EQST insight

Hyper Connected 스마트 공장의 시대, 네트워크 보안 정책 수립의 중요성

Changing Landscape

4차 산업혁명과 미중 갈등, 코로나19 등의 여파로 제조업 글로벌 가치 사슬(Global Value Chain) 구조의 해체 및 약화가 가속화되고 있다. 글로벌 가치 사슬이란 소재 조달과 조립, 유통, 배송 등 제품 생산 전 공정을 세계 각지에서 나눠서 분담하는 국제 분업 구조를 말한다. 생산 설비의 고도화 및 자동화로 단순 인건비보다는 고임금 시장과의 접근성, 인프라의 발달 정도를 함께 고려하면서 저개발 국가에 거점을 둔 공장이 줄고 있다. 특히, IIoT(산업용 사물인터넷) 및 5G를 기반으로 구축한 제조 시설은 AI의 적극적 도입 및 활용을 통해 의사 결정이 이루어진다. 디지털 트윈 더 나아가 메타버스 환경으로 관리가 이뤄지며 각 요소에 로봇공학, 3D 프린팅, 인공지능, 사물인터넷 등 새로운 원천 기술이 접목되면서 구조가 보다 복잡해질 전망이다.

초기 비용을 절감하고 효율성을 향상시키기 위해 새로운 기술을 만들지 않고 기존에 상품화된 대중적인 최신 기술, 제품(COTS:Commercial Off-The-Shelf), 시스템/서비스 등을 사용하면서 외부 네트워크와 시스템 간의 상호 연결이 증가하게 되었다. 반면 제조 기술은 급격한 변화가 일어나기도 하지만 공정 현황에 따라 수십 년 간 운영해 온 Legacy도 병용되는 것이 현실이다.

제조업의 보안 담당자는 이러한 Legacy로부터 최신 Cloud, AI, IIoT 영역까지 식별하여 지켜야 하는 상황이다. 본 기고를 통해 초 연결된 제조업 환경에서 자사의 보호 대상을 어떻게 식별/관리할 것인지, 어떤 네트워크 보호 대책을 설계하여 효율적으로 운영할 것인지 기술하여 도움을 드리고자 한다.

제조업 정보 자산 식별 및 네트워크 보안 전략 수립 시 실용적 접근 방안

네트워크 보안 정책 강화 전략 수립은 전쟁 시 공격/방어 계획을 수립하는 것과 유사하다. 보호해야 할 대상을 정하고(정보 자산 식별), 공격 가능한 모든 경로를 식별하고 차단할 수 있도록 대응 자산을 계획 배치(전사 네트워크 모델링 및 정책 수립)하는 것이다.

1. 제조업 '정보자산'의 식별 및 분류 시, 전사 ITSM(IT Service Management)과 연계/분석하면 효과적이다.

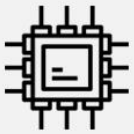
Key point #1

정보 자산의 분류 및 관리 정보의 현행화는 전사 차원의 IT 시스템/서비스 관리 체계와 연계될 때 최대치의 효과를 발휘한다. 생각보다 다수의 현장 보안 담당자/운영자들이 ITSM에 대해 인지하지 못하는 경우가 많다. 기업 규모에 따라 수준의 차이는 있을 수 있어도 ITSM의 각 영역 별로 내재화된 프로세스가 존재하거나, 더 나아가 시스템 기반 운영 중에 있을 것이다.

정확한 위험 평가를 위한 보호 대상의 정의를 위해 보안 담당자는 자사의 정보자산을 식별/분류해야 한다. 정보자산은 정보와 정보를 생성하거나 보관, 처리하는 모든 설비를 포함한다. 즉 회사가 보유하거나 경영 활동 과정에서 생성된 모든 유무형의 정보, 기술, 자료, 정보 시스템, 시설 등을 의미한다. 정보자산은 데이터 및 정보, 하드웨어, 소프트웨어, 물리적 환경, 인적 자산 등으로 분류할 수 있다.

제조업에서는 특히 자사의 공정을 운영하기 위한 시스템인 산업 자동화 및 제어 시스템에 대한 정확한 식별/분류가 필수적이다. 산업 자동화 및 제어 시스템에 대해 IEC-6244에서는 "산업 프로세스 운영과 관련이 있으며 안전, 보안 그리고 안정적 운영에 영향을 미치거나 영향을 줄 수 있는 인력, 하드웨어, 소프트웨어 및 정책 모음"으로 정의하고 있다.

