White Paper

OT 환경을 지키는 보안 기술

개요

산업제어시스템(Industrial Control System: ICS) 환경이 분산화, 초연결화 및 지능화되면서 보안 수요도 갈수록 증가하고 있다. 특히 스마트팩토리 및 자동화 실현의 일환으로 5G, 산업사물인터넷(IIoT), 인공지능(AI) 등을 적용하면서 기존 산업제어시설의 에어갭(Air-Gap: 제어망과 내부 네트워크망을 물리적으로 분리하는 보안전략)이 지속적으로 얇아지고 있어, 보다 견고한 보안 체계가 요구된다.

시장조사기관 마켓츠앤마켓츠(MarketsandMarkets)에 따르면 글로벌 ICS 보안 시장 규모는 2020년 158억 달러(한화 약 17조 6천억 원)에서 2025년 222억 달러(한화 약 24조 8천억 원)까지 늘어날 것으로 전망됐다. 예상 연평균 성장률(CAGR)은 7%였다. 주요 성장 동력으로는 ICS에 대한 공격 고도화와 컴플라이언스 준수 필요성의 증가가 꼽혔다.

ICS 보안 트렌드와 규제

ICS 환경은 산업 규모가 크고 대형 제조 공장 및 발전소 등으로 이루어져 있어 국민의 경제 및 안전과 직결된 분야다. 따라서 이에 걸맞는 투자와 보안 체계 구축이 병행되지 않는다면 각종 보안 위협에 노출되어 향후 커다란 사회적 손실로 되돌아올 수 있다.

그럼에도 ICS 환경은 보안보다 안전성과 가용성에 높은 우선 순위를 두는 경향이 강하다. 여전히 단종된 구형 운영체제(OS)를 사용하고 보안 패치도 제대로 이뤄지지 않는 경우가 많다. 또, IT 환경에 비해 보안 솔루션 사용도 현저히 부족해 보안 위협에 대한 대비가 부족한 상황이다.

IT 환경과 다른 ICS 환경의 보안 위협을 살펴보면 다음과 같다.

・ICS 네트워크에서 정보의 흐름을 차단 또는 지연시켜 PLC(Programmable Logic Controller)와 같은 설비의 작동을 방해

- ICS 설비의 제어 명령, 가이드, 경보 임계값을 무단으로 변경하여 장비를 손상, 불능화 또는 정지시켜 환경적 충격을 초래하거나 사람의 생명을 위협
- 시스템 운영자에게 부정확한 정보를 전송해 무단 변경을 위장하거나 운영자가 부적절한 행동을 시작하도록 하여 다양한 악영향 발생
- ICS 소프트웨어의 형상 설정이 수정되거나 악성코드에 감염되어 다양한 악영향 발생
- 장비 보호 시스템의 작동을 방해해 대체가 어려운 고가 장비의 손상을 초래
- 안전 시스템의 작동을 방해해 인간의 생명을 위협

매년 ICS 환경에서의 대형 보안 사고들이 이슈가 되고 있으며, 이를 통해 공격 기법이 고도화되고 있음을 알 수 있다. 2019년 노르웨이 노르스크 하이드로(Norsk Hydro) 공장의 랜섬웨어 감염, 2020년 일본 혼다(HONDA) 자동차 공장의 SNAKE(EKANS) 랜섬웨어 감염 사례에서 보듯, 공격자들은 고도화된 지능형지속위협(Advanced Persistent Threat: APT) 기법을 통해 특정 타겟을 대상으로 공격을 수행한다. 이는 산업 기밀 유출과 조업의 가용성에 심각한 타격을 주는 관계로 더욱 각별한 대비가 필요하다.

ICS 환경의 보안을 위해서는 많은 요소들이 충족되어야 하지만, 그 중에서도 크게 두 가지가 뒷받침되어야 한다. 바로 구체적인 보안 규정과 효과적인 보안 솔루션 도입 & 운영이다.

먼저 ICS 보안 규정에 대해 살펴보자. 체계적인 규제와 가이드라인 제시는 시장의 성장을 이끄는 원동력이다. 산업이 일정 수준 이상의 규제를 준수하기 위해 개발과 투자를 단행하고 이를 통해 발전이 자연스럽게 따라오기 때문이다. 우리가 흔히 알고 있는 일반 IT 환경의 경우에는 보안 규정이 직접적이고 상세하며 규칙 준수에 대한 의무화가 철저하다. 이에 반해, ICS 보안 규정들은 아직 보완해야 할 측면이 많고, 규정 준수도 의무가 아닌 권고에 머무르고 있다.

