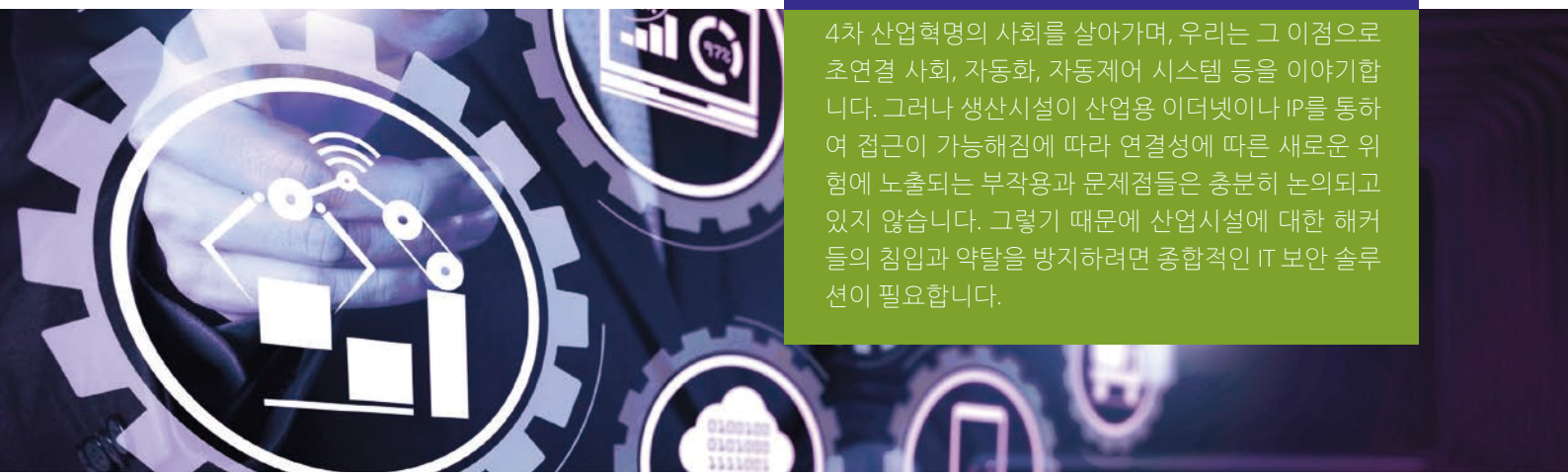
스마트 공장 보호

커넥티드 제조 환경에서 사이버 공격에 대항할 수 있는 종단간 보호는 필수적입니다



4차 산업혁명의 사회를 살아가며, 우리는 그 이점으로 초연결 사회, 자동화, 자동제어 시스템 등을 이야기합니다. 그러나 생산시설이 산업용 이더넷이나 IP를 통하여 접근이 가능해짐에 따라 연결성에 따른 새로운 위험에 노출되는 부작용과 문제점들은 충분히 논의되고 있지 않습니다. 그렇기 때문에 산업시설에 대한 해커들의 침입과 약탈을 방지하려면 종합적인 IT 보안 솔루션이 필요합니다.

문제는 시간입니다. 예를 들어, 24시간동안 풀 가동되는 생산 공장이 있다고 상상해봅시다. 갑자기 여러 대의 컴퓨터에서 터치 스크린이 작동하지 않습니다. 그리고 급히 무엇이 잘못되었는지 확인해본 직원은 중앙 프로세스 데이터에 접근이 차단되었다는 것을 알게 됩니다. 얼마 지나지 않아 그들은 협박 편지를 받게 됩니다.

이는 허구의 이야기가 아닙니다. 실제로 독일에서는 2016년 이후 주요한 여섯 가지 종류의 사이버 공격이 발생했습니다. 독일 연방 정보 보안청 (BSI)에 따르면, 공격받은 회사의 일부는 몇 주간 회사 운영을 중단해야 했고 이로 인해 수백만 유로에 달하는 손실이 발생했습니다. 뿐만 아니라 공장 제어 시스템 및 산업용 컴퓨터에 대한 공격이 증가하고 있다고 밝혔습니다. 커넥티드 프로세스의 수가 증가함에 따라, 해커들이 새로운 공격 루트를 찾아냈기 때문에 이러한 증가 추세를 보이는 것입니다. 독일 연방 정보 보안청의 Arne Schonbohm 청장은 “IT보안 사고가 급격하게 증가하고 있다.”며 “이러한 유형의 사고는 빈번하게 발생하고 있고, 매우 정교한 수준에 이르렀다”고 우려를 나타냈습니다. 이는 4차 산업혁명의 시대를 사는 우리가 아직 보안에 대한 준비는 충분히 되어있지 않음을 보여주는 부분입니다.

산업용 이더넷은 향상된 성능과 함께 새로운 리스크를 야기합니다.

4차 산업혁명은 생산 프로세스에 있어 향상된 효율성, 투명성, 유연성을 약속하지만, 사실 이전보다 더 많은 리스크를 안고 있기도 합니다. 생산시스템이 IP를 통하여 접근될 수 있는 반면, 커넥티드 환경은 과거에 사용되었으나 산업용 이더넷으로 대체된 필드버스를 이용합니다. 이러한 방식으로 시스템을 외부에 오픈하는 것은 제어 소프트웨어와 주요 데이터에 대한 허용되지 않는 접근의 위험을 높입니다. 최근 공격시도가 빈번히 일어났으며 그 중 상당수가 성공적이었습니다. 이는 고도의 IT 인프라를 갖춘 글로벌 기업조차도 위협을 과소평가하고 있었음을 보여줍니다.