위의 두 가지 정의에서 공통된 요소가 있다. 인력, 하드웨어, 소프트웨어, 정책, 데이터 및 정보, 설비 가 그것이다. 정보자산 보호란, '인력이 각 시설에서 설비상 위치한 하드웨어의 소프트웨어를 이용한 데이터 및 정보에의 접속 및 생성~폐기 전반을 정책을 통해 통제하는 것'이다. 정보 자산에 대한 분류는 다음과 같다.

유형	기본 정보	추가 정보
 하드웨어	자산식별코드, 자산 명, 하드웨어 유형, 서버 유형, 용도, 사용자, 소유자, 관리자, 위치	모델명, 운영 체제, 운영 체제 버전, 주요 데이터, 설치 애플리케이션, 호스트명, 제조 업체, 제품명, 도입일, 유지 보수 기간 등
 소프트웨어	자산식별코드, 자산 명, 소프트웨어 유형, 용도, 사용자, 소유자, 관리자	제품 명, 소프트웨어 버전, 제조 업체, 도입일, 유지 보수 기간 등
 시설	자산식별코드, 자산 명, 용도, 모델명, 소유 형태(자체/임대, 소유자), 관리 형태(자체/외주, 관리자), 소유자, 사용자, 관리자, 위치	제조업체, 공급업체 등
 데이터 및 정보	자산식별코드, 자산 명 (전자정보명), 전자정보 유형, 용도, 사용자, 소유자, 관리자, 위치	보관 기간, 생성일, 관련 응용 프로그램 등
 인력	소속 부서, 직무 및 역할, 담당 업무, 자격, 연락처	스킬, 경험 등

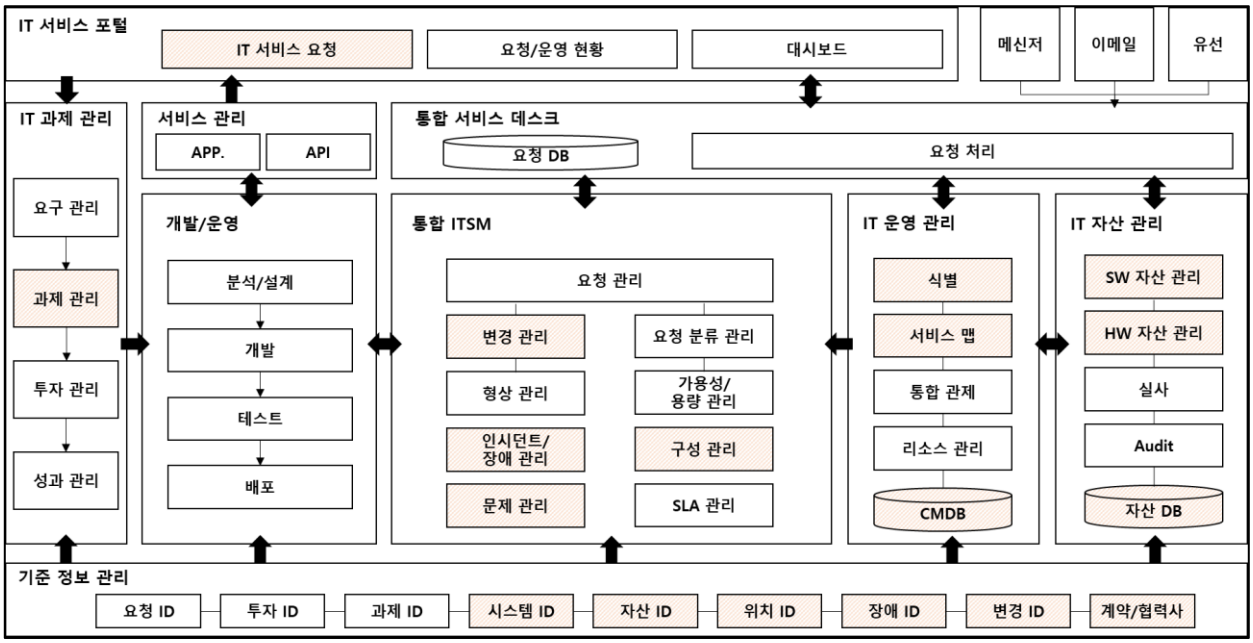
출처: 한국정보통신기술협회

< 정보 자산 분류 및 관리 정보 >

각 유형별 정보 자산을 조사할 때, 전사 ITSM 관리 부서의 담당자(통상 총무팀, IT 서비스/인프라 담당자 등)와 인터뷰를 진행하거나 외부 컨설팅 등을 통해 식별한 IP 목록을 IT 자산 관리 시스템과 교차 검증을 진행하면 효과적이다.