이는 ICS 환경의 특수성에 대해 기존 IT 보안 전문가들의 경험과 이해가 부족했고, IT 환경에 비해 기존 보안 운영 체계를 변경하기 어려운 특성 때문이기도 하다. 또, ICS 환경 자체가 이미 일정 수준 이상의 물리적 규모를 유지하고 있어, 보안 체계 구축 혹은 사이버 보안 규정 준수를 위해 상당한 비용이 요구되는 것도 사실이다.

국내의 규정 현황을 간단히 살펴보면 최근 국가보안기술연구소에서 '주요정보통신기반시설 제어시스템 취약점 분석, 평가 항목' 지침을 개정했다. 또, 한국정보통신기술협회(TTA)에서 '산업제어시스템 보안요구사항'을 개정한 바 있다. 이와 같은 노력을 통해 변화하는 환경에서 산업제어시스템의 안전한 운용을 위한 기술적, 물리적, 관리적 가이드라인을 제공하고 있다. 하지만, 실제 ICS 환경과 비교했을 때 지속적인 개선이 필요할 것으로 보인다.

그래도 고무적인 점은 최근 들어 ICS 환경 보안 문제에 대한 연구가 활발히 진행되고 있어 앞으로 관련 규정들이 지속적으로 개선 및 업그레이드될 것으로 기대된다는 것이다. 업계에서도 경쟁적으로 OT 보안 취약점 진단이나 거버넌스 등의 컨설팅에 대한 투자를 확대해 ICS 환경의 보안 운영 체계를 잡아가고 있다.

다만, 아직 부족한 ICS 보안 규정의 개선에 대한 기대감과는 별개로 ICS 환경의 보안 위협이 갈수록 증가하고 있으며 이에 대한 대응 방안이 조속히 필요한 것은 자명한 사실이다. 이에 기업들은 먼저 기존 IT 환경의 보안 규정을 참고해 당사의 환경에 맞는 보안 규정을 수립하고, 보안 기업의 컨설팅 및 솔루션 도입을 통해 보안 진단과 대응을 고민해야 한다.

안랩 역시 세계적인 제조업 경쟁력을 갖춘 우리나라에서 ICS 보안이 갖는 중요성을 오래전부터 인지하고, ▲보안 솔루션 ▲산업용 제어시스템 보안컨설팅 ▲OT 보안관제 서비스 등으로 이루어진 포괄적인 보안 포트폴리오를 구축해

왔다. 그리고 그 중심에는 특수목적시스템 환경에 최적화된 전용 보안 솔루션 'AhnLab EPS'가 있다.

고도화되는 ICS 보안 위협, AhnLab EPS로 대응

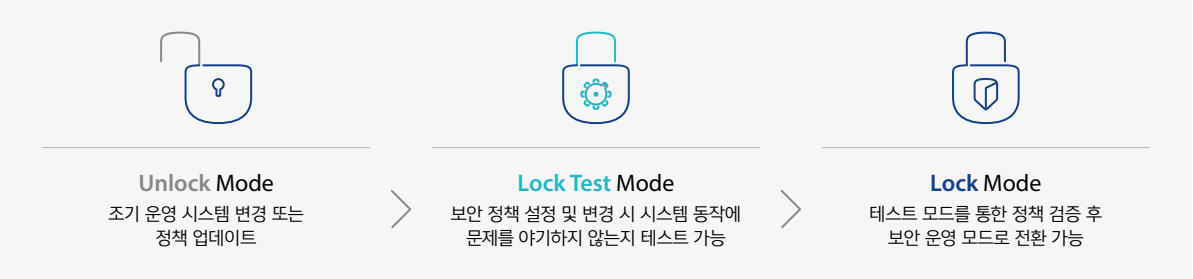
AhnLab EPS는 ICS를 비롯해 POS, 키오스크 등 안정적 운용에 대한 요구가 높고 정해진 프로그램만 사용하는 특수목적시스템에 최적화된 보안 솔루션이다. 악성코드 탐지 및 분석을 EPS 중앙 관리 서버에서 수행해 ICS 환경에서의 운영 안정성을 보장한다. 단말 시스템에 설치되는 초경량 에이전트(EPS Agent)와 중앙 모니터링 및 정책 관리 서버(EPS Server)로 구성되는 것이 특징이다.

