문화정보 이슈리포트
2022-6호(제36호)

제로 트러스트 보안기술 동향과 적용방안

이후기
(건양대학교 사이버보안학과 교수)

KCISA 한국문화정보원

CONTENTS

문화정보 이슈리포트
2022-6호(제36호)

제로 트러스트 보안기술 동향과 적용방안

이후기(건양대학교 사이버보안학과 교수)

요약

클라우드, 빅데이터, IoT 등 4차혁명을 이끌고 있는 핵심 ICT 기술들은 국가 경제 사회 인프라 전반에 걸쳐 통합화되어 활용되고 있으며, 정보시스템 인프라 서비스 이용에 따른 보안 위협도 지속적으로 발생하고 있어, 그에 따른 피해도 크게 증가하고 있다. 기존에는 보안을 강화하기 위한 방안으로 경계 기반 접근 통제 보안이 가장 활발히 활용되었으나, 코로나19로 인한 비대면 접속 기술, 클라우드 전환에 따른 원격 접속, 데이터 활용 등의 발전으로 경계 기반 보호의 핵심인 신뢰/비신뢰 접근통제에서 접근 주체의 보안 환경에 악성행위가 은닉되어 많은 사이버보안 침해사고가 발생하고 있다. 따라서, 누구도 믿을 수 없다란 개념이 적용되어 정보시스템 서비스에 접근하는 모든 주체를 악의적 공격자로 간주하고 검증된 주체 대상으로 최소 권한만을 허용하는 제로 트러스트 모델이 제안되었다. 제로 트러스트 보안기술 모델은 10여년전 발표한 비경계 접근 통제 모델로써, 정보시스템 서비스에 접근하는 주체의 보안 환경 수준에 대한 인증과 검증을 지속적으로 요구한다. 이러한 제로 트러스트 보안기술의 동향과 원리를 알아보고, 그에 따른 실체적 적용 방안을 제시한다.

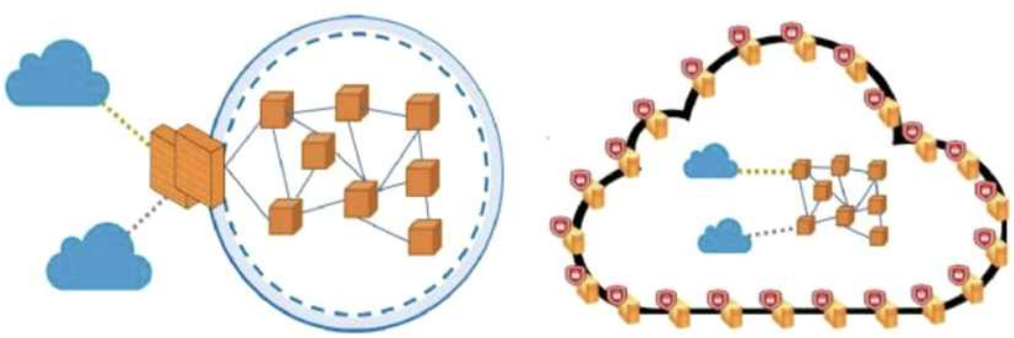
KCISA 한국문화정보원

I. 제로 트러스트 개요 및 동향

1. 제로 트러스트 정의

○ '제로 트러스트'(Zero Trust)는 "아무것도 신뢰하지 않는다"를 전제로 한 사이버 보안 모델로, 외부 접속자뿐만 아니라 내부에 접속한 사용자에 대해서도 무조건적으로 신뢰하지 않고 검증하는 것을 기본으로 하는 개념임.

