번째 병목 현상이 발견될 때까지 시스템에서 생성되는 데이터 볼륨을 꾸준히 늘려 스트레스 테스트를 수행합니다. 이렇게 하면 시스템 예비 용량이 표시되고 시스템 개선이 필요한지 여부를 알 수 있습니다.

3.2 정기적인 유지 관리 수행

시스템을 가동하고 운영할 때는 지속적으로 모니터링하고 업데이트해야 합니다.

하드웨어와 소프트웨어가 예상대로 계속 작동하는지 확인하십시오. 비디오 품질을 검사하고 일정에 따라 카메라 렌즈를 청소하고, 물리적인 훼손이 없는지 확인하고 카메라의 시야각과 방향이 원래대로 유지되는지 확인합니다. 시스템 로그는 로그인, 연결 및 기기 문제에 대한 정보를 제공하므로 정기적으로 검사하십시오. AXIS Camera Station은 발견된 많은 이상에 대한 알림을 제공하고 시스템 로그에 기록합니다. 특히 중요한 사건이 발생한 후 로그를 읽기 전용 원격 스토리지로 전달합니다. 또한 Axis는 모든 설치를 모니터링할 수 있는 온라인 시스템 상태 모니터링 기능을 Integrator Suite의 일부로 제공하여 서비스 및 유지 관리를 용이하게 합니다.

하드웨어와 소프트웨어(운영체제 및 VMS) 모두 정기적으로 업데이트해야 합니다. 항상 최신 소프트웨어 및 펌웨어 버전을 사용하여 시스템은 최신 보안 패치 및 버그 수정의 이점을 누릴 수 있습니다. 이상적으로 VMS는 모든 소프트웨어 및 펌웨어 업데이트를 자동으로 찾아 업데이트 설치를 요청하거나 자동으로 업데이트합니다. 다운로드하는 모든 소프트웨어는 신뢰할 수 있는 소스에서 가져와야 합니다.

3.3 설정된 절차에 따라 증거 처리

보안 감시 시스템의 설계 및 유지 관리에 대한 원칙을 적용했다면, AXIS Camera Station은 카메라로 포착된 사고에 대해 신뢰할 수 있는 증거를 제공할 수 있어야 합니다. 그렇다면 어떻게 진행해야 할지 정해진 절차가 있어야 합니다.

법 집행 기관의 모든 권고를 따라야 합니다. 중대한 범죄의 경우 담당 법 집행 기관은 증거 보호 방법을 결정할 권한이 있으며, 그 지시에 따라야 합니다.

다른 경우에는 증거를 안전하게 내보내는 것이 주요 과정입니다. 이는 시스템 외부에서 내부와 마찬가지로 신뢰성이 보존된 상태로 손상되지 않은 동일한 형태로 제공할 수 있다는 것을 의미합니다.

내보내기는 지정된 운영자가, 가급적이면 목격자와 함께 처리해야 합니다. 이 운영자는 신뢰할 수 있는 내보내기를 제공하고 문서화하는 목적으로만 고용된 외부 전문가일 수 있습니다. 내보내기에 독립적인 제3자를 이용하면 비디오 소유자가 증거 조작을 의심받을 위험을 최소화할 수 있습니다. 운영자는 실제 사건에 대한 비디오를 내보내야 하지만 그로 인한 사건과 여파에 대한 충분한 정보도 제공해야 합니다.

선택한 비디오 클립을 CD-R, DVD-R 또는 Blu-ray(-R)와 같은 읽기 전용 디스크로 내보내 법 집행 기관에 전달할 수 있습니다. 또는 암호화 및 패스워드로 보호된 zip 파일로 비디오 클립을 내보낼 수 있습니다. 이 파일은 사용자 패스워드로 해시된 서명을 사용하여 디지털 서명할 수 있습니다. 해시를 확정하고 파일의 현재 해시를 확인하려면 AXIS File Player에 서명을 입력해야 합니다. 해시가 일치할 경우 해당 파일에서 변경된 데이터가 없는 것입니다.

또한 Axis는 운영자를 위한 고급 내보내기 도구 기능을 하는 AXIS Camera Station Incident Report도 제공합니다. 이 도구는 사고 태그 및 내보내기 위치 등의 데이터를 제공하는 관리자가 미리 설정해야 합니다. 그러면 Incident Report가 내보내기를 자동화하여 태그를 폴더 이름으로 사용하여 사고로 구성된 비디오를 내보낼 수 있습니다. 위치는 NAS(network-attached storage) 같은 로컬 리소스나 SMB 프로토콜을 통해 액세스할 수 있는 경우 클라우드 스토리지 같은 원격 리소스로 설정될 수 있습니다. 보고서는 비디오 파일, .jpg 형식의 스냅샷(보고서를 호출할 때 운영자가 수동으로 AXIS Camera Station에서 생성), .txt 형식의 북마크, .pdf 형식의 보고서에 수집된 모든 정보로 구성됩니다.

4 사이버 보안 리소스

Axis는 기기의 설계, 개발 및 테스트에 사이버 강화를 적용하여 공격에 이용될 수 있는 결함의 위험을 최소화합니다. 당사는 보안 취약성 관리, 안전한 데이터 전송 및 저장 요구 사항, 암호화에 관한 사이버 보안 업계 모범 사례를 준수합니다. 당사는 고객이 적절한 보안 제어를 쉽고 비용 효율적으로 적용할 수 있도록 노력하고 있으며 당사의 기기는 암호화 및 보안 관리를 지원합니다.

시스템 제조업체이자 공급업체인 Axis는 가장 완벽하고 안전한 시스템 또는 솔루션을 제공하기 위해 최선의 노력을 기울이고 있지만, 최종 사용자에게는 보안 모범 사례를 적용할 큰 책임이 있습니다. Axis는 도움이 되는 몇 가지 도구, 가이드, 튜토리얼을 제공합니다. www.axis.com/cybersecurity에서 강화 가이드, 보안 관리 정보 및 사이버 보안에 관한 블로그 게시물 등을 참조하십시오.

T10169774/KO/M1.2/2107

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