백서

물리적 접근 제어의 디지털화 및 사이버 보안

기업이 접근 제어의 잠재력을 최대한 발휘하고 더 스마트하고 안전한 세상을 만들 수 있도록 하는 시스템 및 프로토콜 탐색

8월 2021

AXIS COMMUNICATIONS

목차

1 요약

클라우드 연결의 발전은 물리적 보안 산업의 면모를 변화시키고 있으며 설치업체가 비즈니스를 유지하기 위해 적응하도록 하고 있습니다. 접근 시스템의 제어는 글로벌 기술 회사의 영역으로 이동하는 것으로 보이며, 시스템이 점점 더 지능적이고 확장 가능하며 에지 기반이 됨에 따라 시스템 자체에서 더 큰 가치를 기대하게 됩니다.

다른 기업 시스템과 통합될 가능성과 더불어 이러한 진화는, 특히 기존 인프라를 기반으로 구축되는 경우 시스템 개발 및 배포에서 사이버 보안이 훨씬 더 큰 역할을 해야 함을 의미합니다. 시리얼 아키텍처, MAC 주소 부재 등과 같은 기술적 장벽을 극복하는 것은 현재와 미래의 요구사항을 충족할 수 있는 디지털 접근 제어 시스템으로 전환하는 데 중요한 단계입니다.

접근 제어를 위한 디지털 시스템을 구현하고 보호하는 것은 최상의 보안을 보장하기 위해 모범 사례를 따르는 것을 의미합니다. 장치, 공급업체 또는 프로토콜 등 시스템과 관련된 모든 구성 요소를 평가하고 테스트해야 합니다. 이 모든 것은 믿을 수 있고 신뢰할 수 있어야 합니다. 또한 위협 환경과 새로 발견된 취약점 및 결함으로 인한 위험을 완화하는 방법을 지속적으로 인식해야 합니다.

특히 공급업체는 장치를 네트워크에 연결할 수 있으므로 특별히 고려해야 합니다. 진지한 공급업체는 예를 들어 강화 가이드를 게시하고, 네트워크 장치를 더 쉽게 관리하고 보호할 수 있도록 하는 전용 관리 도구를 제공함으로써 자사의 제품 및 서비스를 보호하기 위한 자체 프로세스를 제공하고 알려야 합니다. 또한 공급업체는 발견된 취약점과 결함을 관리하기 위한 전략에 대해 되도록 개방적이고 정직해야 합니다.

2 서론: 접근 제어의 미래

클라우드 연결은 물리적 보안 업계에 시스템을 배치하고 활용하는 방법에 대한 새로운 비전을 제시했습니다. 최종 사용자와 구매자는 기존의 레거시 기술을 훨씬 능가하는 보안 감시 및 액세스 제어 기능을 갖춘 보다 스마트하고 통합된 비즈니스 중심 솔루션을 요구하고 있습니다.

많은 공급업체가 물리적 보안에 대한 전문 지식, 서비스 및 지식을 중심으로 강력한 비즈니스 모델을 구축했습니다. 그러나 네트워크 연결과 IoT는 시장 변화에 적응하고 관련성을 유지하기 위해 개방형 플랫폼, IP 연결 및 소프트웨어 통합과 같은 물리적 보안의 전통적인 공급업체와 설치 관리자가 IT 언어를 배워야 합니다.

통제권이 전자 액세스 시스템 공급업체에서 글로벌 기술 회사로 빠르게 이동하고 있는 것 같습니다. 이제 글로벌 기술 회사는 기존 운영에 도전하는 방향으로 보안을 형성할 수 있는 힘을 갖게 되었습니다. 스마트 빌딩과 스마트 시티는 커다란 기회를 제공하며, 배포 용이성과 오늘날 기술의 정교함이 스마트 환경에 많은 이점을 제공함에 따라 많은 사람들이 현대식 접근 제어 시장의 급속한 성장을 예상하고 있습니다.

기술 대기업의 영향이 클라우드 기술의 성공을 입증하면서 호스팅 접근 제어를 수용하려는 움직임이 나타난 것은 놀라운 일이 아닙니다. 전 세계적으로 COVID-19 팬데믹 기간 동안 기술 대기업에 너무 많이 의존했습니다. 그러한 기업은 급진적인 변화를 가져올 수 있는 범위, 규모 및 상상력을 가지고 있으며, 기업들이 클라우드의 가치를 깨닫고 모든 보안 및 비즈니스 요구사항을 충족하기 위해 호스팅된 솔루션을 찾음에 따라 물리적 보안도 변화될 것입니다.

그러나 현재 많은 제조업체가 이러한 변화하는 시장에 대한 준비가 되어 있지 않고 여전히 경직된 고유한 설계를 기반으로 하는 비즈니스 모델을 따르고 있습니다. 이러한 전통적인 접근 방식과 직접적으로 대조되는 방식으로 스마트한 물리적 보안 솔루션으로 전환하는 추세이며, 이는 강력한 도전을 받을 수 있습니다. 변화가 하루아침에 일어나지도 않고 새로운 클라우드 호스팅 솔루션이 아직 주류가 되지도 않았지만, 이 유망한 새로운 세상은 지금 우리 업계에 합류하는 새로운 엔지니어의 영역입니다.