- 즉, 사용자 또는 기기가 접근을 요청할 때 철저한 검증을 실시하고, 그 검증이 이뤄진다 해도 최소한의 신뢰만 부여해 접근을 허용하는 방식을 함.
- 해당 용어는 2010년 사이버 보안 전문가이자 포레스터 리서치 수석연구원인 존 킨더버그(John Kindervag)가 제시한 개념으로, '신뢰가 곧 보안 취약점'이라는 원칙을 내세운 것임.
- 또한, 2020년 5월 NIST(미국표준기술연구소)가 발표한 제로 트러스트 아키텍쳐 기술서(800-207)에 의해 기술이 일부 정립되었으며, 단순한 내·외부 혹은 동일 네트워크에 대한 수평적 통신 이동 경계를 넘어서 과립형 경계 보안이라는 개념이 구체화 됨.



〈그림 1〉 제로 트러스트 엣지 보안 모델

자료: Akamai

2. 제로 트러스트 동향

○ 최근 미국을 대상으로 대규모 해킹 피해 공격이 지속적으로 발생하면서, '제로 트러스트'(Zero Trust) 보안의 필요성이 강조됨.

- 2020년 12월, 핵안보위원회, 에너지위원회, 재무부, 상무부, 국토안보부 등 미 정부기관 다수를 대상으로 해킹 공격에 의한 개인정보유출, 자료유출 등의 침해사고피해가 지속적으로 발생함.
- 2021년 5월, 미국 최대 송유관 업체 랜섬웨어 공격으로 인하여 송유관 가동이 중단되는 대규모

해킹 피해가 발생함.

- 결국, 현재 사이버 보안의 최대 취약점은 '기술적 취약성' 보다는 디지털 전환의 속도를 쫓지 못한 낙후된 보안 정책과 내부자에 대한 무비판적 신뢰라고 인식함.

○ 美 조 바이든 대통령은 2021년 5월 **국가 사이버 보안 개선에 관한 행정 명령 (Executive Order on Improving the Nation's Cybersecurity 10428)**을 발의함.

- 연방정부와 클라우드 서비스 공급업체는 제로 트러스트 보안 정책을 채택하고 이에 따른 원칙과 프레임워크를 준수해야 함.
- 2024년까지 연방정부의 사이버 보안을 현대화하고, 클라우드 서비스로의 전환을 가속화하기 위한 제로 트러스트 아키텍처를 요구함.
- 각 기관장은 이를 구축하기 위한 계획을 60일 이내에 수립하도록 명령하는 강력한 행정명령 조치를 발의함.

Executive Order on Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

〈그림 2〉 美 조 바이든 대통령은 국가 사이버 보안 개선에 관한 행정 명령 (Executive Order on Improving the Nation's Cybersecurity 10428)

○ 이에 따라 미국 예산관리국(OMB)은 행정부 각 기관이 2024년까지 제로 트러스트를 채택하기 위해 어떻게 움직여야 하는지에 대한 개요가 포함된 **'제로 트러스트 사이버 보안 원칙을 향한 미국 정부의 움직임(Moving the U.S. Government Towards Zero Trust Cybersecurity**

Principles)'을 포함한 이 전략과 관련된 여러 문서 초안을 발표하였으며, 연방정부 구상안 내용의 일부는 다음과 같음.

- 연방 직원은 엔터프라이즈 관리 계정을 보유하고 있으므로 업무를 수행하는데 필요한 모든 것에 액세스하면서 표적이 되고 정교한 피싱 공격으로부터 안정적으로 보호받을 수 있다.
- 연방 직원이 업무를 수행하는 데 사용하는 장치는 지속적으로 추적 및 모니터링되며 내부 리소스에 대한 액세스 권한을 부여할 때 이러한 장치의 보안 상태가 고려된다.
- 엔터프라이즈 응용 프로그램은 내부 및 외부에서 테스트되며 인터넷을 통해 직원이 안전하게 사용할 수 있다.
- 연방 보안 팀과 데이터 팀은 데이터 범주 및 보안 규칙을 개발하여 중요한 정보에 대한 무단 액세스를 자동으로 감지하고 궁극적으로 차단한다.

