EQST insight

제로 트러스트 시대(Zero Trust) – Never Trust, Always Verify

■ 개요

지난 5 월 헤드라인 'WFA(Work-From-Anywhere) 시대의 사이버보안 위협 대응을 위한 접근권한 제어 7 가지 전략'에서 언급된 제로 트러스트(Zero Trust)가 최근 사이버 보안분야에서 최대 화두로 떠올랐다. 이에 NIST[1] 제로 트러스트 가이드라인(SP 800-207)과 CISA[2] 제로 트러스트 성숙도 모델(Zero Trust Maturity Model, ZTMM)을 기반으로 제로 트러스트 도입 검토 단계에서의 고려사항과 계획 수립 시 참고사항을 설명하고자 한다.

클라우드 서비스 활용이 높아지고 코로나 팬데믹의 영향으로 원격근무가 생활화되면서 기업의 업무 환경은 대대적인 변화를 겪고 있다. 방화벽을 두고 기업의 내부망과 외부망을 구분 짓던 기존의 경계는 희미해지고, 다양한 유형의 디바이스가 등장함으로 인해 '신뢰할 수 있는 기기'를 구분 짓는 것도 점차 어려워지고 있다.

이제 보안을 위해 우리는 "모든 것을 의심하고 확인(Never Trust, Always Verify)"해야 하는 제로 트러스트(Zero Trust) 시대를 준비해야 한다.

[1] NIST (National Institute of Standards and Technology, 미국 국립표준기술연구소)

[2] CISA (Cybersecurity and Infrastructure Security Agency, 미국 사이버보안 및 인프라보안국)

■ 제로 트러스트의 개념 및 확장

2010 년 Forrester Research 에서 최초의 제로 트러스트 개념 및 모델이 제시됐다. 모든 접속 주체들을 신뢰할 수 없기 때문에 기업의 내부 자산에 대한 접근 권한 제한을 주장했다. 즉, 암묵적 신뢰가 보안 문제를 야기할 수 있으므로 신뢰 검증 결과에 의해서만 접근을 허용해야 한다는 의미다. 지금에 이르러서는 기술의 변화에 맞춰 개념이 확장되어 데이터 중심에서 사용자, 디바이스, 네트워크, 워크로드 등으로 대상이 확대되었으며, 이에 대한 가시성 확보, 분석, 자동화 및 통합 운영에 이르기까지 관련 범위도 늘어났다.