특히, ICS 보안 영역에 공을 들여온 안랩은 지난해 초 다방면에서 솔루션 개선을 이뤄내며 AhnLab EPS 2.0을 선보였다. AhnLab EPS 2.0은 기존 윈도우 시스템 대상 미인가 실행파일/시스템변경 차단과 악성코드 검사기능에 더해 ▲리눅스 기반 시스템에 대한 악성코드 검사기능 및 통합(윈도우/리눅스) 보안관리 지원 ▲AhnLab MDS 연동으로 악성코드 위협 탐지범위 확대 ▲관리자의 시스템 변경 시에도 보안정책을 유지하고 변경 사유를 남기도록 긴급점검모드 기능 고도화 ▲예약검사, 보유파일 검사 개선 등 보안성과 관리 편의성을 높였다.

[그림 1] AhnLab EPS 개념도

주요 기능 1: 3단계 운영 모드

AhnLab EPS의 주요 기능으로는 먼저 '3단계 운영 모드(Lock Mode)'를 꼽을 수 있다. 3단계 운영 모드는 편리한 정책 설정 및 관리 역량을 단계 별로 제공해 시스템 중단 없이 안정적으로 보안을 관리하고 운영할 수 있도록 한다.



[그림 2] AhnLab EPS 3단계 운영 모드

먼저 Unlock Mode는 최초 EPS 에이전트를 시스템에 설치한 상태로, 모든 시스템 상의 변경 및 유지 보수 작업이 가능하다. Lock Test Mode는 이미 정의한 보안 설정에 대한 검증을 위한 상태로, 모든 보안 정책 위반 사항은 에이전트에서 서버로 전송되어 관리자 확인이 가능하다. 마지막 Lock Mode는 정의된 보안 정책을 기반으로 시스템상의 모든 변경을 허용하지 않는 상태를 뜻하며 예외 정의 항목을 제외한 모든 변경을 허용하지 않는다.

주요 기능 2: 허용리스트 기반 애플리케이션 제어

AhnLab EPS는 일반적인 안티 멀웨어 솔루션과 달리, 허용리스트 기반으로 운영에 꼭 필요한 프로그램만을 실행해 ICS 환경에 가해질 수 있는 위협을 최소화한다. 실행파일(Portable Executable: PE)의 생성, 수정 등의 변경도 차단된다. 관리자 입장에서는 별도의 애플리케이션 허용리스트 생성 작업을 할 필요가 없어 정책 설정 부담 없이 유연하게 관리할 수 있다.

EPS 허용리스트 기반의 EPS Agent	VS.	차단리스트 기반의 기존 백신 제품
사전 예방	처리 방식	사후 처리
허용된 애플리케이션만 사용	애플리케이션 실행 범위	모든 애플리케이션 사용 가능
변경 없음	엔진 크기	지속적인 변동 발생
낮음	자원 점유율	높음
높음	보안 수준	보통
에이전트에서 업데이트 불필요 (EPS 서버에서 업데이트, 정기적인 시스템 점검 시 스케줄링 가능)	엔진 업데이트	주기적인 엔진 업데이트 필요

