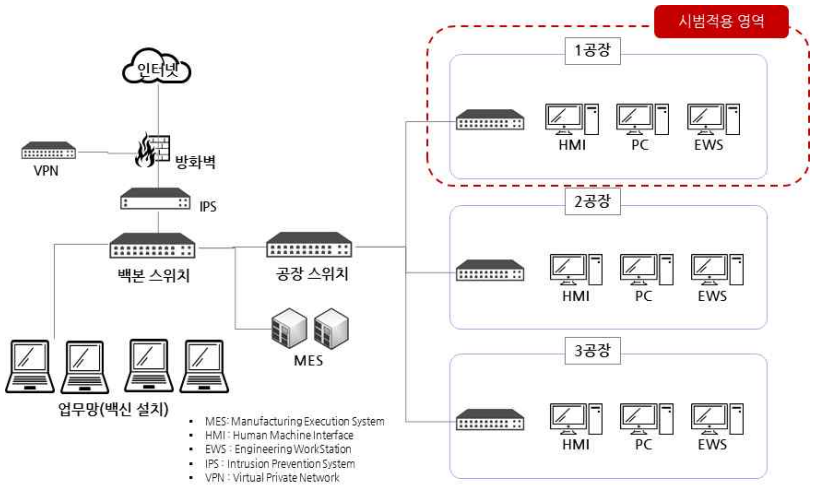
문제 1. 스마트공장을 추진하는 제조기업의 보안강화 방안

<배경 설명>

반도체 관련 소모품을 생산하는 B사는 스마트공장 구현을 위해 MES[1]를 1공장에 시범 적용했으며 그 직후 1공장에 있는 일부 PC가 랜섬웨어에 감염되어 생산이 중단되는 일이 발생함. 경영진이 이에 대한 원인을 파악하고 개선방안을 보고하도록 요구함.



[네트워크 구성도]

<전제 사항>

o 해당 기업의 임직원은 총 300명이며, 별도의 IT부서가 없고 경영지원팀에서 IT운영과 보안 업무를 1명이 담당하고 있음.

o IT 예산(5억원)은 확보하고 있으나 유지보수 비용(5천만원)을 제외한 별도 정보보호 예산은 없음.

o 본사와 공장의 네트워크는 동일 네트워크로 구성되어 있으며 보안솔루션은 아래와 같음.

- 본사 : 방화벽, 침입방지시스템(IPS), 바이러스 백신, VPN
- 공장 : 별도의 보안솔루션 없음

o 담당자가 자체적으로 일부 정보보호 지침을 수립하여 운영하고 있음.

- 정보보호 관리지침, 물리적보안지침, 인적보안지침, 인프라 운영보안지침

o 공장으로 노트북 등 이동단말 또는 이동저장매체 반입 시 별도의 통제는 없으며 공장 정문에서 출입인력 및 차량에 대해서만 통제를 하고 있음.

o 침해사고 대응절차 및 조직이 수립되어 있지 않으며 악성코드 감염 시 대응방안에 대해 이해하고 있는 직원이 거의 없음.

o 직원업무용 PC는 Windows 10으로 모두 업그레이드 하였으나 공장 내 대부분의 PC의 Windows 7을 사용하며 소수의 PC는 Windows XP, Windows 95를 사용하고 있음.

o 공장에서 랜섬웨어에 감염된 PC는 PLC와 연계되어 있으며 작업지시서 등의 정보를 저장하고 있음.

<고려 사항>

o 공장 영역(OT; Operation Technology)의 보안강화를 위한 방안을 포함하여야 합니다.

경영진은 랜섬웨어 감염 예방 및 공장에서 생성되는 중요 정보가 외부로 유출되지 않도록 안전하게 관리할 수 있는 관리적, 기술적 방안을 요구했습니다. 이에 대한 대응 방안을 수립하시길 바랍니다.

---

1) MES: 제조실행시스템(Manufacturing Execution System)은 제조 환경의 실시간 모니터링, 제어, 물류 및 작업내역 추적 관리, 상태파악, 불량관리 등에 초점을 맞춘 현장 시스템

문제 2. 변화한 업무환경을 위한 구조적 정보보호 대응방안 도출

<배경 설명>

클라우드, 모빌리티, OT, COVID 등 업무환경의 변화는 지난 20년간 네트워크와 정보보호를 별개의 항목으로 취급하는 기존 보안체계의 한계를 명확히 드러내고 있다. 랜섬웨어, APT 공격 등은 지난 20년간 벌어지고 있는 보안과 네트워크간의 틈을 공격지점으로 사용하여 기존 보안체계를 우회한 공격으로 기업의 전산 시스템이 아닌 비즈니스 연속성을 파괴하고 있다. 이러한 이격은 클라우드, 재택근무, OT망 운영 등 업무환경의 변화로 점점 더 커지고 있지만 전통적 보안솔루션은 공격의 진행 상황에 대한 가시성을 확보하지 못하여 위협의 시간적 확장에 대응하지 못하고 있다. 또한 전통적 보안통제는 업무 위치를 기반으로 한 공간적 경계모델을 만들어 각 영역 간에 보안수준을 통제하는 방식으로 동작하고 있어 업무환경의 공간적 확장에 대응하지 못하고 있어 변화하는 사이버보안 환경에 대응하기 위한 기술적/구조적 방안마련이 시급한 상황이다.