따라서 접근 제어의 미래와 전체적인 물리적 보안은 더 큰 가치에 대한 기대에 기반할 것입니다. 접근 제어 시스템은 데이터 수집 지점이 될 것이며 도어 컨트롤러는 지능형 I/O 장치가 될 것입니다. 방문자 관리를 위한 QR 코드와 마찰 없는 접근 제어를 위한 생체 얼굴 인식은 카메라 또는 센서의 분석으로 에지에서 점점 더 많이 관리될 것입니다. 접근 제어의 미래는 이를 수용하고 형성하는 데 도움을 줄 준비가 된 사람들에게 흥미롭고 도전적인 시간을 제공합니다. 이는 더 스마트하고 안전한 세상을 위해 혁신할 수 있는 진정한 기회입니다.

이 백서에서는 이러한 시스템의 많은 기본 기능을 포함하여 특히 접근 제어와 관련된 측면을 살펴봅니다. 또한 최종 사용자를 위한 정보 및 제안과 함께 공급업체를 위한 모범 사례를 둘러싼 고려 사항을 살펴볼 것입니다. 이는 최종 사용자에게 자신의 공급업체에 도전하고 더 현명한 구매 결정을 내릴 수 있는 자신감을 제공하기 위한 것입니다.

3 진화하는 접근 제어 시장의 과제

물리적 접근 제어 시스템(PACS)에 초점을 맞출 때, 물리적 진입 허용 또는 차단과 관련된 고려 사항의 관점에서 위험 요소를 다루는 경향이 있습니다. 물리적 접근 제어 시스템 설계에 대해 균형 잡힌 접근 방식을 취하는 것은 잠재적 위협 평가에 기반한 중요한 고려 사항입니다.

오늘날에는 점점 더 정교한 전자 접근 제어 솔루션으로 구내가 보호되고 있기 때문에 이러한 시스템은 기업 전체에 걸쳐 접근을 빠르고 효율적으로 관리할 수 있는 방법을 제공하여, 필요한 경우 검사 및 모니터링할 수 있는 디지털 발자국을 남길 뿐만 아니라 HR 및 방문자 관리와 같은 다른 시스템과 완전히 통합됩니다.

이러한 시스템 통합은 비즈니스 및 보안 의사 결정을 지원하고 접근을 제어하는 강력한 통찰력을 제공하므로, 시스템의 사이버 성숙도를 철저히 평가하는 것이 중요합니다. 범죄자가 점점 더 정교해지고 위협 환경이 계속 진화함에 따라, 복제된 접근 자격 증명, 내부 위협 또는 원격으로 실행되는 사이버 공격의 위험을 완화하는 것이 과제입니다.

그러나 아키텍처 자체가 문제를 제기합니다. 많은 기존 접근 제어 시스템은 오래된 인프라를 기반으로 구축됩니다. 이러한 인프라를 일반적으로 활용하는 보안 기술이 융합하는 경우, 벤더의 과제는 부분적으로 하드웨어를 이러한 기업 네트워크에 연결하도록 조정하고, IT 보안의 중요성과 기업에 제기된 많은 위험을 철저히 평가하고 보호할 필요성을 유발하는 보안 환경의 변화를 인식하는 것입니다.

사이버 보안 고려 사항은 새로운 보안 시스템 개발의 핵심 요소가 되어야 합니다. 접근 제어 기술은 모든 물리적 보안 솔루션에서 필수적인 역할을 하므로 인정된 사이버 보안 원칙, 사고 보고 및 모범 사례에 따라 제조되어야 합니다. 시스템의 무결성은 가장 약한 링크 만큼만 강력하다는 것을 인정하는 것이 중요합니다. **이를 수용할 준비가 되어 있지 않은 시스템은** 잠재적 노출 위험을 구성합니다. 공개적으로 인정된 복구 조치를 수락하고, 알리고 실행할 준비가 되어 있음을 입증할 수 없는 경우, 이는 궁극적으로 배치된 필요한 수준의 물리적 보안을 제공하는 능력에 부정적인 영향을 미칠 것입니다.

3.1 사이버 보안 자격 증명(사이버 성숙도)

IT 산업의 참여가 증가하면서 기술의 평가, 배포 및 유지 관리되는 방식이 변화하고 있습니다. IT 이해 관계자에 대한 주요 고려 사항은 벤더 사이버 보안 지식에 중점을 두고 비즈니스 사이버 보안 자격 증명을 평가하는 것입니다. 이 지식은 사이버 성숙성이라고도 합니다. 사이버 성숙성은 위협 지형 및 위험 완화를 양호하게 이해하고 있음을 나타내는 것입니다. 네트워크 카메라용으로 이미 개발된 광범위한 사이버 보안 문서 및 지침은 사이버 위험 및 공격 가능성의 문제, 평가 및 설명이 이러한 제품에도 동등하게 관련되기 때문에 물리적 접근 제어에도 적용될 수 있습니다.

3.2 보안 시스템 아키텍처의 미래

최신 접근 제어 장치는 네트워크 케이블과 RJ45 커넥터를 통해 연결됩니다. 네트워크는 장치와 중앙 관리 시스템 간의 통신은 물론 접근 제어 장치에 전원을 제공합니다. 접근 제어의 원동력은 TCP/IP 기반 시스템으로의 전환입니다. 2013년 최초의 진정한 IP 지원 도어 컨트롤러(AXIS A1001)가 출시된 이후로 PACS는 계속해서 발전해 왔으며, 이제는 레거시 기술에만 의존해서는 불가능했을 광범위한 고급 기능을 제공합니다.

