https://doi.org/10.33778/kcsa.2022.22.3.003

제로 트러스트 원리를 반영한 보안 강화 요소 기술 적용 방안 연구

이 다 인*, 이 후 기**

요 약

갈수록 정교해지는 사이버 위협, 클라우드 도입의 가속, 코로나19 팬데믹으로 인한 원격 및 하이브리드 근무환경 도입 등으로 인하여 많은 기업이 경계 안에 있는 모든 것을 암묵적으로 신뢰하는 전통적인 보안 모델이 경계가 존재하지 않고 데이터와 사용자가 갈수록 탈중앙화되는 오늘날 환경에 적합하지 않다는 사실이 부각되면서 제로 트러스트라(Zero Trust)는 개념이 갈수록 주목받고 있다. 제로 트러스트는 '아무도 신뢰하지 않는다'는 전제의 사이버 보안 모델로, 전체 시스템에서 안전한 영역 또는 이용자는 전무하다는 것을 원칙으로 내부 이용자도 검증을 거치며, 네트워크 접속 환경에 따른 정보 접근 범위도 차등 및 최소화하는 방안이다. 코로나19 팬데믹으로 인하여 재택근무가 일상화되고, 기존 사이버 보안방안이 한계에 부딪히면서 제로 트러스트(Zero Trust) 기술이 한층 더 주목을 받고 있다. 이에 따라 우리 정부도 NIST 표준을 참고로 제로 트러스트 도입 시 국내 공공 및 민간부문의 수용 가능성 현황, 개선이 필요한 과제 등을 점검할 것으로 예상된다. 이 논문에서는 이러한 제로 트러스트와 제로 트러스트의 기본원리, 철학, 고려사항에 대해 설명하고, 제로 트러스트의 기술을 접목시켜 보안을 강화하는 실무적인 기초 방안에 대하여 제시한다.

A Study on the Application of Security Reinforcement Technology Reflecting Zero Trust Principles

DA-IN Lee*, Hoo-Ki Lee**

ABSTRACT

With increasingly sophisticated cyber threats, accelerating cloud adoption, and the adoption of remote and hybrid work environments due to the COVID-19 pandemic, the traditional security model, in which many businesses implicitly trust everything within their boundaries, is changing without boundaries, allowing data and users The concept of zero trust is getting more and more attention as the fact that it is not suitable for today's increasingly decentralized environment has been highlighted. Zero Trust is a cyber security model on the premise that 'no one trusts'. In principle, there is no safe area or user in the entire system, and internal users are also verified. is a way As telecommuting becomes commonplace due to the COVID-19 pandemic, and existing cyber security measures are facing limitations, Zero Trust technology is drawing more attention. Accordingly, it is expected that the Korean government will also check the status of acceptability of the domestic public and private sectors and tasks that need improvement when introducing Zero Trust with reference to the NIST standard. In this paper, the basic principles, philosophy, and considerations of Zero Trust and Zero Trust are explained, and practical basic measures to strengthen security by combining Zero Trust technology are presented.

Key words : Zero Trust, COVID-19, NIST, technology

접수일(2022년 08월 30일), 수정일(2022년 09월 08일), 게재확정일(2022년 09월 26일)

* 티앤디 시큐리티

** 건양대학교/사이버보안학과(corresponding author)

1. 서론 및 연구 동향

최근 코로나로 인해 재택근무 등의 원격접속이 새로운 근무 형태로 자리를 잡게 되면서, 기존 사이버 보안방안이 한계에 부딪히고 있다[1]. 이러한 보안 환경의 한계점을 극복하기 위한 방법으로 제로 트러스트 접근통제 모델이 제안되었다[2]. 제로 트러스트는 '아무도 신뢰하지 않는다'는 전제의 사이버 보안 모델로, 사이버 보안 전문가이자 포레스터 리서치 수석연구원인 존 킨더버그(John Kindervag)가 2010년 제시한 개념이다[3]. 제로 트러스트 모델은 일반적으로 정보 서비스에 접근하는 주체의 보안 환경 수준에 대한 검증을 요구한다. 만약 접근 주체의 보안 환경이 충분히 안전하다고 판단할 수 없을 경우에는 검증된 주체라도 접근할 수 없으며[4], 모든 네트워크 트랜잭션이 이루어지려면 먼저 인증을 받아야 하고, 권한이 부여된 사용자와 장치만을 애플리케이션 및 데이터에 접속을 허용한다는 개념이다[5].