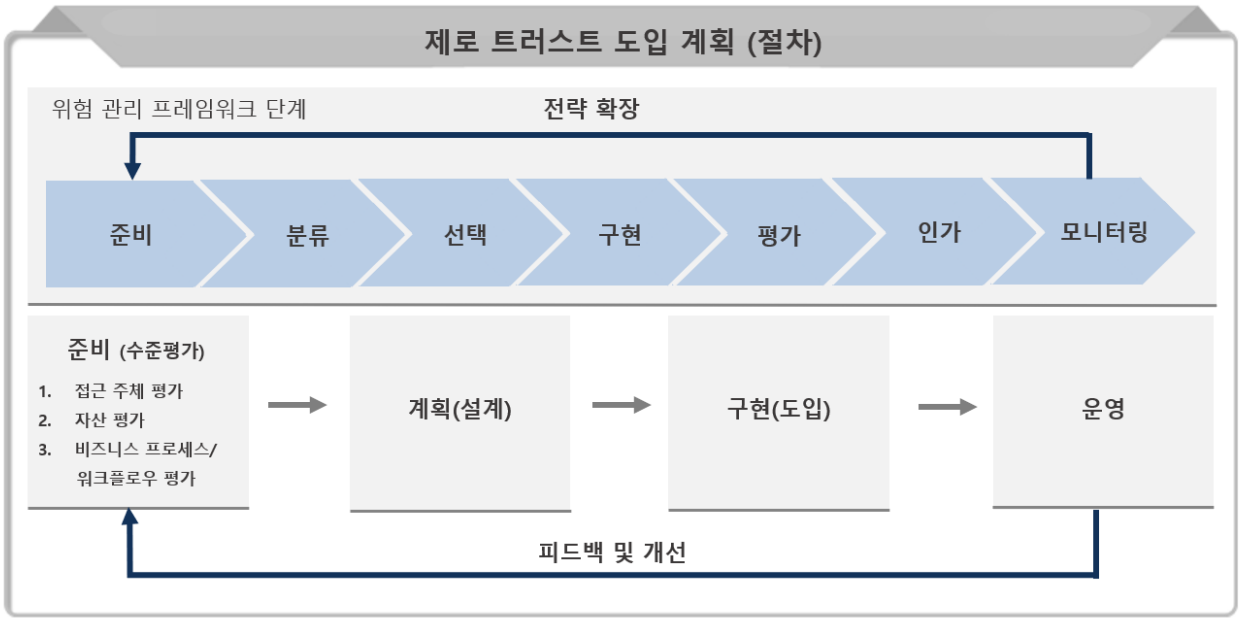
■ 제로 트러스트 도입 계획

기업에서 제로 트러스트를 적용하려고 할 때 먼저 고려해야 하는 사항은 제로 트러스트가 단일 기법이나 제품이 아닌 보안 정책에 사용되는 모든 원칙들의 집합이며, 따로 정해진 정답이 없다는 점이다.

미국 NIST 2020년 연례보고서에서는 '제로 트러스트 도입을 위한 가이드라인(NIST SP 800-207)'을 구현하기 위한 상세한 지침을 소개하고 있다. 특히 "기업별 활용 사례와 데이터 Asset 이 고유하므로 단일한 구축 플랜은 존재할 수 없다"고 설명하며, 그만큼 많은 자원, 시간, 소요예산 등이 필요하므로 충분한 검토 및 체계적인 준비를 요한다고 강조하고 있다.

사이버 보안 체계 구축을 위해서는 경영진의 적극적인 지원이 항상 우선시되어야 한다고 한다. 하지만 제로 트러스트를 구현하기 위해서는 기존의 '암묵적 신뢰' 기반의 시스템 접근 권한 부여가 아닌 컨텍스트(Context)에 맞도록 상시 평가하고 필요할 경우 재승인을 해야 한다는 기본 원칙이 전제되어야 하므로, 기존 인프라 시스템에 대한 변경이 불가피하다. 따라서 데이터 및 시스템 운영자, 사용자들의 적극적인 참여와 협력이 필요하다.

도입 계획 수립은 보유 자원에 대한 보안 위협을 줄이기 위한 절차로 NIST 위험관리 프레임워크(NIST SP 800-37)와 연계하여 검토를 진행한다.