<전제 사항>

- o A사는 COVID-19 확산 방지를 위해 사내 인원의 50% 이상이 원격근무를 시행하고 있음.
- o A사는 수도권에 위치한 본사 및 제품 생산을 위한 다수의 지역거점을 운영하고 있음.
- o A사는 분기별 악성코드 모의훈련, 기술적 취약점 점검, 모의해킹, 웹 애플리케이션 모의해킹 등을 수행.
- o A사는 알려진 악성코드 및 악성 IP 정보를 보안 인텔리전스 서비스를 통해 공급받음.
- o A사가 운영 중인 정보보호 장비는 룰셋기반의 대응체계를 갖추고 있음.
- o A사는 보안정책/장비 운영/보안감사/사고 대응/모의해킹/취약점 진단 업무를 수행.

<고려 사항>

- o 현 정보보호 체계가 변화한 환경에서 고려하고 있지 못한 비 연속적 관리대상 네트워크에 대한 물리적/논리적 시야 확보의 문제.
- o 취약점 대응 및 알려진 악성행위지표(IoC) 기반 대응에서 오는 알려지지 않은 위협탐지의 한계를 어떻게 극복할 것 인가에 대한 고려.
- o 차단중심의 대응으로 내부에 침투한 공격자에게 운영 중인 방어체계 우회가 가능하도록 하는 단편적 대응 개선방안 고려.

A사의 경영진은 변화하는 사이버보안 환경에 대응하기 위한 기술적/구조적 방안을 요구했습니다. 이를 위한 정보보호 위협대응 방안을 수립하시길 바랍니다.

문제 3. 클라우드 보안 아키텍처 설계 및 운영 방안 수립

<배경 설명>

쇼핑몰을 운영하는 A사는 최근 개인정보가 포함되어 있는 일부 서비스를 클라우드로 이관했다. 일부 내부 업무 서비스는 클라우드를 이용하는 것이 적합하지 않은 것으로 판단되어 기존의 온프레미스 환경에 남겨뒀다. 서비스가 급박하게 클라우드 이관되어 보안 요구사항을 충분히 반영하지 못한 상황이어서 정보보호 담당자는 클라우드 서비스에 대한 보안 강화가 필요하다고 판단하고 있다. 또한, 클라우드로 이관 이후 해킹을 당한 것이 아닌지 의심 가는 상황이 발생했지만, 클라우드 환경이 익숙하지 않아 명확한 해결책을 찾지 못하고 있다. 정보보호 담당자가 의심하는 정황은 아래와 같다.

- o 내부 계정으로 클라우드 가상자원이 생성되었으나 해당 계정의 소유자가 생성하지 않음.
- o 일부 가상서버가 사용자가 없는 새벽 시간대에 급격하게 리소스 사용률이 늘어남.
- o 백신 소프트웨어 등으로 검사를 해 보았으나 특이사항을 발견하지 못함.
- o 개발 업무를 위해 개발자 PC에서 외부 깃허브에 접속할 수 있도록 허용이 되어 있으며, 과거에 개발자가 깃허브에 소스코드를 업로드 하는 과정에서 내부 인증 정보가 같이 업로드 되어 문제가 발생한 적이 있음.

정보보호 담당자는 현재 구성되어 있는 하이브리드 환경(클라우드, 온프레미스)에 대한 정보보호 아키텍처를 설계하고 클라우드 접근 권한 관리, 가상자원에 대한 가시성 확보, 모니터링 등 운영방안을 수립하고 싶다.

<전제 사항>

1. 일반사항
   - o 임직원 수는 200명이고, 보안 조직은 5명으로 구성되어 있음.
   - o 개발조직은 DevOPS로 구성되어 있으며, 모든 개발자가 클라우드 관리콘솔에 대한 권한을 보유하고 있음.
   - o 대부분의 임직원은 개발자로 구성되어 있어 아이디어가 있다면 자체 구축 가능함.

2. 서비스 구성
   - o 서비스는 클라우드, 온프레미스 하이브리드로 구성되어 있음.
   - o 서비스가 마이크로서비스 아키텍처로 구성되어 있어 클라우드 네트워크는 5개 이상의 VPC로 구성되어 있음.
   - o 서비스 운영을 위해 IaaS, PaaS, SaaS 서비스를 적절히 혼합해서 사용하고 있음.
   - o 어플리케이션은 도커, 쿠버네티스 등 컨테이너 환경으로 배포하고 있음.
   - o 일부 어플리케이션은 서버리스 환경에서 구동되고 있음.

3. 보안 현황

o 사내망

- 방화벽, IPS, NDLP, DRM, PC보안, 백신 솔루션, VPN이 구축되어 있음.

o 온프레미스

- 방화벽, DDoS, IPS, 백신 솔루션이 구축되어 있음.

o 클라우드 서비스

- Security Group으로 접근통제를 수행하고 있음.

o 사내망과 온프레미스망 사이, 온프레미스망과 클라우드 서비스망 사이는 전용선을 이용해 연결되어 있음.

<고려 사항>

o 배경 및 전제 사항에서 언급된 모든 사항이 누락 없이 아키텍처 수립대상에 포함해야함.

o 클라우드 제공 서비스, 써드파티 제품, 자체 구축 등 다양한 방법으로 정보보호 아키텍처를 구성할 수 있으며, 필요한 경우 조직 및 프로세스 재구성 가능.

o 정보보호 아키텍처는 개인정보보호법, 정보통신망법 등 관련 법률 요구사항을 충족해야함.

귀하는 클라우드 보안을 책임지고 있는 책임자입니다. 최적의 정보보호 아키텍처를 설계하고 클라우드 접근 권한 관리, 가상자원에 대한 가시성 확보, 모니터링 방안 등 클라우드 보안을 효율적으로 수행할 수 있는 관리적/기술적 운영방안을 수립하시길 바랍니다.