2020년 5월 미국은 인사관리처(OPM)의 협력업체인 키포인트 시스템즈(Keypoint systems)의 서버 접속 자격 증명을 가로채 이를 이용해서 서버에 접속하여 해킹을 시도하여, 미국 연방정부 공무원과 시민 2,150만명의 개인 신상정보가 유출된 것으로 드러났으며, 정보 유출 규모는 미국 역사상 최대로 추정된다. 2021년 5월 경 미국 콜로니얼 송유관 해킹으로 인하여 송유관 가동이 중단되는 대규모 해킹 피해가 발생했다. 전 미 정부 관계자와 업계 관계자들을 인용해 다크사이드가 '랜섬웨어' 공격으로 콜로니얼 파이프라인의 시스템을 해킹해 송유관 가동을 중단시킨 것으로 보인다고 보도했다. 결국 현재 사이버 보안 패러다임의 가장 큰 약점은 '기술의 취약성' 보다는 디지털 전환의 속도를 좇지 못한 낙후된 보안 정책과 내부자에 대한 무비판적 신뢰라는 것이다.

미국에서는 이미 미국표준기술연구소(NIST)가 '제로 트러스트 네트워크 액세스'(ZTNA) 표준 모델을 제시했고 민간에서도 MS(마이크로소프트)와 시스코, IBM 등 굴지의 ICT(정보통신기술) 기업들이 제품에 제로 트러스트 기능을 업데이트 하고 있는 상황이다.

조 바이든 대통령은 2021년 5월 국가 사이버 보안 개선에 관한 행정 명령(Executive Order on Improving the Nation's Cybersecurity 10428)을 발의하여, 연방정부와 클라우드 서비스 공급업체는 제로 트러스트 보안 정책을 채택하고 이에 따른 원칙과 프레임워크를 준수해야 하며, 2024년까지 연방정부의 사이버 보안을 현대화하고, 클라우드 서비스로의 전환을 가속화하기 위한 제로 트러스트 아키텍처를 요구하였으며, 각 기관장은 이를 구축하기 위한 계획을 60일 이내에 수립하도록 명령하였다.

미국 예산관리국(OMB)은 행정부 각 기관이 2024년 9월까지 제로 트러스트를 채택하기 위해 어떻게 움직여야 하는지에 대한 개요가 포함된 '제로 트러스트 사이버 보안 원칙을 향한 미국 정부 이동(Moving the U.S. Government Towards Zero Trust Cybersecurity Principles)'을 포함해 이 전략과 관련된 여러 문서 초안을 발표했다. 또한, CISA 는 기관이 제로 트러스트 아키텍처로 전환할 때 참조할 수 있도록 '제로 트러스트 성숙도 모델'을 발표하였는데, 성숙도 모델은 OMB 의 Federal Zero Trust Strategy 를 보완하며 기관에 최적의 제로 트러스트 환경을 달성하기 위한 로드맵과 리소스를 제공하도록 설계되었으며, Identity(신원), Devices(디바이스), Network(네트워크, Application Workload(응용프로그램 작업)의 내용이 포함된다. 국가안보통신자문위원회(National Security Telecommunications Advisory Committee, NSTAC)는 연방 제로 트러스트 전략(Federal Zero Trust Strategy)이 발표된 직후 '제로 트러스트 및 신뢰할 수 있는 ID 관리 보고서(Zero Trust and Trusted Identity Management report)'를 발표했으며, 이 보고서에는 민간 분야에서 시작된 제로 트러스트의 역사와 정부 기관에서 꾸준히 내놓고 있는 다양한 제로 트러스트 관련 활동과 지침, 요구사항이 잘 요약돼 있다. 대표적인 것이 '행정 명령(Executive Order) 14028 : 국가 사이버보안 개선'이다. 이 행정 명령에 따라 NSTAC 는 제로 트러스트 및 신뢰할 수 있는 신원 관