* 출처: 과학기술정보통신부 제로 트러스트 가이드라인 이미지 재가공

[그림 1] 제로 트러스트 도입을 위한 세부 절차

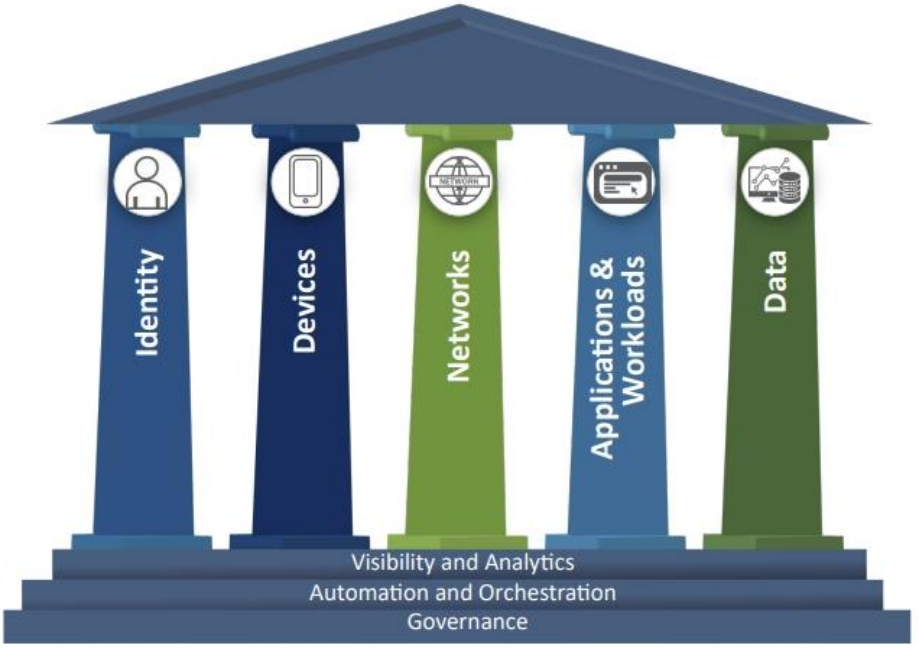
〈표 1〉 제로 트러스트 도입을 위한 세부 절차

준비	제로 트러스트를 도입하기 전 **핵심요소***를 중심으로 기업의 **현재 보안대상/수준****에 대한 평가 필요 * 식별자, 기기, 네트워크, 시스템, 응용 및 워크로드, 데이터 ** 접근 주체, 자산/기기, 비즈니스 프로세스/워크플로우 식별 및 성숙도 평가
계획	**성숙도 모델**을 기반으로 기존 보안체계와 **조화**를 이루어 **더 높은 수준**의 보안성 확보를 위한 **도입 설계 및 예산 검토**
구현	주요 자원의 **위치, 프로토콜***, 다양한 서비스 등을 고려하여 기업의 생태계에 적합한 **솔루션 검토 및 구현** * (자원 위치) On-Premise, Cloud 등, (프로토콜) 웹, SSH, IPv4, IPv6 등
운영	구현된 제로 트러스트 아키텍처에서 **기본철학***을 중심으로 **핵심원칙****이 적절하게 동작할 수 있도록 설정/관리 *모든 종류의 접근에 대해 신뢰하지 않을 것 *일관되고 중앙 집중적인 정책 관리 및 접근제어 결정/실행 필요 *사용자, 기기에 대한 관리 및 강력한 인증 *자원 분류 및 관리를 통한 세밀한 접근제어(최소 권한 부여) *논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용 *모든 상태에 대한 모니터링, 로그 기록 등을 통한 신뢰성 지속 검증/제어 **인증 체계 강화: 신뢰도 기반 인증 정책 수립 **마이크로 세그멘테이션: 보안 게이트 웨이를 통한 개별 자원 그룹 배치 **소프트웨어 정의 경계: 정책 엔진 결정에 따르는 네트워크 동적 구성, 사용자 신뢰 확보 후 자원 접근을 위한 채널 생성
피드백/개선	제로 트러스트 성숙도 기반의 **완성도 비교**, **모니터링** 및 **개선방안 도출** 등 각 단계의 **반복적 관리**를 통한 수준 고도화

* 출처: 과학기술정보통신부 제로 트러스트 가이드라인

■ 제로 트러스트 성숙도 모델 (Zero Trust Maturity Model, ZTMM)

제로 트러스트 성숙도 모델(ZTMM)은 제로 트러스트 모델 기반의 보안 개념이 잘 적용되어 운영되고 있는지를 객관적으로 표현하기 위한 모델이다. '성숙도'는 단번에 높은 수준으로 도달할 수 있는 것이 아닌 점진적인 변화를 통해 최적화 수준에 도달하는 형태로 발전하게 된다. 제로 트러스트 아키텍처를 설명할 때 기준이 되는 요소를 5 개의 기둥, 그리고 이 각각의 기둥에 공통으로 적용되는 교차 기능으로 도식화해 표현하고 있다.

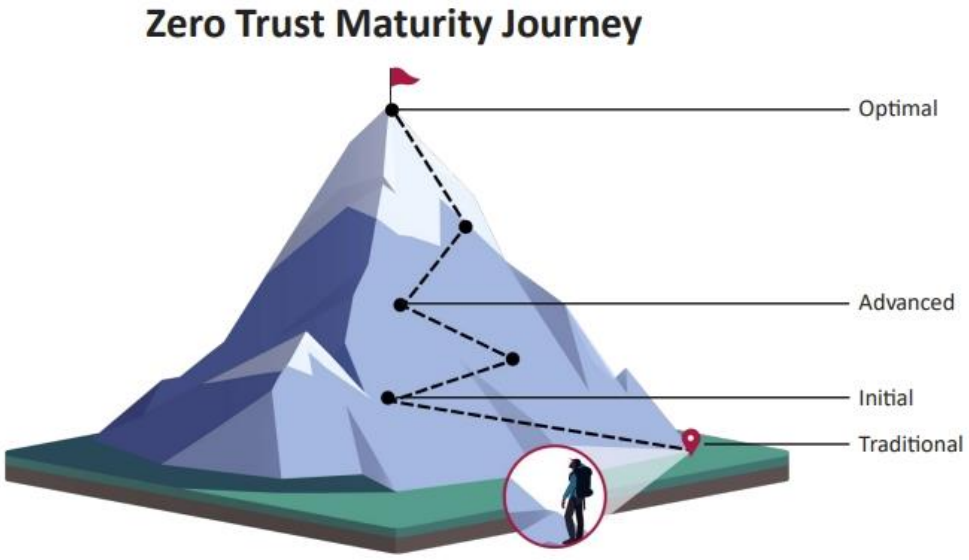


* 출처: 미국 CISA

[그림 2] CISA 제로 트러스트 성숙도 모델(ZTMM)