이러한 혁신의 예로는 터치 없는 접근 제어를 용이하게 하는 QR 코드 리더, 네트워크 카메라와의 통합을 통한 안면 인식, 번호판 판독이 있으며, 이러한 예는 모두 PACS 데이터베이스와 상호 작용하여 출입 허가 또는 거부에 대해 에지 기반 결정을 내릴 수 있습니다. IP 시스템의 주요 이점은 간단한 구성 및 장치 관리를 통한 낮은 설치 비용입니다. 다른 장치와 손쉽게 통합할 수 있다는 것은, 새로운 보안 기술과 향상된 기능을 사용할 수 있게 되면 그러한 기술과 기능을 플러그 앤 플레이 방식으로 간단히 연결할 수 있도록 하는 미래 지향적인 솔루션을 의미합니다.

3.3 IP vs. 기존 접근 제어

IP의 장점은 새롭고 현대적인 접근 제어 설계에서, 특히 최종 사용자가 표준으로 기대하는 비접촉 시스템에서 실현될 것입니다. 또한 사용자는 접근 제어가 모바일 자격 증명뿐만 아니라 스마트폰 및 태블릿 사용에 맞게 조정되는 것을 보고 싶어할 것입니다. 업계가 어떻게 더 우수하고 유용하며 시간/비용을 절약하는 접근 제어 시스템을 제공할 수 있을까요? 또한 대기업이 주도하는 혁신 주기에 업계가 보조를 맞출 수 있을까요? 이는 업계의 공급업체 측에서 해결해야 할 과제입니다.

지금까지 이러한 기회는 활용되지 않았습니다. 이는 레거시 접근 제어 시스템이 시리얼 아키텍처에 설치된 도어 컨트롤러에 의존하고 RS-485 케이블을 통해 중앙 장치 또는 서버에 연결되기 때문일 수 있습니다. 대부분의 시스템은 또한 독점적입니다. 즉, 도어 컨트롤러는 공급업체가 지정한 소프트웨어를 통해서만 관리할 수 있도록 '잠겨' 있습니다. 이는 최종 사용자를 단일 하드웨어 및 소프트웨어 공급업체로 제한하고, 이러한 시스템의 복잡성으로 인해 설치 및 구성을 위한 전문 인력이 필요한 경우가 많습니다.

기존 접근 시스템을 확장할 때 일반적인 중앙 제어 장치가 특정 수의 도어를 수용하도록 설계되었다는 사실로 인해 프로세스가 복잡해지며, 비표준 구성은 제한된 시스템 유연성으로 인해 높은 비용을 발생시킵니다. 예를 들어, 도어를 하나만 추가하면 비용이 훨씬 더 많이 들어 도어 추가 비용이 너무 많이 들 수 있습니다.

IP 네트워크는 훨씬 더 뛰어난 유연성과 사용자 정의를 통해 훨씬 간단하고 설치하기 쉬운 PACS 아키텍처를 도입할 수 있게 해주었습니다. IT 전문가는 진정한 IP 장치 그리고 네트워크 기반 접근 제어 시스템에서 IP 장치를 사용하는 것을 매우 선호합니다. 이러한 인력은 확장 비용을 절감하는 데

핵심적인 역할을 하며 향후 접근 제어 설계의 요구 사항이 될 것이기 때문에 향후 설계 프로세스에 포함시키는 것이 중요합니다.

3.4 개방형 프로토콜

접근 제어의 미래는 개방형 프로토콜 포럼에서 자신의 기술과 능력을 공유하려는 제조업체의 의지에 달려 있습니다. 많은 접근 시스템 개발자가 최종 사용자를 자신의 솔루션에 연결하여 미래의 수익을 보장하는 프로세스를 선호하는 것처럼 보이기 때문에 이러한 개방성에 대한 저항이 있는 것은 당연합니다. 그러나 이 접근 방식에는 장기적인 가치가 없습니다. 사용자는 솔루션에서 더 많은 것을 요구하고 있으며 이를 위해 기꺼이 데이터를 공유합니다.

시스템 설계자와 접근 하드웨어 공급업체는 포괄적인 물리적 보안 시스템의 일부로 사용자가 요청하는 모든 솔루션을 제공할 수 있는 리소스나 IT 노하우를 거의 갖고 있지 않습니다. 많은 기업이 비즈니스 모델과 접근 제어 시장에서 자신의 입지를 위협하는 혁신적인 새로운 솔루션으로 인해 자신의 제품이 빠르게 사라지고 있다는 사실을 진정으로 인식하지 못하는 것 같습니다. 최신 시스템의 기능과 현대적인 혁신의 속도 덕분에 이제 접근 제어 장치가 거의 필요하지 않습니다. 지능형 I/O 장치가 확실한 대체품이 되었습니다.

개방성을 통해 벤더는 소규모 접근 시스템에 적합한 장치를 구축할 수 있습니다. 이러한 장치는 단순성이 핵심이고 구매 및 설치 비용이 경쟁력이 있어야 합니다. 그런 다음 이러한 동일한 장치를 필요에 따라 더 크고 기술적으로 복잡한 작업에 맞게 조정할 수 있습니다. 이러한 유연성은 현대 보안의 특징이며, 현재 구입한 시스템이 사용자의 비즈니스가 성장하고 요구사항이 변경됨에 따라 미래에도 여전히 관련성이 있을 것임을 보장합니다.

개방성과 개방형 기술에 대한 자세한 내용은 개방형 표준을 지향하는 개발을 추진하기 위해 설립된 산업 기관인 ONVIF 웹사이트 *www.onvif.org*에서 찾을 수 있습니다.