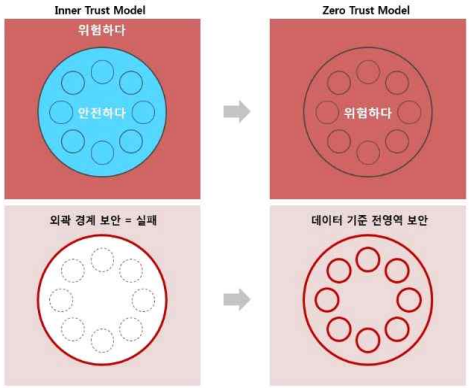
리를 포함한 주요 이슈에 초점을 맞추었다. 또한 보고서는 제로 트러스트 구현의 과제와 실현을 위한 조건을 강조했다. 적절한 감독 및 성숙도 지표, 투명성, 그리고 지속적 개선에 집중해야 할 필요성과 같이 모두 연방 정부뿐 아니라 민간 분야에도 적용되는 조건이다. 공공 및 민간 분야의 보안 리더가 NSTAC 보고서에서 주목해야 할 8가지 핵심적인 내용을 정리했다. 이에 따라 우리 정부도 NIST 표준을 참고로 제로 트러스트 도입 시 국내 공공 및 민간부문의 수용 가능성 현황, 개선이 필요한 과제 등을 점검할 것으로 예상된다.

본 연구에서는 대표적인 제로 트러스트 반영 모델들을 대상으로 접근 방법과 구조, 적용 전략 등을 종합 정리한다. 이를 통하여 제로 트러스트 기본원리를 반영한 보안 강화 방안과 고려사항 등을 제시한다.

2. 선행연구

2.1 제로 트러스트 기본 모형

제로 트러스트 기본 모형은 시스템 전체를 한꺼번에 지켜야 할 하나의 큰 덩어리로 보지 않고 모든 부분들을 '미세 분할(micro segmentation)' 요소로 나누고, 각 요소에 대하여 '과립형 경계 시행(granular perimeter enforcement)' 방식으로 보안을 적용해야 한다.



(그림 1) 제로 트러스트 기본 모형

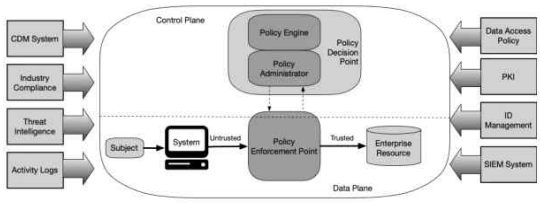
'비경계 기반의 보안 모델(Un-perimeter based Security Model)'인 제로 트러스트는 해당 모델이라 정의되기 위해 충족하여야 하는 조건을 보유하고 있는데, 다수의 기관에서 입을 모아 이야기하고 있는 조건은 '식별하고, 검증하고, 확인하는 단계를 통해 최소한의 접근만을 허가' 한다는 내용을 공통된 골자로 삼고 있으며, 아래 <표 1>과 같은 4가지 조건을 충족시켜야 한다,

<표 1> 제로 트러스트 충족조건

순번	조건
1	Identify business-based data
2	Internal design of assets and data to be protected
3	Permission setting based on minimum access rights
4	Inspection and logging of all traffic

2.2 NIST 800-207

NIST 는 제로 트러스트에 대한 개념을 실체화하기 위하여, 제로 트러스트 모델 적용을 위한 구축 전략과 운영 조건, Framework 수준의 구조를 제안하였다. NIST 는 제로 트러스트 논리 구성요소를 다음 (그림 2)와 같이 정의하였으며, 각각 정책 엔진, 정책 관리자, 정책 시행시점으로 분류하였다[6].



(그림 2) NIST Zero Trust Logical Components

정책 엔진(Policy Engine)은 엔터프라이즈 정책, 외부소스의 입력 및 신뢰할 수 있는 알고리즘을 기반으로 사용자, 디지털기기 또한 어플리케이션 사용자에게 액세스 권한을 부여하는 궁극적인 정책을 결정하며, 정책 관리자(Policy Administrator)는 사용자와 대상 리소스 간의 통신 경로를

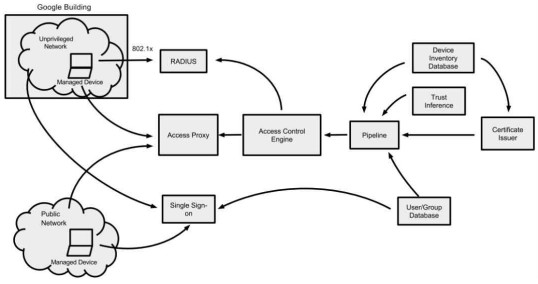
설정하거나 종료할 책임을 가지며, 엑세스 권한 부여에 대한 정책 엔진의 최종승인을 받으면 정책 시행 지점이 사용자 엔터프라이즈 리소스에 액세스 하는데 사용되는 인증정보, 키 또는 토큰을 통해 세션 시작을 명령한다. 정책 시행시점(Policy Enforcement Point)는 전체 통신경로의 게이트웨이 역할을 수행하며, 사람, 시스템, 어플리케이션과 대상 엔터프라이즈 리소스 간에 세션 활성화, 모니터링 시작 및 종료하는 역할을 담당한다[7].