○ 美 인프라 보안국(CISA)은 예산관리국(OMB)의 지침에 맞춰 **'제로 트러스트 성숙도 모델(Zero Trust Maturity Model, ZTMM)'**을 공개함으로써 각 기관의 제로 트러스트 구축을 통한 개선 방안 상세 모델을 일부 제시함

- 성숙도 모델은 OMB의 Federal Zero Trust Strategy를 보완하며 기관에 최적의 제로 트러스트 환경을 달성하기위한 로드맵과 리소스를 제공하도록 설계됨.
- 신원(Identity), 디바이스(Devices), 네트워크(Network), 응용프로그램 작업(Application Workload)로 분류하여 작성됨.

〈그림 3〉 CISA 제로 트러스트 성숙도 모델(Zero Trust Maturity Model, ZTMM)

자료: https://www.cisa.gov/zero-trust-maturity-model

○ 이와같이 제로 트러스트 보안의 필요성이 대두되면서 우리 정부도 NIST 표준을 참고로 제로 트러스트 도입 시 국내 공공 및 민간부문의 수용 가능성 현황, 개선이 필요한 과제 등을 점검할 것으로 예상됨.

- 최근 과학기술정보통신부에서는 "팬데믹에 따른 초연결 사회가 급속하게 도래하면서, 사이버 보안의 글로벌 트렌드 역시 '초안전 환경' 구축을 위한 제로 트러스트로 급속하게 전환되고 있다"며 "국가 차원의 '제로 트러스트' 정책 도입을 목표로 본격적인 사전 연구에 착수했다"고 밝힘.
- 아울러 윤석열 정부의 '디지털 플랫폼 정부' 공약이 AI(인공지능), 빅데이터 기반의 국정운영 시스템으로 행정 효율화를 꾀하는 모델인 만큼, 이를 뒷받침 할 보안 전략으로 제로 트러스트의 효용성을 타진할 것으로 보여짐. 정부 관계자는 "올 하반기쯤 연구의 성과물을 내놓고, 이를 바탕으로 정책 개발에 나서게 될 것"이라고 언급함.

[단독] "문제는 사람, 아무도 믿지 마!"...국가 사이버보안 전략 '대전환'

머니투데이 원문 | 기사전송 2022-03-26 08:02 최종수정 2022-03-27 13:19

댓글 0 0 공유 가 가

[머니투데이 변휘 기자] [편집자주] 러시아의 우크라이나 침공이후 사이버 전쟁도 확전 양상이다. 일상을 마비시키는 사이버전은 재래식 전쟁에 못지않은 파급력을 보인다. 분단국이자 IT강국인 한국 역시 예외가 아니다. 디지털서비스 의존도가 높아진 만큼 정부 공공기관과 대기업, 개인 대상 탈취도 일상화됐다. 사이버 전쟁과 진화하는 해킹의 유형, 우리의 대응수준과 새 정부의 보안정책 방향을 짚어본다.