4 채택에 대한 기술적 장벽

디지털 접근 제어를 가능하게 하는 기술적 연결, 인터페이스 및 장치 측면에서 고려해야 할 사항이 많습니다. 기존 시스템에서 클라우드 지원 시스템으로 이동한 결과로 인한 영향이 나타날 수 있습니다. 다음 섹션에서는 기존 기술과 관련 프로세스에 도움이 되고, 새로운 솔루션을 업그레이드하고 수용하는 데 장애가 되지 않도록 하기 위해 고려해야 하는 사항에 대해 자세히 설명합니다.

4.1 RS-485 컨트롤러

한 가지 고려 사항은 RS-485 컨트롤러의 배치, 그리고 MAC(미디어 접근 제어) 주소를 거의 소유하지 않아 식별하기 어려운 반지능형 장치를 설치할 잠재적 위험입니다. TIA-485(-A) 또는 EIA-485라고도 하는 RS-485는 시리얼 통신 시스템에서 사용하기 위한 드라이버 및 수신기의 전기적 특성을 정의하는 표준입니다. 전기 신호가 균형을 이루고 멀티포인트 시스템이 지원됩니다. 그러나 RS-485는 물리 계층, 즉 제너레이터와 리시버만 지정합니다. 중요한 통신 계층을 제어하지 않습니다.

MAC 주소가 없거나 시리얼 아키텍처를 채택한다고 해서 접근 제어 시스템의 작동 신뢰성 문제가 발생하거나 접근 제어 시스템의 운영에 해로운 영향을 주는 것은 아닙니다. 이러한 설계는 30년 이상 접근 제어의 핵심이었습니다. 그러나 접근 제어 시스템의 모든 제어 장치가 지능적이고 개별적으로 처리되

지 않는다면 보안 기대치의 발전을 시각화하기가 어렵습니다. 우리는 완전히 지능적인 시스템과 완전히 접근 가능한 장치만이 기대되는 미래 가치를 제공할 수 있다고 가정합니다. '완전히 접근 가능'하다는 것은 사이버 보안이 취약한 장치를 의미하는 것이 아니라 그 반대입니다.

4.1.1 OSDP(Open Supervised Device Protocol)

IEC에서 승인하고 접근 통신의 보안을 강화할 수 있는 가능성을 제공하는 새로운 통신 방법은 OSDP(Open Supervised Device Protocol: 개방형 관리 장치 프로토콜)입니다. 이는 접근 제어 및 보안 제품 간의 상호 운용성을 향상시키기 위해 SIA(Security Industry Association: 보안산업협회)에서 개발한 접근 제어 통신 표준입니다. OSDP는 128비트 암호화를 사용하고 멀티드롭 설치를 지원하며 연결을 감독하여 리더 문제를 보고합니다. 주목해야 할 추가 사항은 OSDP가 이전에 필수였던 도어당 다중 연결이 아니라 오직 2개의 와이어를 사용하여 카드 리더, 도어 스트라이크, 알람 접점 및 종료 요청 기능을 지원한다는 것입니다. SIA 웹사이트에서는 다음과 같이 보고합니다. 'OSDP는 2020년 5월 국제전기기술위원회(International Electrotechnical Commission)의 국제 표준으로 승인되었으며 2020년 7월 IEC 60839-11-5로 발표될 예정입니다. SIA OSDP는 업계 최고의 위치를 유지하기 위해 지속적으로 개선되고 있습니다.'

4.2 MAC 주소가 있는 장치의 가치

MAC 주소는 단일 네트워크 어댑터 또는 장치의 전역적으로 고유한 하드웨어 주소입니다. IT 네트워킹과 관련하여 MAC 주소는 IP 주소만큼 중요합니다. MAC 주소는 LAN에서 컴퓨터를 고유하게 식별하며 TCP/IP와 같은 네트워크 프로토콜이 작동하는 데 필요합니다. MAC 주소는 장치에 하드코딩되어 있으며, 운영 체제를 통해 스푸핑할 수 있지만, 이는 물론 바람직하지 않으며 주소는 보안 솔루션으로 보호해야 합니다.

TCP/IP 및 기타 주류 네트워크 아키텍처는 일반적으로 네트워크 기능이 계층으로 세분화되는 OSI(Open Systems Interconnection) 모델을 채택합니다. MAC 주소는 데이터 링크 계층(OSI 모델의 계층 2)에서 작동하며 컴퓨터가 네트워크에서 고유하게 식별할 수 있도록 합니다. MAC 주소 필터링은 추가 보안 계층을 추가합니다. 장치가 네트워크에 연결되도록 허용하기 전에 라우터는 승인된 주소 목록과 장치의 MAC 주소를 확인합니다. 클라이언트 주소가 라우터 목록에 있으면 액세스가 허용되고, 그렇지 않으면 액세스가 거부됩니다.

4.2.1 PoE(Power over Ethernet)

PoE는 애플리케이션 간에 일관된 두 가지 이점인 비용 절감 및 장치 배치의 유연성을 제공합니다. PoE는 동일한 케이블로 데이터와 전원을 모두 전달하므로 기존 설계에 비해 장치 아키텍처를 단순화할 수 있습니다. 많은 접근 제어 시스템이 IP 연결 시스템이라고 홍보된다는 점은 주목할 가치가 있습니다.