2.3 제로 트러스트 반영 모델

제로 트러스트를 반영한 실제 모델로는 구글의 비욘드코프(BeyondCorp)를 통하여 구현 가능성을 보여주었으며, 그 외에도 Forrester 의 Zero Trust eXtended, MS 의 Azure Active Director 등을 제시하였다.

2.3.1 구글 비욘드코프(BeyondCorp)

비욘드코프(BeyoundCorp)는 구글의 네트워크 구축 경험을 바탕으로 전통적인 VPN 을 사용하지 않고 접근제어 기능을 네트워크 기반이 아닌 사용자 개인 기기 기반으로 수행할 수 있는 제로 트러스트 환경을 가리킨다. 구글의 비욘드코프(Beyond Corp) 모델은 방화벽이나 VPN 과 같은 전형적인 보안 장비 없이 기기, 사용자 인증을 비롯한 다양한 요소를 분석한 결과만으로 접근 제어를 수행한다는 것이 특징이며, 기능을 크게 세가지로 분류할 수 있다.



(그림 3) 구글의 비욘드코프 구성요소

첫 번째, 구글의 임직원용 시스템 서비스는 인증된 기기에서만 접속이 가능하며, 사용자 기기에 관련된 다양한 정보를 수집하고 분석하여, 안전한 기기에서만 접근을 허용하도록 검증하고, 다음으로는 사용자를 인증하며 기기 인증과 마찬가지로 사내 시스템은 인가된 사용자에게만 접속이 허용된다. 두 번째, 모든 User 및 Group 데이터베이스와 연동되어 있어 사용자명, 소속, 그룹, 업무 카테고리, 사용자 근무 위치 정보를 반영하여, 임직원의 업무가 변경되거나 퇴사 등 인사 변경이 발생하게 되면 즉시 DB 에 반영되어 시스템 접속 허용 여부를 결정한다. 세 번째, 접근제어 엔진이 위에서 언급한 다양한 요소를 분석/판단하여 접속을 허용하거나 차단하는 역할을 수행한다.

2.3.2 Forreste ZTX(Zero Trust eXtended)

2018년 포레스터 리서치(Forrester Research)의 수석 애널리스트 체이스 커닝햄 (Chase Cunningham)은 프로세스와 기술을 결합한 총체적인 접근 방식의 변화를 통해 보다 발전된 형태의 제로 트러스트 모델인 ZTX(Zero Trust eXtended)를 발표한다.

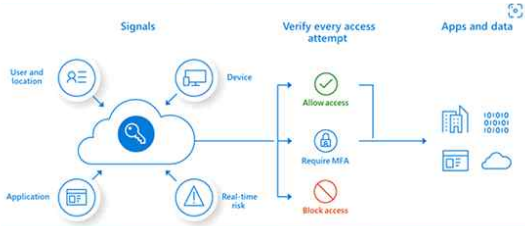
(그림 4) Forreste ZTX 구성요소

2010년도에 제로 트러스트의 컨셉을 이야기할 때는 네트워크에 집중되어 보안 모델을 이야기하였으나, 이제까지의 경계선 보안(Perimeter Security)의 실패로 더 이상 네트워크뿐만이 아닌 영역을 넓혀서 데이터와 아이덴티티 중심으로 전환하

여야만 디지털 환경에서의 비즈니스 요구 사항을 충족시킬 수 있다고 언급하였다.

2.3.3 MS 액티브 디렉터리(Azure Active Directory)

마이크로소프트의 액티브 디렉터리(Azure Active Directory)는 ID를 기반으로 사용자 인증을 진행하고, 싱글사인온을 통해 기업 ID로 클라우드 접속을 진행하며, 이와 동시에 MFA를 통해 보안키, 지문, 얼굴 등을 인증하는 구조로, 다음 (그림 5)와 같이 제시되었다.