규모가 있는 제조업의 ITSM 담당자는 기준 정보(사내의 다양한 경영 활동 전반에서 사용되는 각종 시스템의 기초 운영 데이터)의 표준 관리 방식과 거버넌스를 수립하고 정비하는 체계인 MDM (Master Data Management)를 운영하고 있다. 해당 기준 정보는 전사 구성원의 소통 기준이며, 명확한 거버넌스를 정의하여 관리된다. 그리고 기준 정보는 데이터의 유형에 따라 실시간으로 변경 관리하기도 하고 주기적으로 갱신 관리 (정기 실사 등)하기도 한다.

정보 자산의 식별 관리 시 해당 정보를 관리하는 시스템과의 연계 인터페이스를 잘 설계하면 불필요한 수동 식별 작업을 상당 수 해소하여 자동화할 수 있다.



< ITSM 중 정보 자산 식별 관련 영역 >

ITSM의 구성 요소이다. 음영 처리된 부분은 정보 자산 식별에 필요한 데이터가 존재하는 영역이다. 각 영역별 데이터 스키마를 확인하여 정보 자산 식별에 필요한 정보를(식별 코드, 필요 항목, 갱신 주기 등) 식별 취합한다.

물론 있는 그대로 해당 정보를 정보 자산 정보로 활용할 수는 없다. 다수의 정보보호 담당자가 필요한 수준과는 다소 차이가 있기 때문이다. 따라서 각 정보보호 시스템(NAC, IDS, FW, SIEM, OT/ICS 가시성 확보 솔루션 등)을 통해 식별한 정보자산 기본 정보(예, IP, HOSTNAME, OS 종류 등)에 전사 기준 정보(전사 자산 식별 코드, 위치 정보, 담당자/소유자/사용자, 구성 정보, 변경 및 장애관리 정보 등)를 부가하여, 유관 부서(IT인프라, IT서비스 담당자 등)와의 소통을 원활하게 함으로써 보안 정책 현황 분석에 필요한 인사이트를 확보할 수 있다.

예를 들면 특정 10.10.10.10 서버의 프로토콜 취약점을 발견했을 때 전사 자산 정보를 기준으로 해당 서버는 전사 구성원 대상 ERP 서비스이며, 투자 과제 ID를 기준으로 HW, SW 아키텍처 및 구성 요소를 추적 가능하게 하고, 서비스 장애 레벨을 통해 중요도를 인지할 수 있으며, 담당자/소유자/실 사용자를 식별할 수 있게 되는 방식으로 활용할 수 있게 된다.

2. 정보 자산 보호 전략 수립은 전사 네트워크의 모델링부터 시작한다.