5 모범 사례의 특징

접근 제어 관리는 사람의 흐름을 효과적으로 처리하고 접근을 통제하는 중요한 구성 요소입니다. 기업은 개선된 고객 서비스 관계와 높은 수준의 보안 및 안전을 항상 제공하기 위해 도어를 잠그거나 장벽을 세우는 것보다 훨씬 더 나은 제어 옵션이 필요합니다. 포괄적인 접근 제어에 대한 모범 사례 접근 방식을 채택하는 것은 올바른 도구를 선택하는 것을 뛰어넘는 것입니다. 이는 올바른 아키텍처

를 갖추고, 고품질 기술을 통합하고, 올바른 절차와 프로토콜을 따르고, 직원과 이해 관계자에게 올바른 태도와 행동을 취하도록 권장하는 것과 관련된 것입니다.

5.1 이해관계자 관리 및 통합 보안 접근 방식

기술 환경이 동일한 인프라에 걸쳐서 통합되어 이러한 사이트가 원활하게 작동하는 데 필요한 운영 기술을 제공하므로, 통합된 의사 결정 프로세스도 필요합니다. 우리는 이미 통합 보안 접근 방식이 벽을 허물고 서로 다른 비즈니스 팀이 협력할 수 있도록 하는 성공적인 예를 보았습니다. 이러한 통합이 기존의 전자적 및 물리적 보안 제품이 기업 네트워크에 나란히 존재하는 오늘날처럼 그 어느 때보다 더 중요한 적은 없었습니다.

물리적 보안 팀은 운영 요구사항을 지원하고 관련 위험을 해결하는 동시에 IT 보안 정책을 지원하고 물리적 장치가 기업 네트워크의 백도어가 되지 않도록 하는 기술에 의존할 수 있어야 합니다. 모든 이해관계자가 협력하여 안전한 사이버 및 물리적 환경을 만들 수 있습니다.

5.2 파트너, 벤더 및 공급업체에 기대할 수 있는 사항

타사 자신이 수행하는 모든 작업의 선두에서 보안 모범 사례를 유지하는 것의 중요성을 이해하고 특정 요구 사항을 충족하도록 운영하는 것이 중요합니다. 제3자와의 관계는 건전한 공급망을 구축하고 강력하고 신뢰할 수 있는 유대를 형성하기 위한 열쇠입니다.

타사를 평가할 때의 주요 고려 사항 및 이러한 고려 사항이 공급망에 미치는 영향:

- 사이버 보안과 관련된 위험을 이해하고 인식하는가
- 사용 가능한 프로세스와 도구로 성숙한 사이버 보안 접근 방식을 입증할 수 있는가
- 규제와 법률이 자사 제품에 미치는 영향을 이해하는가
- 사용자의 규정 준수 요구 사항을 어떻게 지원할지 입증할 수 있는가
- 사이버 보안은 단순한 기술이 아닌 프로세스이므로, 사용자의 기업을 보호하기 위해 사이버 보안 라이프사이클 관리를 실증할 수 있는가.

5.3 보안 관리: 거버넌스 및 벤더 프로세스

모든 효과적인 보안과 마찬가지로 사이버 보안도 방어의 깊이와 관련되어 있습니다. 사이버 보안은 선택한 제품 및 파트너에서 요구 사항 모음에 이르기까지 모든 수준에서 IP 카메라 네트워크를 적절하게 보호하는 것에 관한 것입니다.

5.3.1 표준 및 지침

ISO 27001 – Information Security Management(정보 보안 관리) ISO/IEC 27001은 다음을 요구하는 보안 관리 시스템입니다.

- 위협, 취약성 및 영향을 고려하여 조직의 정보 보안 위험에 대한 체계적인 조사

- 수용할 수 없는 것으로 간주되는 위험을 해결하기 위한 일관성 있고 포괄적인 정보 보안 제어 및/또는 기타 형태의 위험 관리(예: 위험 회피 또는 이전)의 설계 및 구현
- 정보 보안 제어가 조직의 정보 보안 요구사항을 지속적으로 충족할 수 있도록 하기 위한 전반적인 관리 프로세스의 채택.

5.3.2 Cyber Essentials Plus

Cyber Essentials는 조직이 일반적인 온라인 위협으로부터 스스로를 보호할 수 있도록 돕기 위해 정부가 후원하고 업계에서 지원하는 제도입니다. Cyber Essentials는 사이버 보안이 제기하는 문제를 이해하는 기업을 위한 효과적인 지표이며 기업의 정책 및 프로세스에 대한 평가입니다. 구체적으로 다음을 살펴봅니다.

- 보안 구성
- 접근 제어 및 관리
- 맬웨어 보호
- 패치 관리
- 방화벽 및 인터넷 게이트웨이

기술 제조업체의 경우 첫 번째 방어선은 자체 시스템과 관련된 위험을 완화하는 것입니다. 2014년 10월 1일부로 정부는 특정 민감한 개인 정보의 취급과 관련된 계약에 입찰하는 모든 공급업체에 Cyber Essentials 제도에 따라 인증을 받을 것을 요구했습니다.

5.3.3 설계에 의한 보안, 기본에 의한 보안

2019년 감시 카메라 위원회(Surveillance Camera Commissioner)가 시작한 **Secure by Design, Secure by Default(설계에 의한 보안, 기본에 의한 보안)**는 감시 카메라 시스템 및 구성 요소 제조업체에 대한 최소 요구사항을 설정합니다. 이 기준은 제조업체가 증상을 처리하기보다는 근본 원인에서 보안 문제를 해결하기 위해 전체적인 접근 방식을 취할 것을 요구합니다. 즉 시스템이나 구성 요소 유형에 대한 전반적인 피해를 줄이기 위해 규모를 갖춰 대응할 것을 요구합니다.