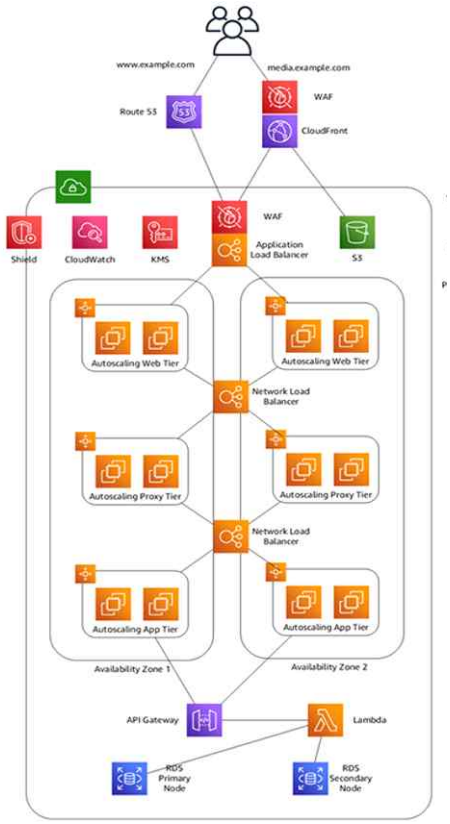


(그림 5) MS 액티브 디렉터리 구조

모든 액세스 요청은 보안을 위반하며, 내/외부 접근 구분 없이 개방형 네트워크에서 발생했다고 가정하였으며, 요청의 시작 위치나 액세스하는 리소스와는 무관하게 무조건 신뢰하지 않고 항상 확인해야 한다고 설명하였다. 또한, 모든 액세스 요청은 액세스 권한을 부여하기 전에 완전히 인증, 승인 및 암호화가 되며 측면 이동을 최소화하기 위해 마이크로 세분화 및 최소 권한 액세스 원칙이 적용되며, 풍부한 인텔리전스와 분석을 활용해 이상 현실을 실시간으로 감지하고 대응한다는 것이 주요 특징이다.

2.3.4 AWS 제로 트러스트 아키텍처

AWS에서는 클라우드 환경에서의 제로 트러스트 보안이 적용된 아키텍처를 다음 (그림 6)과 같이 설계하였다. 각 모델에서 일관된 트래픽 흐름을 제공하도록 구현이 필요하며, Amazon Cloud Watch Anomaly Detection을 구현하여 머신 러닝(ML) 일고리즘을 사용해 비정상적으로 많은 네트워크 트래픽을 생성하는 특정 리소스에 대한 탐지를 수행하고, Amazon SNS(Simple Notification Service)를 사용해 대상 항목에 자동으로 위협을 알리며, 위협이 발생한 리소스를 제거하고 동작을 중지한 다음, 그룹으로부터 분리하여 추가 분석을 수행할 수 있는 Amazon Lambda 기능을 구현하였으며, AWS KMS(Key Management Service)를 활용하여 정보 노출, 변조 및 거부를 방지하기 위해 암호화 및 최소한의 권한을 부여하여 제어한다는 것이 주요 핵심이다.



(그림 6) AWS의 제로 트러스트 웹 호스팅 아키텍처

3. 구현 조건

미 국가안보통신자문위원회(National Security Telecommunications Advisory Committee, NSTAC)에서 발표한 '제로 트러스트 및 신뢰할 수 있는 ID 관리 보고서(Zero Trust and Trusted Id

entity Management report)'에서는 제로 트러스트 구현의 과제와 실현을 위한 조건을 정리하였으며, 해당 내용은 다음과 같다.

