EQST insight

WFA 시대의 사이버보안 위협 대응을 위한 접근권한 제어 7 가지 전략

■ 개요

코로나 팬데믹으로 인해 일상 생활의 많은 변화가 일어났다. 특히 IT 분야에서는 오랜 시간 전통처럼 유지됐던 사무업무 환경이 변화해 불편함을 초래했다. 원격 업무 트렌드는 점차 가속화되어 확대되었으며, 현재는 지속가능한 하이브리드(혼합형)환경으로 자리를 잡아가고 있다.

하이브리드형 환경은 IT 기술을 적극적으로 사용할 때 구현된다. 비대면 업무를 위한 도구로 다양한 원격 회의 및 채팅 프로그램이 사용되고 있으며, 클라우드 기술을 이용한 협업도 이뤄지고 있다.

즉, 접속 채널이 많아 복잡한 하이브리드 환경은 뉴 노멀(새로운 기준)이 필요해짐을 의미한다. 사용자가 네트워크에 접속하는 방법, 사용자-장비 간의 다양한 구성에 대응하는 보안 정책 숙지, 변화하는 환경에 적절하게 통제하는 방법 등 새로운 엔드포인트 보안 전략이 필요한 시점이다.

■ WFA 로 인한 뉴 노멀(New Normal) 시대

하이브리드 업무 환경은 WFA(Work-From-Anywhere), 어디서나 근무할 수 있음을 의미하며 WFA 시대의 보안은 움직이는 데이터들을 보호할 수 있어야 한다. 공격자가 기업 데이터와 자산 탈취를 위해 주로 노리는 POLR 도 변화하고 있어 보안팀의 IT 위험관리 우선 순위도 바뀌어야 한다.

기존 IT 업계의 보안은 바이러스 백신과 방화벽을 최우선순위로 반영해 보안 환경을 구성했다. 그러나 바이러스 백신은 전체 사이버 공격의 60% 정도를 탐지하지 못하고, IoT 및 OT(Operation Technology) 환경에서는 백신 소프트웨어 설치조차 어려운 환경이다. 또한, 방화벽 정책 역시 늘어나는 클라우드 및 분산 컴퓨팅 환경으로 인하여 자주 무력화되거나 제 역할을 다하지 못하고 있는 상황이다.

또한, WFA 환경 구축에 있어 가장 까다로운 문제는 엔드포인트의 보안 문제다. 보통의 기업 네트워크 시스템에서는 방화벽을 활용해 외부에서 내부로 들어오는 접근을 차단하는 역할을 한다. 그러나, 저장된 데이터와 계정의 유출로 엔드포인트가 악성코드에 감염되어 있는 상황에서 사용자가 VPN 을 연결할 경우, 악성코드는 방화벽을 거치지 않고 내부 시스템으로 유입되어 네트워크까지 감염시킬 수 있다.

따라서, WFA 환경에서는 기존 보안 정책으로 외부 공격을 막기가 어려워지고 있으며, 다양한 보안 위협에 대비하기 위한 정책과 솔루션 구축이 요구되고 있다.

■ 접근 권한 제어 기반의 7 가지 보안 전략

디지털 환경을 구축한 조직은 보안 격차를 해결하고 능동적으로 위협 요소를 관리해야 한다. 최근 IT 보안은 새롭게 등장하고 있는 사이버 위협으로부터 대응하기 위해 네트워크 보안 전략으로 아이덴티티(Identity)를 기반으로 하는 '제로 트러스트(Zero Trust)'라는 핵심 보안 솔루션 모델을 제안하고 있다.

제로트러스트란(Zero Trust), '아무것도 신뢰하지 않는다'는 것을 전제로 한 사이버 보안 모델로, 사용자 또는 기기가 접근을 요청할 때 철저한 검증을 실시하고, 그 검증 과정에서 최소한의 권한만 부여해 접근을 허용하는 방식

기업이 제로 트러스트(Zero Trust)의 핵심 아키텍처 구성 요소를 구축하기 위해서는 PAM(Privileged Access Management)이라고 불리는 '특권 접근 관리'가 필수적이다. 권한 있는 액세스 관리 솔루션은 기업의 핵심인 가장 중요한 시스템과 자산을 보호하도록 설계되어 액세스 정책을 최적화할 수 있다.

사이버보안 생존 가이드 2022 (2022 Cybersecurity Survival Guide)[1]에서 급변하는 사무·업무 패러다임, 증가하는 위협 상황, 치밀한 사이버 범죄 전술 등 최신 보안 위협에 더 효과적으로 대응하기 위한 권한 제어 기반의 7가지 보안 전략을 제시하고 있다.