Secure by Design, Secure by Default는 올바른 보안 기본 요소가 소프트웨어 및 하드웨어에 구축되도록 하기 위한 장기적인 기술적 노력을 다룹니다. 또한 시장에서 쉽게 채택할 수 있는 방식으로 이러한 기본 요소를 사용할 수 있도록 하는 동등한 요구 작업을 다룹니다.

기술을 지원하기 위해 Axis는 국가 사이버 보안 전략 행동 강령(National Cybersecurity Strategy code of conduct)에 따라 Secure by Design, Secure by Default를 다음에 적용했습니다.

- 패스워드 프롬프트
- 패스워드 강도 표시기
- HTTPS 암호화
- 802.1x
- 원격 액세스 비활성화(NAT 통과)

6 가이드 및 도구(벤더 프로세스)

네트워크 보안과 관련하여 조직은 종종 단일 장애 지점 및 노출 지점을 제한하는 데 도움이 되는 '계층화된 방어' 접근 방식을 만들기 위해 여러 기술 제어를 배치합니다. 그러나 종종 간과되는 중요한 프로세스 중 하나는 '시스템 강화'입니다. 여기에는 정보 보안 위협으로부터 시스템을 더 안전하게 보호하기 위해 기본 시스템 설정의 구성을 변경하는 작업이 포함될 수 있습니다. 또한 이 프로세스는 모든 시스템에 존재하는 내재된 취약점의 양을 줄이는 데 도움이 됩니다.

6.1 제조 강화 가이드

네트워크에 연결된 모든 장치를 위한 시스템 강화 프로세스가 있어야 합니다. 여기에는 워크스테이션, 서버 및 기타 네트워크 장치가 포함됩니다. 각 제조업체는 자신의 시스템 설정과 구성을 누구보다 잘 알고 있으므로, 파트너와 사용자에게 장치의 무결성과 최종 사용자의 설치를 보호하는 데 필요한 정보를 제공하는 것은 제조업체의 책임이어야 합니다. 강화 가이드는 영상 감시 솔루션 배포와 관련된 모든 사람에게 기술적인 조언을 제공해야 합니다. 강화 가이드는 기본 구성을 설정해야 하고, 진화하는 위협 환경을 처리하는 것에 대한 포괄적인 정보를 제공해야 합니다.

모든 벤더는 장치의 설계, 개발, 테스트에 사이버 보안 모범 사례를 적용하여 공격에서 악용될 수 있는 결함의 위험을 최소화하기 위해 최선을 다해야 합니다. 그러나 네트워크, 네트워크 장치 및 네트워크가 지원하는 서비스의 보안을 유지하려면 전체 벤더 공급망과 최종 사용자 조직이 적극적으로 참여해야 합니다. 보안 환경은 사용자, 프로세스 및 기술에 따라 달라집니다. 좋은 강화 가이드는 CIS Controls-Version 6.1과 같은 기준의 사용을 따라야 합니다. 이러한 제어는 이전에 SANS Top 20 Critical Security Controls로 알려져 있었습니다.

6.2 장치 관리

장치 관리자는 연결된 장치를 관리하는 간단하고 비용 효과적이며 안전한 방법을 제공하는 구내 도구입니다. 장치 관리자는 설치업체와 시스템 관리자가 모든 주요 설치, 보안 및 유지보수 작업을 매우 효과적으로 관리할 수 있는 도구입니다.

장치 재고/자산 관리 시스템:

- 계정 및 패스워드 정책
- 펌웨어 업그레이드 및 애플리케이션의 효율적인 설치
- 사이버 보안 제어 적용 - HTTPS 관리 및 IEEE 802.1x 인증서 업로드, 계정 및 패스워드 관리
- 인증서 수명 주기 관리 - 모든 주요 설치, 보안 및 운영 작업 관리
- 간편하고 신속하게 새로운 장치 구성 - 설정 백업 및 복구
- 모든 규모의 사이트에 적합 - 단일 또는 다중 사이트 설치

6.3 OEM/ODM과 관련된 과제

OEM(Original Equipment Manufacturer)은 자신의 이름과 브랜드로 다른 회사의 제품을 재판매하는 제조업체입니다. ODM(Original Design Manufacturer)은 판매를 위해 다른 회사가 사양을 지정하고 최종적으로 브랜드화한 제품을 설계 및 제조하는 회사입니다. 이러한 회사는 브랜드 회사가 공장을 시작하거나 운영하지 않고도 생산에 참여할 수 있도록 합니다.

다른 공급업체에 제품 OEM 또는 ODM을 위탁하는 제조업체에는 많은 장점이 있습니다. 첫 번째는 제조 위험과 비용을 제거하고 조직이 판매 및 마케팅 프로세스에 집중할 수 있다는 것입니다. 이것이 보안 업계의 많은 카메라 제조업체가 자사 브랜드 제품을 OEM 또는 ODM을 통해 생산하는 주요 이유 중 하나입니다.

이는 몇 가지 과제를 제시하며 가장 분명한 것 중 하나는 사이버 보안입니다. 한 제조업체의 제품에 취약점이 있는 경우 이는 공급망 전체의 다른 모든 리셀러 및 파트너에게 영향을 미칠 수 있습니다. 또한 공급망의 완전한 가시성을 매우 어렵게 만들 수 있습니다. 운영 중인 OEM 및 ODM의 수가 많기 때문에, 실사를 따르고 특정 제조업체의 기술을 거부한 최종 사용자는 무의식적으로 해당 기술을 브랜드 이름을 변경한 형태로 사용하게 되지만 사실을 전혀 인식하지 못할 수 있습니다.