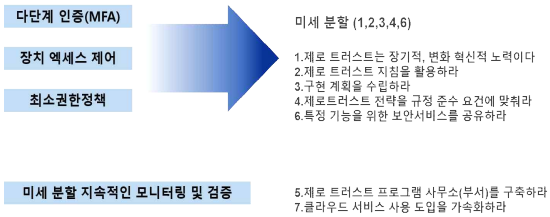
첫 번째, 제로 트러스트는 장기적 변혁적 노력이다. 가장 중요한 점은 제로 트러스트가 10년 이상의 장기적인 노력을 필요로 하는 변혁적인 활동임을 인식하는 것이다. 제로 트러스트 문화를 이끌고 조직의 기술 시스템 체계를 근본적으로 재설계하는 방대한 작업을 시작하기 위한 산업 및 조직 정책 변화도 필요하다. 두 번째, 제로 트러스트 지침을 활용하여야 한다. 제로 트러스트에 대한 지식을 갖추려면 잘 정립된 지침과 자료를 찾아보면 된다. 다양한 제로 트러스트 지침과 문서를 통해 기업은 연방 정부처럼 대형 기관을 끌어들이는 제로 트러스트의 특성과 권장 사항, 각 정부의 목표를 잘 이해할 수 있다. 세 번째, 구현 계획을 수립하라. 모든 장기적이고 전략적인 프로젝트가 그렇듯이 제로 트러스트 구현에도 계획이 필요하다. NSTAC 지침은 제로 트러스트 구현을 위한 5단계(보호 표면 정의→트랜잭션 흐름 매핑→제로 트러스트 아키텍처 구축→제로 트러스트 정책 마련→네트워크 모니터링 및 유지)를 제안한다. 네 번째, 제로 트러스트 전략을 규정 준수 요건에 맞추어라. 제로 트러스트를 추구하는 것이 지난한 과정인 것은 부정할 수 없다. 비용, 시간, 노동력 투입이 필요한 과정이다. 다섯 번째, 제로 트러스트 프로그램 사무소를 구축하여라. 제로 트러스트 프로그램 전담 사무소, 주요 영역의 공유 서비스 사용 최대화도 권장 사항이자 제로 트러스트 실현을 위한 요건이다. 여섯 번째, 특정 기능을 위한 보안 서비스를 공유하라. 중앙 프로그램 사무소를 기반으로 인터넷 액세스 자산 검색과 같은 특정 기능을 위한 보안 서비스를 공유하는 것이 좋다. 일곱 번째, 클라우드 서비스를 사용하여 도입을 과속화하여라. NSTAC 는 “클라우드 서비스의 빠른 도입은 연방 기관의 제로 트러스트 도입을 대폭 가속화할 것”이라고 언급했다. 클라우드의 이점은 데이터, ID, 자동화 같은 모든 분야를 포괄한다. 또한 클라우드 도입은 원격 인력의 증가에 대처해야 하는 기관과 조직에도 도움이 될 수 있다. 여덟 번째, 성공적인 제로 트러스트 환경 구축을 위해서는 효과적인 신원관리가 필수이다. 마지막 핵심 내용은 ID 가 제로 트러스트에서 근본적인 요소라는 점이다. 사람뿐 아니라 사람이 아닌 개체 모두 ID 에 포함된다. 지침은 연방 및 민간 분야 조직이 직면한 현대 클라우드 네이티브 및 원격 인력 환경에 대응하는 현대적 ID 관리 솔루션의 필요성을 강조한다[8]. 지금까지 살펴본 내용은 제로 트러스트 도입의 기회와 과제에 대한 권장 사항과 유용한 정보 가운데 일부로, 이렇듯 제로 트러스트는 단기간 내에 구현하기 어렵고, 10년 이상의 중장기적인 노력을 걸쳐서 TF 나 전담 부서를 설립하는 것이 효과적이다. 또한, 효과적인 신원관리가 무엇보다 중요하다. 그렇기 때문에 효과적인 신원관리와 구현을 위해서는 아래 <표 2>와 같은 장기적이고 전략적인 구현 계획이 필요하다.

<표 2> 제로 트러스트 구현 계획

순번	내용
1	Defining Your Protect Surface (보호 범위 정의)
2	Map the Transaction Flows (트랜잭션 흐름 매핑)
3	Build a Zero-Trust Architecture (제로 트러스트 아키텍처 구축)
4	Create Zero Trust Policy (제로 트러스트 정책 만들기)
5	Monitor and Maintain the Network. (네트워크 모니터링, 유지관리)