[그림 3] AhnLab EPS vs 기존 백신 제품

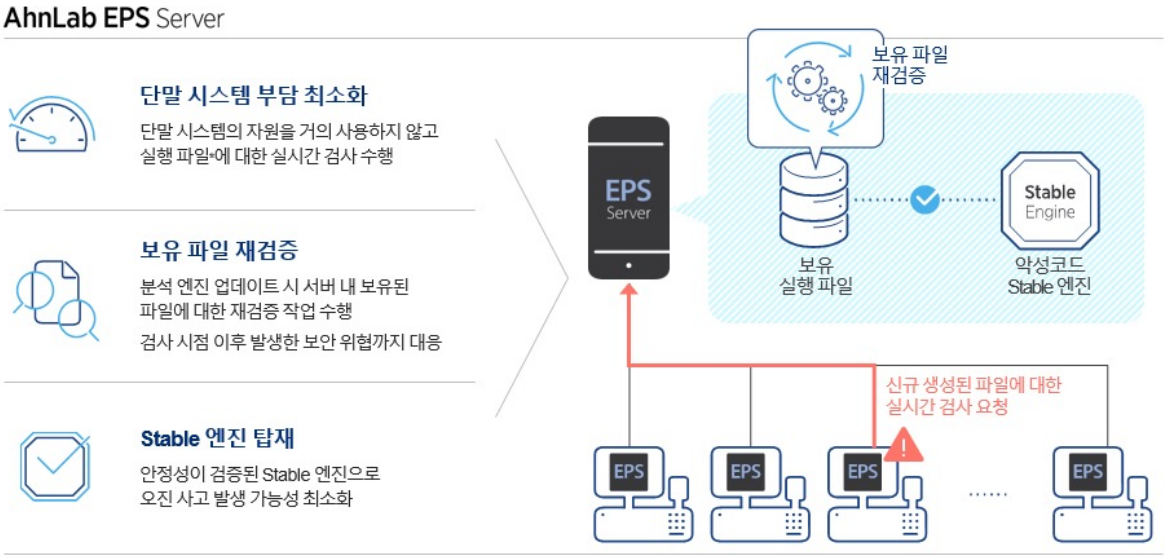
보안 운영 모드인 Lock Mode에서 예외적으로 파일 실행을 허용해야 하는 경우에는 Lock Mode 예외 허용 목록 관리 기능을 활용하면 된다. 신뢰할 수 있는 지정 업데이터(Trusted Updater)를 이용해 Lock Mode에서 운영에 필수적인 프로그램의 설치 및 업데이트가 지원된다.

이 밖에 USB 등 다양한 이동형 매체에 대한 접근을 제어하고 자동 실행을 차단해 불필요한 매체를 통한 악성코드 유입을 막는다. 같은 목적에서 허가되지 않은 IP & 포트로의 네트워크 통신도 차단해 악성코드 유입과 내부 확산을 미연에 방지한다.

주요 기능 3: 최적화된 악성코드 대응

AhnLab EPS는 산업제어시스템 운영 환경의 특수성을 고려해 EPS Server에 탑재된 악성코드 분석 엔진을 활용, EPS Agent가 설치된 단말 시스템의 네트워크 및 시스템 자원에 영향 없이 악성코드를 탐지 및 차단한다.

AhnLab EPS는 단말 시스템의 자원을 거의 사용하지 않고 실행 파일에 대한 실시간 검사를 수행한다. 단말 시스템의 부담을 최소화한다는 점이 관리자 입장에서 상당히 매력적이다. 그리고, 보유하고 있는 파일들을 재검증하는 작업을 거쳐 검사 시점 이후에 발생한 위협까지도 대응이 가능하다. 또한, 안정성이 검증된 'Stable Engine'을 탑재하고 있어 오진 가능성을 최소화한다.



[그림 4] AhnLab EPS 악성코드 대응

이처럼 EPS Server에 탑재된 악성코드 분석 엔진은 EPS Agent가 설치된 윈도우 및 리눅스 OS 기반의 단말 시스템에 대해 주기적인 악성코드 검사를 진행한다. 악성코드 검사는 상황에 따라 수동 및 예약으로도 수행 가능하며 정책 설정에 따라 탐지된 악성코드에 대해 OS별 대응을 지원한다.

주요 기능 4: 편리한 중앙 관리

AhnLab EPS의 웹 기반 관리 시스템을 통해 각각의 설비 시설에 산재되어 있는 시스템을 효율적으로 통합 관리할 수 있다. 또한, 관리 대상 시스템을 그룹으로 설정해 공통 또는 개별 보안 정책을 일관성 있게 설정 및 적용할 수 있으며, 모든 시스템에서 발생하는 로그를 한 곳에서 확인 가능하다.