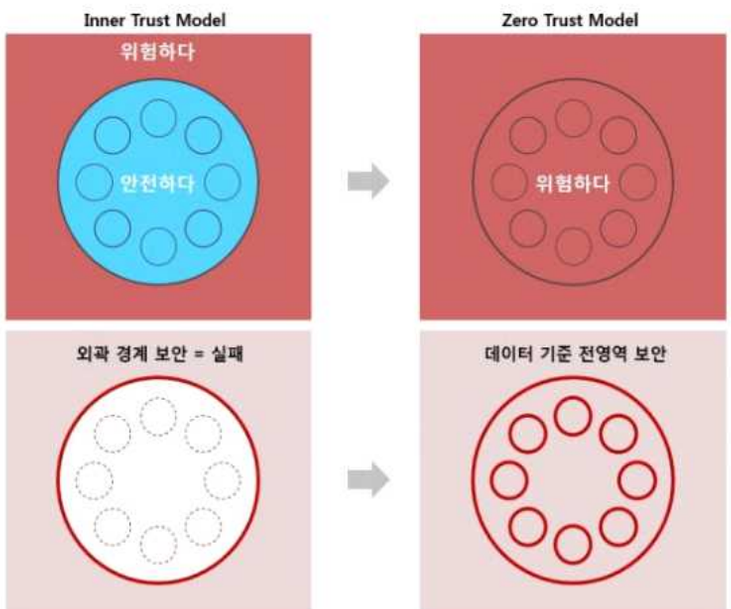
〈그림 4〉 제로 트러스트 관련 기사

자료: https://news.nate.com/view/20220326n03012?mid=n0600

Ⅱ. 제로 트러스트 기술 및 구축사례

1. 제로 트러스트 기술

○ 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 함.



〈그림 5〉 제로 트러스트 기본 모형

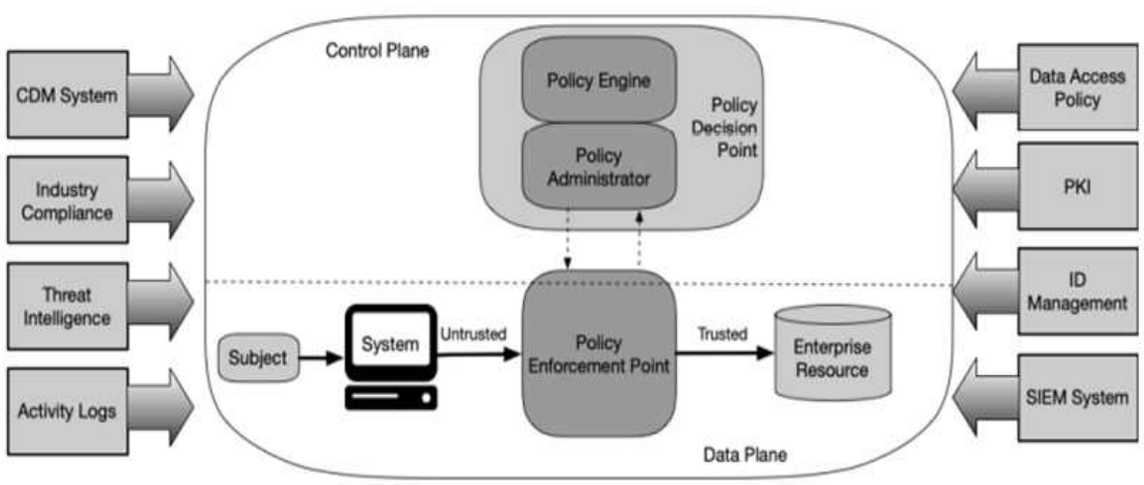
자료: https://www.pentasecurity.co.kr/column/제로-트러스트의-구체적-방법/

○ **'비경계 기반의 보안 모델(Un-perimeter based Security Model)'**인 제로 트러스트는 해당 모델이라 정의되기 위해 충족하여야 하는 조건을 보유하고 있음. 다수의 기관에서 입을 모아 이야기하고 있는 조건은 '식별하고, 검증하고, 확인하는 단계를 통해 최소한의 접근만을 허가' 한다는 내용을 공통된 골자로 삼고 있으며, 조건은 다음과 같음.

- Identify business-based data (비즈니스 기반 데이터 식별)
- Internal design of assets and data to be protected (보호할 자산 및 데이터의 내부 설계)
- Permission setting based on minimum access rights (최소 접근 권한에 따른 권한 설정)
- Inspection and logging of all traffic (모든 트래픽의 검사 및 로깅)

○ NIST는 **제로 트러스트 논리 구성 요소**를 다음 〈그림 6〉과 같이 정의하였으며, 각각 정책 엔진, 정책 관리자, 정책 시행시점으로 분류함.