4. 제로 트러스트 기술 적용 보안 강화 방안

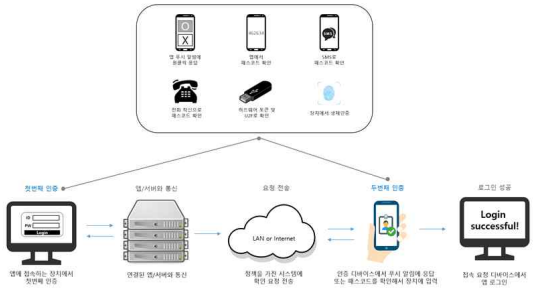
제로 트러스트는 새로운 기술이 아닌 기존 기술과 작은 기술의 추가로 보안전략을 세울 수 있다. 위에서 언급한 제로 트러스트 구현 방안 8가지 철학을 그룹핑하여, 아래 (그림 7)와 같이 다단계 인증, 장치 액세스 제어, 최소권한정책, 미세분할 지속적인 모니터링 검증의 제로 트러스트 기술 요소와 접목시킬 수 있다.[11]



(그림 7) 제로 트러스트 철학 그룹핑

4.1 다단계 인증(MFA)

다단계 인증은 사용자가 이미 가지고 있는 속성들을 활용하여 인증하는 방식이다. 시스템이 요청하여 사용자가 응답하는 프로세스에서는 인증을 통하여 사용자가 맞음을 증명할 수 있을 때 인증이 완료된다. 단계별로 인증이 진행되면서 보안 안정성이 요구되는 서비스에서 활용할 수 있다[9]. 아래 다단계 인증(MFA) 예시에서 확인할 수 있듯이, 생체인증, 패스코드, 토큰 등의 인증방식을 통하여 다단계 인증을 수행할 수 있다.



(그림 8) 다단계 인증(MFA) 예시

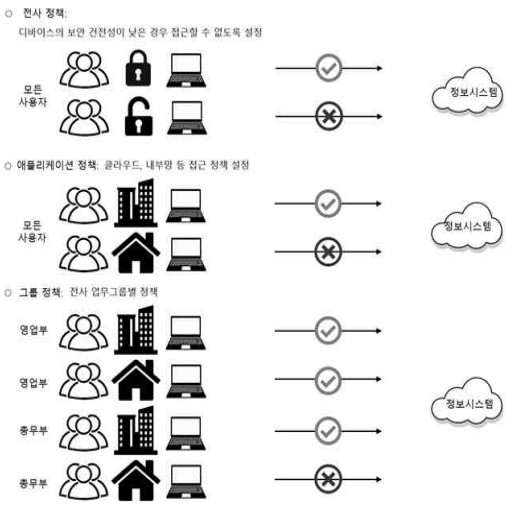
4.2 장치 액세스 제어

장치 액세스 제어란 인증을 시도하는 모든 장치를 제어하는 기술을 의미하며, 디바이스 정보 파악, 취약점 점검, 보안 패치 관리 등을 수행하여, 인증 시도 및 접속 기기에 대한 제어를 수시로 진행하여야 한다. 위에서 제시한 다단계 인증(MFA)을 수행할 때도 장치 액세스 제어 기술을 추가로 접목시켜 보안성을 강화하여야 한다. 예시로는 (그림 9)와 같이 대시보드를 통해 디바이스 정보를 파악하거나, 사용자 접속 기기에서 보안 상태 등을 확인하는 기술 등이 있다.

(그림 9) 장치 액세스 제어 예시

4.3 최소권한정책

제로 트러스트 보안의 핵심은 불법적인 접근이나 사용자를 찾아내 차단하는 것이 아니라 접근하려는 주체에 대한 엄격한 검증과 최소한의 접근을 허용해 해당 주체만을 집중적으로 감시하는 것이다[10]. 최소권한정책이란 접근하는 서버에 대하여 최소한의 정책 권한을 주어, 관리하는 기술을 의미한다. 아래 예시 그림과 같이 전사 정책, 애플리케이션 정책, 그룹 정책 등으로 분류하여 지속적인 정책 확인 및 모니터링이 중요하다.

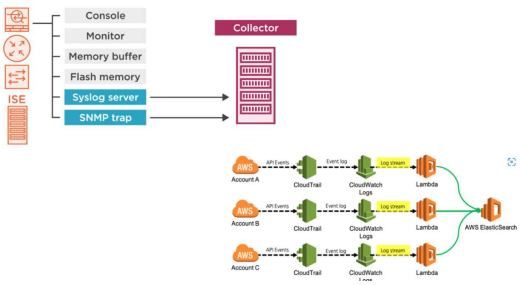


(그림 10) 최소권한정책 예시

4.4 미세 분할 지속적인 모니터링 및 검증

미세 분할 지속적인 모니터링 및 검증은 위에서 언급한 기술들과 정책, 그리고 보안 안정성 등

을 지속적으로 모니터링 및 검증하는 단계로 로그 확인, 사용자 인증강화, 기기 검증, 권한 관리, 통합·중앙화와 같은 방안이 존재하며, 각각의 서버에 대한 지속적인 보안 관리 또한 중요하다.