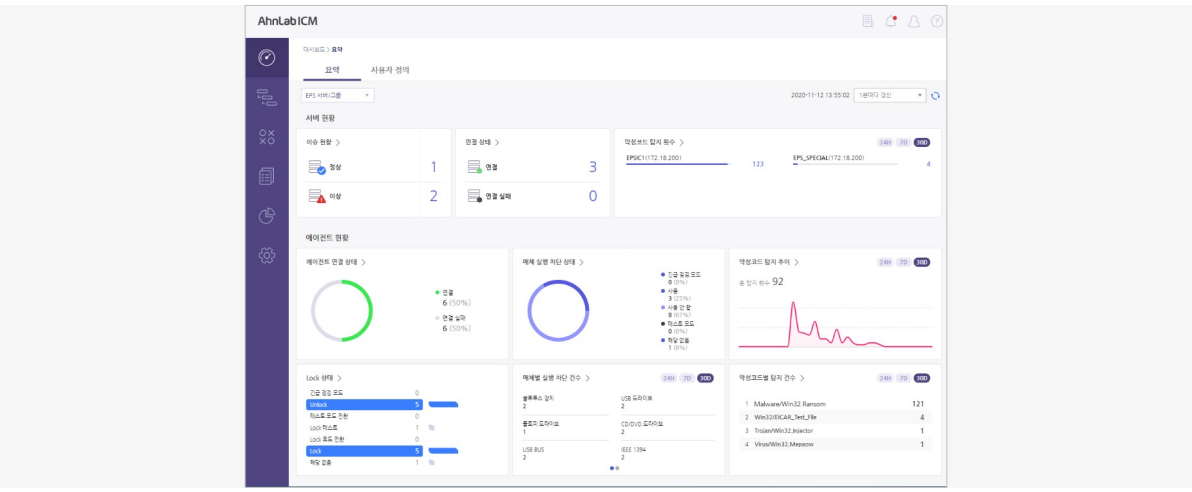
[그림 5] AhnLab EPS 통합 관리 대시보드

이 밖에 AhnLab EPS는 오프라인 운영 환경에서 정해진 애플리케이션만을 사용해야 하는 시스템을 위해 'Standalone' 형태로도 제공된다. AhnLab EPS Standalone은 가용성 및 운용 안정성에 대한 요구가 높은 특수목적 시스템 보안에 최적화된 '독립형 에이전트' 솔루션으로, 네트워크, EPS 서버에 연결되지 않는 독립된 운영 환경의 단말을 각종 보안 위협으로부터 안전하게 보호한다.

연동으로 진일보한 중앙 관리와 위협 대응

안랩은 본문 서두에 언급한 ICS 환경 위협의 고도화 및 다각화에 대응해 AhnLab EPS 솔루션 업데이트에 더해 신제품과의 연동도 진행했다. 이는 관리 편의성 제고와 진일보한 위협 대응 역량 제공을 위함으로, 그 결과 탄생한 것이 바로 AhnLab ICM과 AhnLab Xcanner다.

먼저 AhnLab ICM은 AhnLab EPS 서버 중앙 모니터링 및 통합 관리 솔루션이다. 보호 대상 특수 목적 단말 전체에 대한 통합 가시성 확보와 이슈 발생 시 전체적인 관점에서 신속한 탐지 및 대응의 필요성을 충족하기 위해 출시했다.



[그림 6] AhnLab ICM 대시보드

AhnLab ICM은 AhnLab EPS 서버의 데이터를 취합하고 시각화하여, 다수 서버에 연결된 단말의 이슈를 신속하게 확인하고 조치할 수 있도록 한다. 사용자는 직관적인 인터페이스로 시스템을 효율적으로 모니터링 할 수 있으며, 다양한 리포트와 알림 기능을 통해 관리로 발생되는 총 소유 비용(TCO)을 절감하고 보다 효과적으로 시스템을 관리할 수 있다.

AhnLab ICM이 AhnLab EPS의 통합 관리 영역을 발전시켰다면 AhnLab Xcanner는 한층 효율적인 차원에서의 위협 대응 역량을 더했다. AhnLab Xcanner는 윈도우 기반 시스템에서 악성코드를 찾아 제거하기 위한 수동 검사 기반 악성코드 진단 및 치료 프로그램이다. 실시간 대응이 어려운 악성코드 감염 시스템에 대한 보안 조치 필요성이 높아짐에 따라, 관리자가 감염된 시스템을 효과적으로 사후 치료할 수 있도록 지원한다.

결론: ICS 보안, 더 이상 간과할 수 없는 주요 사안

앞서 다룬 ICS 환경에 대한 보안 위협 고도화, 보안 침해가 가져오는 파급력, 우리나라에서 제조업이 차지하는 비중 등을 고려하면 ICS 보안은 더 이상 과거와 같이 간과해서는 안되는 주요한 사안이다. 이에 맞춰 아직은 부족한 ICS 보안 규정들도 개선의 움직임을 보이고 있다. 만약 독자 여러분의 ICS 환경에서 구형 OS 사용, 보안 패치 미적용 등 아직까지 보안 태세가 제대로 갖춰져 있지 않다면 전문적인 진단을 통해 개선점을 점검하고 강력한 보안 솔루션 도입을 고려해볼 필요가 있다.

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901