6.4 CPU 마이크로프로세서 칩

장치에 설치된 일반 CPU 처리 칩이 많은 취약점이 식별되어 해커의 표적이 되고 있습니다. 이에 대한 주요 이유 중 하나는 식별된 단일 취약점에서 생성되는 확장성입니다. 최근의 예로는 권한 없는 코드를 사용하여 데이터에 불법적으로 액세스할 수 있는 능력이 있는 최신 CPU 마이크로프로세서에 대한 두 가지 관련 사이드 채널 공격인 '멜트다운(Meltdown)' 및 '스펙터(Spectre)' 결함이 있습니다.

스마트폰에서 데이터 센터의 하드웨어에 이르기까지 대부분의 장치는 어느 정도 취약할 수 있습니다. 주요 운영 체제 공급업체는 문제를 완화하는 패치를 만들었지만, 일부 패치는 플랫폼별 요소가 포함되어 있으므로 장비 제조업체(OEM)를 통해 설치해야 합니다. The National Cybersecurity Centre(NCSC)는 최대한 빨리 장치를 패치할 것을 권고합니다.

6.5 펌웨어 전략

Signed Firmware는 최종 사용자에게 중요하며 물류 및/또는 배포 과정을 통해 장치가 변조될 수 있는 일부 잠재적 위험을 완화합니다. 해시라고도 하는 서명은 배포 시 펌웨어에 추가됩니다. 프로세서는 자체 해시를 계산하고 신뢰하는 인증서로 서명된 것과 일치하는 해시가 있는 펌웨어 이미지만 로드합니다.

6.6 취약성 관리

사이버 범죄 및 관련 위험의 지속적인 성장으로 인해 많은 조직이 정보 보안에 더 집중해야 합니다. 취약성 관리 프로세스는 조직이 정보 보안 위험을 통제하기 위해 기울이는 노력의 일부여야 합니다. 이 프로세스를 통해 조직은 IT 환경의 취약성과 이와 관련된 위험을 지속적으로 파악할 수 있습니다. IT 환경의 취약점을 식별하고 완화해야만 공격자가 네트워크에 침투하여 정보를 훔치는 것을 방지할 수 있습니다.

공급업체는 모든 시스템의 취약점을 감지 및 수정하고 변경 프로세스 및 새 시스템 배포 중에 도입되는 새로운 취약점을 방지하는 프로세스를 포함하여 운영에서 취약점 관리가 다루어지도록 하는 것이 중요합니다. 공급업체가 수용하는 위험과 관련된 모든 문제는 최종 사용자와 소통하고 합

의해야 합니다. 이 원칙이 구현되지 않으면 공격자는 시스템 내의 취약성을 이용하여 기업과 공급업체에 사이버 공격을 수행할 수 있습니다.

IT 보안 패치 및 보안 취약성 업데이트는 보안 침해를 방지하기 위해 적시에 승인된 프로세스를 통해 설치되어야 합니다. 어떤 이유로든 업데이트할 수 없는 공급업체 시스템은 취약한 시스템을 보호하기 위한 조치를 구현해야 합니다. 모든 변경은 공급업체의 변경 관리 프로세스에 따라 수행되어야 합니다.

6.7 보안 권고 알림

보안 권고는 알려진 취약점으로 인한 위험을 줄이는 데 도움이 됩니다. 보안 권고는 공식 CVE(Common Vulnerability and Exposure) 또는 기타 취약점 보고서를 참조할 수 있으며 여기에는 취약점 설명, 위험 평가, 권장 사항 및 서비스 릴리스가 제공되는 시기에 대한 정보가 포함됩니다. 대부분의 공급업체는 간접 판매 모델을 구현하고 파트너 프로그램을 갖추고 있습니다.

보안 권고 알림(Security Advisory Notifications)을 사용하면 제조업체의 파트너 프로그램에 등록되지 않은 고객이 관련 사이버 보안 알림을 가능한 한 빨리 받을 수 있으며 채널과 통신할 때 얻을 수 있습니다. 이것은 장비가 설치되어 있지만 원래 설치를 수행한 회사와 계약을 체결하지 않은 최종 사용자를 위한 중요한 도구입니다.

6.8 Building Security in Maturity Model(BSIMM)

BSIMM은 조직이 소프트웨어 보안을 다른 계획과 비교하고 현재 상태를 확인할 수 있도록 지원하기 위해 마련된 소프트웨어 보안 측정 기준입니다. BSIMM은 다음과 같은 프로세스, 활동, 역할 및 책임을 평가하는 데 도움이 됩니다.

- 설계 및 아키텍처 검토
- 코드 검토
- 알려진 취약점 테스트
- 오픈 소스 패키지에서 CVE 취약점을 찾을 수 있는 표준 취약점 스캐닝 도구 실행

6.9 장기 지원(LTS)

LTS(Long Term Support)는 표준 버전보다 더 오랜 기간 동안 안정적인 소프트웨어 릴리스를 유지하는 제품 수명 주기 관리 정책입니다. LTS 펌웨어에는 안정성, 성능 및 보안을 위한 패치만 포함되어야 합니다. 공급업체는 장치가 시장에 출시된 후 최대 10년 동안 LTS 펌웨어를 제공합니다.

LTS는 기존의 활성 소프트웨어 지원과 병행하여 존재하겠지만, 독립적으로 존재할 것으로 예상됩니다. LTS 지원의 주요 이점 중 하나는 원래 펌웨어 버전과 관련된 타사와의 통합을 유지한다는 것입니다.

