엔드포인트 보안과 제로 트러스트 기반 대응 전략 보고서

1. **제로 트러스트 보안 개요**

제로 트러스트(Zero Trust)는 “아무도 신뢰하지 말고 항상 검증하라”는 원칙에 기반한 보안 모델이다. 기존의 경계 기반 보안이 내부 사용자를 기본적으로 신뢰했던 것과 달리 제로 트러스트는 내부 및 외부 모두를 잠재적 위협으로 간주한다.

최근 LG유플러스, KT, SKT 등 국내 주요 통신사들은 제로 트러스트 기반 보안 아키텍처 구축에 수천억 원을 투자하며 실전형 대응 체계를 강화하고 있다.

주요 특징은 다음과 같다:

A. 지속적인 인증 및 검증: 사용자, 디바이스, 애플리케이션 모두 지속적으로 검증
B. 최소 권한 원칙: 필요한 리소스에만 접근 허용
C. 침해 가정 기반 대응: 이미 침해되었을 가능성을 전제로 보안 설계
D. 마이크로세그멘테이션: 네트워크를 세분화하여 수평 이동 차단

2. **엔드포인트 보안 취약점**

엔드포인트는 사용자의 디바이스(PC, 노트북, 스마트폰 등)로, 네트워크의 가장 취약한 지점 중 하나다. 특히 BYOD 환경, 원격 근무, IoT 확산으로 인해 공격 표면이 급격히 확대되고 있다.

IBM 보고서에 따르면 전체 사이버 공격의 90%가 엔드포인트에서 시작되며 데이터 유출의 70%가 엔드포인트 취약점과 관련되어 있다.

주요 취약점 유형은 다음과 같다:

취약점 유형	설명
악성코드 감염	이메일, 웹사이트, USB 등을 통한 감염 경로 다양화
파일리스 공격	메모리 기반 공격으로 탐지 회피
인증 정보 유출	브라우저 저장, 키로깅 등을 통한 크리덴셜 탈취
보안 패치 미적용	오래된 OS, 앱의 취약점 방치
내부자 위협	권한을 가진 사용자의 악의적 행위 또는 실수

3. **엔드포인트 보안 대응 방안**

A. 기술적 대응
   i. EDR 및 XDR 솔루션 도입: 실시간 위협 탐지 및 자동 대응
   ii. DLP 및 DRM 적용: 민감 정보의 유출 방지 및 문서 암호화
   iii. 애플리케이션 제어: 승인되지 않은 앱 실행 차단
   iv. 샌드박싱 및 메모리 분석: 파일리스 공격 대응

B. 운영적 대응

i. 보안 정책 수립 및 교육: 사용자 인식 제고

ii. 정기적 패치 및 취약점 스캐닝: 최신 상태 유지

iii. 제로 트러스트 연계: 엔드포인트 상태 기반 접근 제어

4. **엔드포인트 보안 및 제로 트러스트 기반 대응 전략에 관한 종합적인 고찰**

엔드포인트 보안은 단순한 기술적 문제를 넘어 조직의 보안 문화와 직결된 과제다. 아무리 강력한 솔루션을 도입하더라도 사용자의 실수나 내부자의 악의적 행위는 기술만으로 막기 어렵다.

제로 트러스트는 이러한 한계를 보완할 수 있는 전략이다. 특히 엔드포인트를 신뢰하지 않고 지속적으로 검증하는 구조는 내부자 위협과 파일리스 공격에 매우 효과적이다. 하지만 제로 트러스트의 도입은 단순한 기술 구현이 아니라, 조직 전체의 보안 인식 변화와 운영 체계의 재설계를 요구한다.

결론적으로 엔드포인트 보안은 제로 트러스트 모델과 결합될 때 가장 강력한 방어선을 구축할 수 있다. 기술적 대응과 함께 사람 중심의 보안 전략이 병행되어야 진정한 보안 체계가 완성된다.