- 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 결정함.
- 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 명령함.
- 정책 시행시점(Policy Enforcement Point)은 전체 통신경로의 게이트웨이 역할을 수행하며, 사람, 시스템, 어플리케이션과 대상 엔터프라이즈 리소스 간에 세션 활성화, 모니터링 시작 및 종료하는 역할을 담당함.



〈그림 6〉 NIST Zero Trust Logical Components

자료: https://cpl.thalesgroup.com/blog/encryption/key-components-function-in-zero-trust-architecture

○ NIST 제로 트러스트 논리 구성요소의 Eight Data Source Drive Zero Trust Access Decisions는 다음과 같음.

- CDM System(지속적인 진단 및 완화 시스템)은 엔터프라이즈 아키텍처의 시스템 무결성을 모니터링, 보고, 수정하는 시스템임.
- Threat Intelligence(위협 인텔리전스 피드)는 정책엔진의 엑세스 결정을 돕기 위해 새로

발견된 공격 또는 취약성 정보와 같은 내·외부 정보를 제공함.

- Data Access Policy(데이터 액세스 정책)은 허용되는 제어 동작을 이해하고 제어 기능을 제공함.
- PKI(공개 키 인프라)는 리소스, 주체, 서비스 및 App에 대한 기관에서 발급한 인증서를 생성하고 기록함.
- Activity Logs (네트워크 및 시스템 활동 로그), SIEM System (SIEM(보안 정보 및 이벤트 관리)시스템), Industry Compliance (산업 규정 준수 시스템)과 같은 시스템, 네트워크 엑세스 및 활동 로그는 이벤트와 활동을 일괄적으로 감사 및 추적하여 엑세스 기록에 대한 분석 또는 보고를 제공하는 역할을 담당함.

○ 위와 같은, 제로 트러스트 아키텍처를 통한 제로 트러스트를 기술적, 관리적으로 구현하고 운영하기 위한 기본 원리는 다음과 같이 정의할 수 있음.

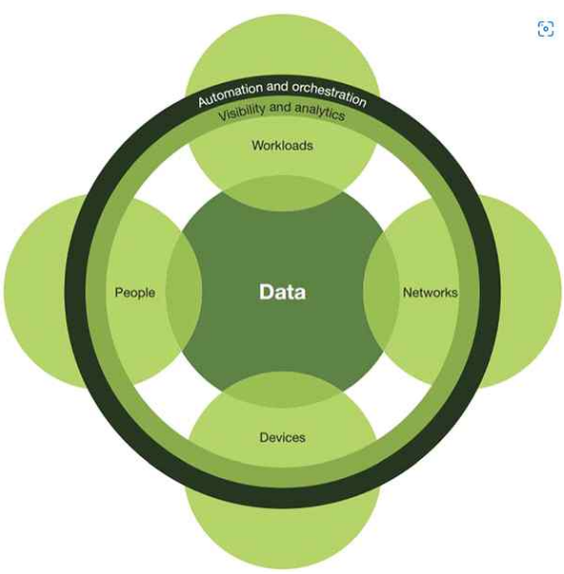
- All data sources and computing services are considered resources. (모든 데이터소스와 컴퓨팅 서비스는 리소스(보호대상)로 간주한다.)
- All communication is secured regardless of network location. (네트워크 위치(내/외부)와 관계없이 모든 통신을 안전(동일)하게 만든다.)
- Access to individual enterprise resources is granted on a per-session basis. (개별 엔터프라이즈 리소스에 대한 액세스는 세션 각각으로 승인(검증)된다.)
- Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. (리소스에 대한 액세스는 클라이언트 ID와 애플리케이션, 서비스, 요청 자산의 관측 가능한 상태 등 동적 정책에 의해 결정된다. 또 다른 동작, 환경적 속성이 포함 될 수도 있다.)
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets. (기업은 모든 소유 및 관련 자산의 무결성과 보안 상태를 모니터링하고 측정한다.)
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed. (모든 리소스 인증 및 권한 승인은 가변적(동적)이며 액세스를 허용하기 전에 엄격히 적용한다.)
- The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. (기업은 자산, 네트워크, 인프라, 통신의 현재 상태에 대한 정보를 가능한

많이 수집하고, 이를 활용해 보안 상태를 개선한다.)