6.10학습 및 협업

기술 공급업체를 선택할 때 고려해야 할 주요 영역 중 하나는 기술 공급업체가 제공하는 교육 및 지원입니다. 특히 사이버 보안과 관련하여 채널과 산업이 직면한 문제가 진화함에 따라, 제조업체

는 사전에 문제를 해결하고 시장에 부수적인 정보 및 콘텐츠를 제공해야 합니다. 잠재적인 예에는 다음이 포함됩니다.

- 사이버 보안에 대한 무료 강의실 교육 과정
- 온라인 사이버 보안 교육
- 온라인 사이버 보안 간편 테스트
- 보안 강화 가이드
- 취약점 정책
- 사이버 보안 모범 사례
- 사이버 보안 개념 및 용어

7 사이버 예방 조치 프로파일 생성: 다음 단계 및 고려 사항

우수한 사이버 예방 조치에는 조직의 주요 서비스 및 제품에 대한 위험의 식별, 우선 순위 지정 및 대응이 포함됩니다. 사이버 예방 조치 보안 모범 사례를 시행하면 데이터 침해 및 잘못된 시스템 구성을 방지하고 비즈니스에 대한 관련 위험을 최소화하는 데 도움이 됩니다. 주요 위협 영역에 대한 이해 관계자의 동의를 얻어 위험 관리의 주요 목표에 집중하는 것도 중요합니다.

전체 목록은 아니지만, 다음 고려 사항은 사이버 위협을 처리하는 효율성을 높이는 데 도움이 됩니다.

7.1 공급업체

등록 및 인증 확인

적절한 등록 및 인증 검토: 예를 들어 ISO9000 등록 및 기타 품질 인증의 자료를 요청합니다. 공급업체의 제품이 회사 네트워크에서 사용하도록 설계되었는지 확인합니다.

모범 사례 자료 찾기

선택한 공급업체가 사이버 보안 모범 사례를 보여줄 수 있는지 확인합니다. 선택한 공급업체는 사이버 및 물리적 보안 조치를 설명하는 사이버 강화 가이드와 네트워크를 보호하는 데 도움이 되는 모범 사례를 제공해야 합니다.

공급업체 감사

구매를 약속하기 전에 철저한 감사를 수행합니다. 비즈니스 조건을 확인하여 명확하고 투명한지 확인합니다. 재정적 관점에서 비즈니스에 문제가 발생할 경우 제품 및 지원에 어떤 일이 발생하는지 묻는 것이 중요합니다.

지속적인 지원을 위한 리소스 확인

공급업체가 미래에 필요할 것으로 예상하는 솔루션을 계속 생성할 수 있는 자원을 보유하고 있는지 확인합니다. 공급업체가 향후의 비즈니스 요구사항을 지원할 수 있는 규모, 범위 및 능력을 갖추고 있는지 확인합니다.

미래의 비즈니스 필요 사항 정의

미래에 대한 필요 사항에 집중합니다. 지능형 장치 및 솔루션은 비즈니스를 향상하고 미래에도 비즈니스를 지속되게 수 있는 기능을 갖추고 있으므로 공급업체가 유지관리 계약 및 지속적인 지원을 통해 기대치를 충족하거나 초과할 것이라고 확신해야 합니다.

윤리적 비즈니스 관행의 검증을 추구

윤리적이고 지속 가능한 관행의 증거를 확인합니다. 신뢰와 공동의 목표를 기반으로 하는 파트너십은 장기적 존속을 위한 강력한 기반입니다. 공급업체가 환경 관리 시스템, 기업의 사회적 책임(CSR) 프로그램 또는 윤리적 소싱 정책을 갖추고 있습니까?

7.2 제품 및 시스템

실사 실행

시스템 및 핵심 요소에 대한 기술 실사를 수행하여 시스템이 가치를 제공하고 지속적인 운영에 영향을 미칠 수 있는 기본 요소가 없는지 확인합니다. 위험 평가 및 위험 완화에 대한 정보가 명확하고 사용 가능한지 확인합니다.

유지보수 계약 확인

서비스 및 유지보수 계약에 제조업체 소프트웨어 업데이트 및 펌웨어 업그레이드가 포함되는지 여부와 같이 계약의 일부로 포함된 항목을 확인합니다.

연결된 장치의 보안

네트워크에 연결된 물리적 보안 시스템이 안전한지 확인하십시오. 보안 시스템은 사이버 보안을 염두에 두고 배치해야 합니다. 기본 사용자 이름 및 패스워드 변경, 최신 펌웨어 설치, 암호화 활용(이상적으로는 HTTPS), 원격 액세스 비활성화를 염두에 두어야 합니다.

설계 보안 문서 요청

공급업체는 네트워크 연결 장치에 대한 사이버 보안 상태의 증명으로 설계 보안 문서를 제공할 수 있어야 합니다.

시스템의 인텔리전스 평가

완전히 지능적인 연결된 장치는 MAC 주소로 네트워크로 연결되고 시스템 아키텍처의 본질적인 부분을 형성하는 장치입니다. MAC 주소가 없는 장치는 지능적이지 않으며 개별적으로 식별, 관리 또는 보호할 수 없습니다.

GDPR/Data Protection Act 준수 평가

GDPR은 개정된 1998년 Data Protection Act와 함께 2018년에 발효되었습니다. 제품 및 시스템이 Data Protection Act 2018 및 GDPR을 준수하는 기능을 지원하는지 확인합니다.

T10168631/KO/M3.2/2108

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