(그림 11) 미세 분할 지속적인 모니터링 및 검증 예시

5. 결론

갈수록 정교해지는 사이버 위협, 클라우드 도입의 가속, 코로나19 팬데믹으로 인한 원격 및 하이브리드 근무환경 도입 등으로 인하여 많은 기업이 경계 안에 있는 모든 것을 암묵적으로 신뢰하는 전통적인 보안 모델이 경계가 존재하지 않고 데이터와 사용자가 갈수록 탈중앙화되는 오늘날 환경에 적합하지 않다는 사실이 부각되면서 제로 트러스트라는 개념이 갈수록 주목받고 있다.

본 연구에서는 제로 트러스트의 기본원리를 통하여 보안강화 기초 방안을 연구하였다. 제로 트러스트의 정의와 개념, 기본원리에 대한 개요를 제시함과 동시에 구글 비욘드코프, Forreste ZTX 등 다양한 제로 트러스트 모델을 제시하였다. 또한. 제로 트러스트 구현 조건으로 8가지 원리를 제로 트러스트 요소 기술과 그룹핑하여 다단계 인증(MFA), 장치 액세스 제어, 최소권한정책, 미세 분할 지속적인 모니터링 검증 4가지로 분류하여 연구를 수행하여 실무적인 보안강화 방안을 제시하였다. 이 연구를 토대로 제로 트러스트 기반의 보안기술 활용의 실현으로, 보이지 않는 위협을 예방하고 한층 더 강화된 보안 체계를 구축할 수 있을 것을 희망한다.

참고문헌

[1] Daesung Lee, “A Study on Strategies for Applying Zero Trust”, Catholic University of Pusan, p.387-396, 2021.

[2] Sung-Hwa Han, Hoo-Ki Lee. “Real-Time File Access Event Collection Methodology for Zero Trust Environment”, Journal of the Korea Institute of Information and Communication Engineering, vol.25, no.10, 2021.

[3] Min-Hyuck Ko, Daesung Lee, “Zero Trust-Based Security System Building Process”, Journal of the Korea Institute of Information and Communication Engineering, vol.25, no.12, 2021.

[4] Kindervag John, “Build security into your network’s dna: The zero trust network architecture.”, for Security & Risk Professionals, 2010.

[5] Daesung Lee, “A Study on Zero Trust Building Process”, Catholic University of Pusan, 2021.

[6] Hyun-jin Lee, Kyung-hoSon, “A Study on a Smart City Supply Chain Security Model Based on Zero-Trust”, Journal of The Korea Institute of Information Security & Cryptology, vol.32, no.1, 2022.

[7] Scott Rose, Oliver Borchert, Stu Mitchel,l Sean Connelly, “NIST Special Publication 800-207 Zero Trust Architecture”, National Institute of Standards and Technology, 2020.

[8] NSTAC, “Zero Trust and Trusted Identity Management report”, 2021.

[9] Semin Kim, Sunghyuck Hong, “Design of Multi-Step Authentication Method using Blockchain”,Jeonju National University of Education·Baekseok University, 2021.

[10] Seon-A Lee, Beomseok Kim, Hyein Lee, Wonhyung Park, “An Enhancement of The Enterprise Security for Access Control based on Zero Trust”, Journal of the Korea Institute of Information and Communication Engineering, vol.26, no.2, 2022.

[11] Hoo-k Lee, Cultureinfomation issuere-port(2022-06), 2022

〔저자소개〕

이 다 인 (DA-IN Lee)
㈜티앤디시큐리티 연구원
관심분야 : 악성코드 분석, 보안관제 시스템, 클라우드 보안, 디지털포렌식, 시스템 보안
email : dilee@tndsecurity.com

이 후 기 (Hoo-Ki Lee)
건양대학교 사이버보안학과 교수
숭실대학교 공학박사
정보보호영재교육원 부원장
관심분야 : 침해지표 연구, 제로 트러스트 보안, 지능형 보안관제시스템, 악성코드 분석
email : hk0038@konyang.ac.kr