○ NIST800-207설계의 기반은 **구글의 비욘드코프(BeyondCorp)**를 통하여 구현 가능성을 보여준 것을 기초한 것으로 추측됨.

- 비욘드코프는 2014년부터 구글의 네트워크 구축 경험을 바탕으로 전통적인 VPN을 사용하지 않고 접근제어 기능을 네트워크 기반이 아닌 사용자 개인 기기 기반으로 수행할 수 있는 제로 트러스트 환경을 가리킴.
- 사용자의 네트워크 위치와 상관없이 기기 인증, 사용자 인증, 접근 제어 총 3단계를 거치며, 보안 정책만으로도 네트워크 제어가 가능하게 되는 구조를 말함.

○ 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 모델을 구현해냄.



〈그림 8〉 Forrester의 Zero Trust eXtended 시스템 구성요소

자료: https://www.igloo.co.kr/security-information/

○ 또한, 일부 연구소, 사이버보안 전문기업은 제로 트러스트의 정의를 완전히 준수하려면 상당한 시간이 걸리고 기존 인프라를 완전히 교체해야 할 수 있으므로 오늘날 우리가 직면한 원격/분산 환경을 위해 'ZTNA(Zero Trust Network Access)'로 전환이 필요하다고 주장함.

- ZTNA(제로 트러스트 네트워크 액세스)는 인증된 사용자, 장치 및 응용 프로그램의 트래픽에만 조직 내의 다른 사용자, 장치 및 응용 프로그램에 대한 액세스 권한이 부여되는 보안 아키텍처임.

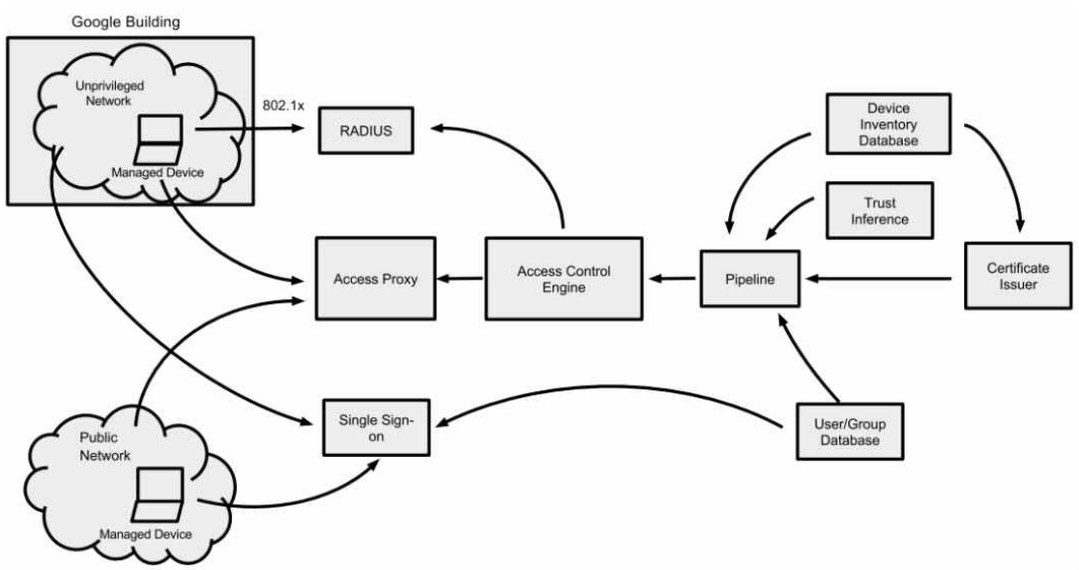
〈그림 9〉 가트너의 ZTNA 베스트 프랙티스

자료: 가트너

2. 제로 트러스트 구축사례

○ 구글의 비욘드코프(Beyond Corp) 모델은 방화벽이나 VPN과 같은 전형적인 보안 장비 없이 기기, 사용자 인증을 비롯한 다양한 요소를 분석한 결과만으로 접근 제어를 수행하며, 기능을 크게 세가지로 분류할 수 있음.