CISA 에 따르면, 제로 트러스트 구현 초기 단계에서 조직은 "5 개의 기둥(아이덴티티, 디바이스, 네트워크, 어플리케이션&워크로드, 데이터)에 대한 속성 할당 자동화 및 라이프사이클 구성, 정책 결정 및 시행, 외부 시스템 통합으로 초기 교차 기능"을 구축하는데 초점을 맞춘다.

23 년 4 월에 발표된 ZTMM 버전 2 에서는 아래 그림과 같이 성숙 단계를 버전 1 보다 세분화하여 기존 환경(Traditional), 초기(Initial), 고급(Advanced), 최적(Optimal) 4 가지 단계로 구분하였다.



* 출처: 미국 CISA

[그림 3] 제로 트러스트 성숙 단계

이는 전통적인 아키텍처에서 시작해 초급, 고급, 최적으로 향하는 과정이 간단한 과정이 아님을 의미한다. 초기 단계에서는 어떤 방법을 사용해도 지름길은 없다는 사실을 인식하고 측정할 수 있는 방식을 통해 점진적으로 초기단계에서부터 최적까지 달성해 나가야 한다는 것을 보여준다.

〈표 2〉 제로 트러스트 성숙도 단계별 수준/정의

구분	Traditional	Advanced	Optimal
User/Identity	* 암호 또는 다단계 인증(MFA) * 제한된 위험 평가	* MFA * 클라우드 및 온프레미스 시스템과의 일부 ID 연합	* 지속적인 검증 * 실시간 기계학습 분석
Device	* 규정 준수에 대한 제한된 가시성 * 단순 인벤토리	* 규정 준수 적용 * 데이터 액세스는 최초 액세스시 장치 상태에 따라 다름	*지속적인 장치 보안 모니터링 및 검증 * 데이터 액세스는 실시간 위험 분석에 따라 달라짐
Network	* 대규모 Macro Segmentation * 최소한의 내부 또는 외부 트래픽 암호화	* 수신/발신 마이크로 경계로 정의됨 * 기본 분석	*완전히분산된수신/발신마이크로경계 * 머신러닝 기반 위협 방어 * 모든 트래픽 암호화
Application	* 로컬 인증에 기반한 액세스 * 워크플로우와의 최소한의 통합 * 일부 클라우드 접근성	* 중앙 집중식 인증 기반 액세스 *애플리케이션워크플로우에 기본통합	* 액세스가 지속적으로 승인됨 * 애플리케이션 워크플로우에 대한 강력한 통합
Data	* 인벤토리 미흡(Not Well) * 정적 제어 * 암호화되지 않음	* 최소 권한 제어 * 클라우드 또는 원격 환경에 저장된 데이터는 유휴 상태에서 최소화	* 동적 지원 * 모든 데이터가 암호화 됨

* 출처: Canadian Centre for Cyber Security

■ 맺음말

그동안 사이버보안은 트렌드에 민감하게 반응을 해왔으며, 현재는 제로 트러스트라는 개념이 새로운 트렌드로 등장한 상태다. 기술이 발전하는 속도로 보았을 때 오랜 기간동안 트렌드를 주도할 것으로 보인다. 제로 트러스트 구현은 이제 선택이 아닌 필수다.

제로 트러스트는 네트워크 경계가 사라지고, 다양화·지능화되는 사이버 위협 속에서 기업의 보안 위협을 줄이는 수단으로 큰 도움이 될 것이다. '모든 것을 의심하고 확인한다'는 원칙 아래 빈틈없는 보안 환경을 구현해 가기를 희망한다.

■ 참고문헌

[1] NIST SP 800-207, “Zero Trust Architecture”, 2020.08

[2] CISA, “Zero Trust Maturity Model”, 2023.04

[3] 과학기술정보통신부, “제로 트러스트 가이드라인 1.0”, 2023.06