중소기업들은 사이버 보안에 지속적인 투자를 하지 못하고 있습니다. 일반적으로 중소기업들은 해커가 생산시설에는 관심이 없을 것이라고 오해하고 있으나, 실제로는 그렇지 않습니다. 중소기업의 생산 관련 IT 시스템들은 중단 없이 운영되는 경우가 많기 때문에 보안 업데이트가 제때 이루어지지 못하여 공격에 취약합니다. 뿐만 아니라 스마트 공장에 연결되지 않는 장비조차도 유지보수 중에 허가되지 않은 USB 인터페이스를 통한 공격이 이루어질 수 있습니다. 더 나아가 해커가 보다 광범위한 공급망의 일부로서 제조사을 공격할 가능성이 있습니다. 이에 따라 독일의 IT 보안법과 같은 새로운 규정들은 ‘회사가 법에 따라 산업의 IT 보안 조치를 적절히 이행해야 한다’고 명시하고 있습니다.

전문가가 필요한 영역

사이버 범죄의 위험으로부터 커넥티드 생산설비를 안정적으로

보호하는 유일한 방법은 전체적인 보안 솔루션을 적용하는 것입니다. 생산환경의 다양한 IT시스템에 대한 깊은 이해를 바탕으로 위험을 체계적으로 식별하고 평가하며 보안 목표를 정의하는데 필요한 세부사항을 분석해야 합니다. 장비가 24시간동안 가동되는 시설에서도 유지, 보수 및 업데이트가 가능한 보안 계획이 있어야 합니다. 또한 여러 운영자가 개별적인 시스템에 접근할 수 있어야 합니다. 이런 보안 계획은 패스워드를 이용하는 보안 시스템을 실용적이지 못한 시스템으로 전락시킬 수 있습니다. 사무용 IT를 익숙하게 다루는 팀이라도 생산 시스템을 위한 총체적인 보안 시스템은 스스로 개발하기가 어렵습니다. 따라서 이러한 분야는 전문가들이 필요합니다.

결국 보안은 모든 수준에서 다루어져야 합니다. 그러기 위해서는 조직, 프로세스, 인식에서의 IT 보안을 확고히 할 수 있는 적절한 조치가 개발되어야 합니다. PDCA(plan, do, check, act)주기를 사용하여 솔루션의 효율성을 검증하는 것은 정보보안 관리 시스템(ISMS)을 보유하는 것만큼이나 중요합니다. 전체적인 보호의 핵심은 위험 방지, 주요 사건 식별 그리고 그러한 사건을 방지하기 위한 신속한 사고 대응을 포함하고 있습니다. End-to-End 보안 솔루션은 미래의 위협에 대한 결론을 이끌어낼 수 있어야 합니다. 이러한 방식만이 기업이 커넥티드 생산설비의 모든 IT 구성요소와 시스템의 무결성, 가용성, 신뢰성을 보장하고 관련 데이터의 기밀성을 보호할 수 있습니다. .

구체적인 보안 대책

IT시스템은 본질적으로 다양하기 때문에, 생산라인을 완벽하게 보호하기가 쉬운 일은 아닙니다. 이러한 이유로 각 장비나 보안 영역에 대한 보호수단을 업스트림 시스템에서 구현하는 것이 권고하고 있습니다. 우선 외부와의 프로세스 통신을 차단하고 의심스러운 네트워크 트래픽을 필터링합니다. 이것은 더 나아가 바이러스 백신 소프트웨어, 방어 기능, 응용프로그램 인식 및 생산 활동을 중단하지 않고 사용자 ID 인식 업데이트 등을 가능하게 합니다. 또한 Zone model은 방화벽이 개별 생산 영역간의 통신을 모니터링 하는 보호기능을 제공합니다. 대상에 관한 정보를 기반으로 권한이 없는 네트워크 트래픽을 필터링합니다. 이 영역을 설정하기 위해서는 IT 전문가와 생산 전문가의 긴밀한 협력이 필요합니다. 만약 보안 시스템이 이러한 방식으로 나눠진다면, 그 후에는 업데이트 구현이나 법률상의 불만 신고와 같은 작업을 관리하기 쉽도록 유지하는 것이 중요합니다.

Best practice: 설계단계부터의 종합적 보안 구성

그러나 새로운 스마트팩토리는 상황이 다릅니다. 산업부문의 사이버 보안이 설계단계에서부터 생산라인의 소프트웨어 및 하드웨어 제어시스템에 직접 통합할 수 있기 때문입니다. 새로운 보안 조직, 지속적 IT 보안 관리, 구성요소 및 시스템 보호는 처음부터 종합적으로 고려되어, 공장 및 시스템 전체 라이프사이클을 포괄하도록 설계될 수 있습니다. 이러한 설계방식에 의한 종단간 보안 접근법은 생산설비가 IT 시스템 자체에 연결되어 4차 산업혁명의 핵심에 보안을 부여한다는 것을 의미합니다. ■

저자

노만 웽크(Norman Wenk), 에스크립트, IT보안 컨설팅 담당 매니저.

Best practice: 설계단계부터의 종합적 보안 구성

*) Source: BSI-Magazin 2018/1