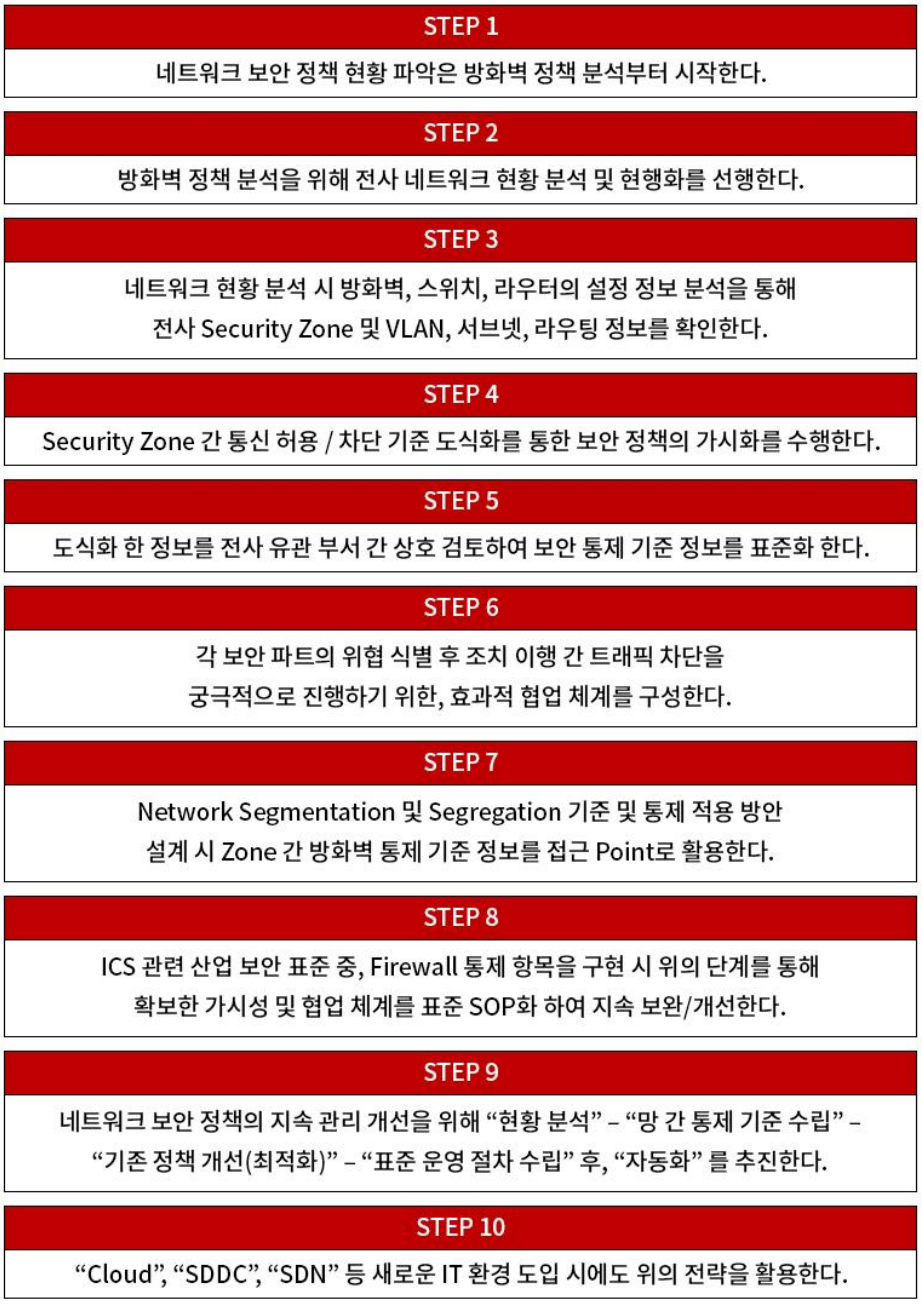
서두에 네트워크 보안 정책 강화 전략은 전쟁 시 공격/방어 계획을 수립하는 것과 유사하다고 언급한 바 있다.

핵심 공격 목표 또는 방어 대상을 지도 상에 간략히 표현하고, 모든 경로 중 핵심 보호 경로를 지정하여 보유한 전략 자산들을 효과적으로 배치한다. 이때 반드시 필요한 허가 대상 및 물자 등은 통과시키고 그 이외는 모두 차단하는 것이다.

지도 상에 아군 중 누가 봐도 이해할 수 있도록 이러한 전략을 약속된 기호로 그리고 소통하는 것이 바로 '모델링'이다. 즉, 일반적으로 모두에게 공통적으로 이해되도록 약속된 방식(수식, 그림 등)으로 표현하는 것이다. 정보 자산에 대한 보호 전략 분석/수립 시 전사 네트워크의 모델링부터 시작하면 효과적이다.

전사 네트워크 모델링을 통한 효과적 현황 분석 및 보안 정책 수립 방안을 알아보자.