1. 권한 있는 계정 보호
모든 권한 있는 계정의 검색 및 보호 자동화
모든 권한 있는 자격 증명 보관 및 관리
적응형 액세스 제어(Enforce adaptive access controls)
권한 있는 계정 및 권한 있는 활동과 관련된 모든 세션을 지속적으로 모니터링
다중 인증 적용(MFA)
공유 계정 제거
내장된 암호 제거·삭제

2. 보안 원격 접속
단일 접근 경로를 통한 모든 연결 중개
접근 경로 및 기타 중요 소프트웨어에 대한 프록시 액세스
네트워크 구역화 및 세분화
최소 권한 액세스 제어
관리 자격 증명 자동 제어
BYOD 관리 구현
애플리케이션 수준의 마이크로 세분화
원격에서 시작된 모든 세션 모니터링, 관리 및 감사

3. 엔드포인트 권한 관리 적용
전체 환경에서 최소 권한 적용
특정 유닉스(Unix) 및 리눅스(Linux) 명령어 제어
직무 분리 및 권한 분리 시행
고급 애플리케이션 제어 및 최소 권한 애플리케이션 관리 적용
S/W 실행 및 설치 차단으로 보안 강화

[1] https://www.paloaltonetworks.com/resources/techbriefs/cybersecurity-survival-guide

4. 취약성 관리 및 경화(Hardening)
IT 환경 강화 BIOS 강화 및 보호 지속적인 취약점 관리 구현

5. 모바일 및 원격 엔드포인트 변조 방지
디스크 암호화 구현 내장형 하드 디스크 사용 장치 봉인 컴퓨터 보안 케이블 배포 및 사용 요구 BIOS 변조 방지 적용

6. 서비스 데스크 보안 및 권한 관리 강화
모든 원격 지원 세션에 대해 강력한 권한 있는 액세스제어 클라이언트 세분화 자격 증명 보안 모범 사례 구현 플랫폼 독립적 지원 활성화 워크플로를 간소화하고 다른 서비스 데스크 도구와 통합 원격 지원 도구와 함께 엔드포인트 권한 관리 배포

7. 원격 사용자 침투(모의 해킹) 테스트
개인, 가정 기반 네트워크 다른 회사가 소유한 장치 개인 및 IoT 장치 동일한 BYOD 자산에 있을 수 있는 개인 이메일 주소 휴대폰 번호 비사업용 소셜 미디어 계정

위의 7 가지 보안 전략이 필요한 보안 사고의 가장 큰 원인은 내부 사용자의 무분별한 권한 남용과 업무 PC 의 랜섬웨어 감염이다. 이를 대응하기 위해 사용자 환경, 엔트포인트 권한을 제어해 보안을 강화해야 한다.

사용자 환경인 엔드포인트의 최소권한 환경구축은 '언제', '어디서', '누가', '무엇을'과 같은 세밀한 항목을 정의하고, 이를 토대로 사용자 환경에 대하여 관리자 권한을 제거하는 등 업무 목적 및 권한 등에 적합한 명령어, 애플리케이션 실행 제어를 목표로 한다. 엔드포인트 권한 관리 적용은 이와 같은 목표 달성을 위한 필수 보안 툴이며 임의 실행되는 환경, 특히 랜섬웨어 실행 환경 차단에 효과적이므로 보안의 최우선이 되어야 한다

■ 제로트러스트(Zero Trust) 원칙의 실용적인 구현

앞서 제시한 7 가지 보안 전략을 충족하기 위해서는 NIST SP 800-207 에서 정의하는 제로트러스트 원칙을 스마트하고 실용적으로 지향하고, 복원 및 변화에 대응이 가능한 상태를 유지해야 한다. 또한, 원격 작업 및 디지털 전환에 필요한 보안 환경 구현을 위한 완벽한 특권 접속 관리 플랫폼(Privileged Access Management Platform)이 제공되어야 한다.

〈표 1〉 NIST SP 800-207 에서 정의하는 제로트러스트(Zero Trust) 원칙

제로트러스트(Zero Trust) 아키텍처란, 제로트러스트(Zero Trust) 개념을 사용한 기업 사이버 보안 계획이며, 컴포넌트간 관계, 워크플로우 설계, 액세스 정책이 포함된다. 또한, 제로트러스트(Zero Trust) 엔터프라이즈란 이러한 제로트러스트(Zero Trust) 아키텍처를 실행함으로써 기업에 존재하는 네트워크 인프라스트럭처(물리·가상) 및 정책을 의미한다.

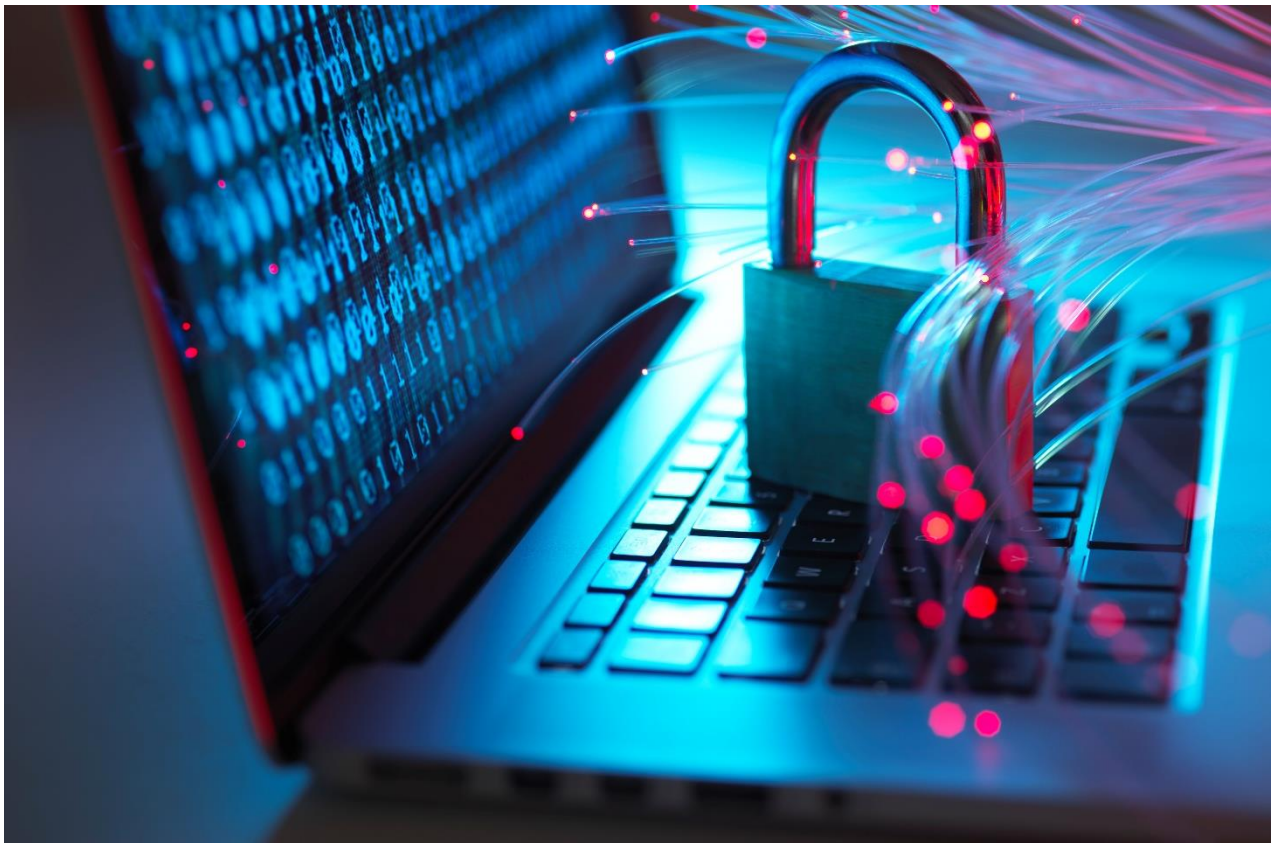
* 출처: 미국 NIST, "제로 트러스트 아키텍처", 2020[2]

[2] https://csrc.nist.gov/publications/detail/sp/800-207/final

■ 맺음말

개별·통합 구축이 가능한 플랫폼은 온프레미스(On-Premise), 클라우드 및 하이브리드 환경 모두 지원해야하며, 각각의 솔루션별로 구축하거나 통합 플랫폼의 일부로 함께 구축해야 보안 시너지 효과를 누릴 수 있고 한 단계 더 높은 수준으로 보안을 강화할 수 있다.

실제 A 사는 엔드포인트 솔루션 PAM(Privileged Access Management)을 도입하여 운영 중이며, 특히 원격자의 접속 권한을 통제하고 사용자 업무 PC 환경의 보안을 강화하고 있다. 이를 통해 제로트러스트 원칙에 충족하는 거버넌스와 컴플라이언스를 수행할 수 있으며, 보다 효과적인 IT 보안 구현이 가능하다.



> 우리는 확실하게
> "제로트러스트(Zero Trust)"의 시대에 진입했으며,
> 주변에서 일어나고 있는
> 기술의 변화에 따라 향상된 보안 환경을 구축해야 합니다.

■ 참고사이트

url: https://ponemonsullivanreport.com/2020/05/the-state-of-endpoint-security-risk-its-skyrocketing/