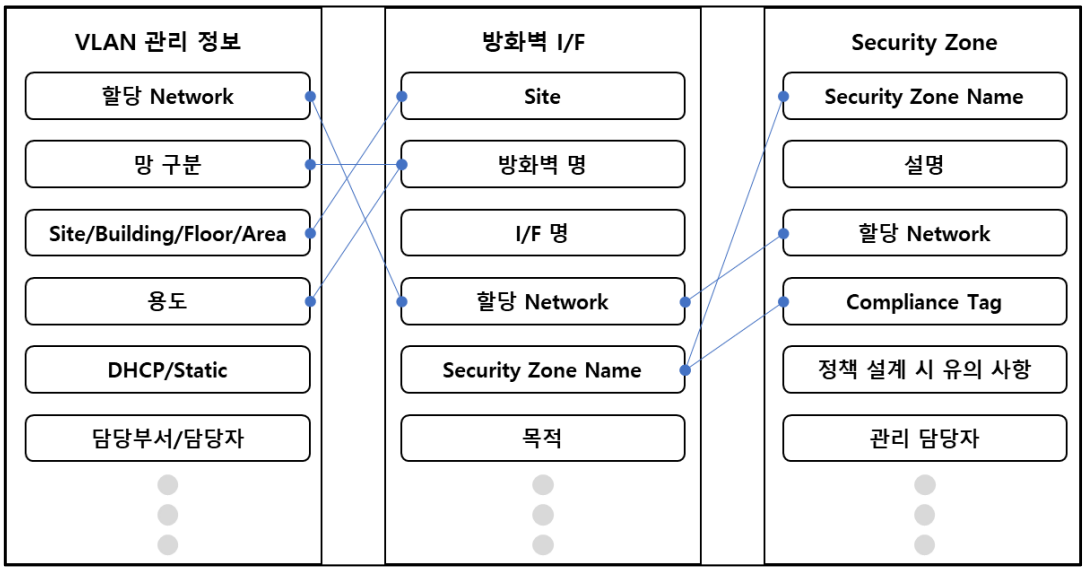
infosec



위 전사 네트워크 모델링의 필수 단계인 Security Zone 간 허용/차단 기준 가시화 방안과 가시화를 위한 기본 정보인 VLAN 정보와 Security Zone 매핑 방안 2가지 항목에 대해 집중적으로 살펴보겠다.

우선 VLAN 정보와 Security Zone 매핑 방안을 살펴보면 VLAN은 각 스위치/라우터에 설정된 네트워크 분리 단위를 의미한다. 전사 VLAN 정보를 목록화하고, 각 VLAN에 설정된 Network 대역을 현행화한다. 이때 지역 정보(Site/건물/층/상세 위치 등), 용도, 담당자 정보 등을 추가 취합한 후 이 정보를 보안 정책 적용 단위인 Security Zone과 교차 매핑하면 전사 네트워크 구조를 효과적으로 파악할 수 있는 수단이 된다.

해당 사항을 도식화하면 아래 그림과 같다.



< VLAN – 방화벽 I/F – Security Zone 매핑 관계 >

해당 매핑을 통해 식별한 Security Zone을 활용하면 Security Zone 간 허용/차단 기준 가시화가 가능하게 된다. 아래 그림을 참고하여 현재 보안 정책을 적용하면 현 상황의 파악이 가능해지고, Compliance의 기준을 세우는데 효과적으로 활용할 수 있다. 네트워크 규모에 따라 수기 작성이 불가능할 경우에는 방화벽 정책 관리 자동화 솔루션 또는 Micro Segmentation 솔루션을 활용하면 효과적으로 수행할 수 있다.

From Zone \ To Zone	DMZ	사무망	생산 서버팜	생산 라인
DMZ	Allow all	Partially Open	Partially Open (ssh, sftp, db)	Deny all
사무망	Partially Open (http(s))	Allow all	Partially Open	Partially Open (remote)
생산 서버팜	Partially Open (http(s))	Partially Open	Allow all	Deny all
생산 라인	Deny all	Deny all	Partially Open (ssh, sftp)	Allow all

< Security Zone 간 허용/차단 Matrix >

맺음말

정보 보안 담당자는 정보자산 보호 정책을 수립하고 운영하는 과정에서 명확한 Concept과 전략을 내재화해야 한다. 이를 위해서는 외부의 산출물을 참고하고 활용하는 방식을 통해 해당 Concept과 전략을 정교화하고 필요한 근거를 확보할 수 있다.

위에서 기술한 정보 자산의 전사 ITSM 연계/분석과 전사 네트워크 모델링을 통한 보안 통제 정책 수립 전략을 통해 안전한 제조 환경을 보장하고, 지속 가능한 안녕을 제공하는 든든한 보안 담당자가 되길 기원한다.