- 구글의 임직원용 시스템 서비스는 인증된 기기에서만 접속이 가능함. 사용자 기기에 관련된 다양한 정보를 수집하고 분석하여, 안전한 기기에서만 접근을 허용하도록 검증하고, 다음으로는 사용자를 인증하며 기기 인증과 마찬가지로 사내 시스템은 인가된 사용자에게만 접속이 허용됨.
- 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 DB에 반영되어 시스템 접속 허용 여부를 결정함.
- 접근제어 엔진이 위에서 언급한 다양한 요소를 분석/판단하여 접속을 허용하거나 차단하는 역할을 수행함.



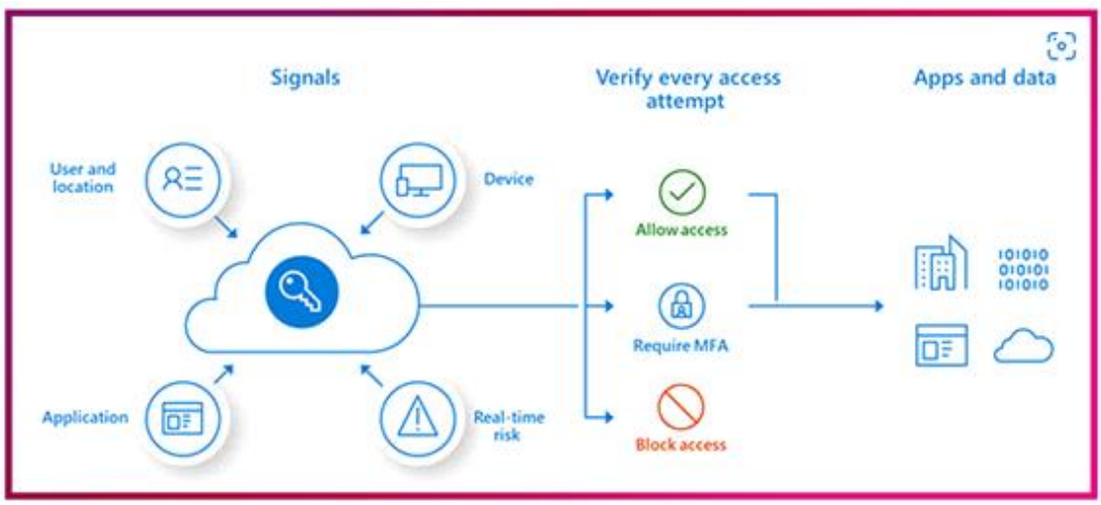
〈그림 10〉 구글 비욘드코프(BeyondCorp) 구성요소

자료: https://www.igloo.co.kr/security-information/

○ MS의 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 구조임.

- 모든 액세스 요청은 보안을 위반하며, 내/외부 접근 구분 없이 개방형 네트워크에서 발생했다고 가정함.

- 요청의 시작 위치나 액세스하는 리소스와는 무관하게 무조건 신뢰하지 않고 항상 확인함.
- 모든 액세스 요청은 액세스 권한을 부여하기 전에 완전히 인증, 승인 및 암호화가 되며 측면 이동을 최소화하기 위해 마이크로 세분화 및 최소 권한 액세스 원칙이 적용됨.
- 풍부한 인텔리전스와 분석을 활용해 이상 현실을 실시간으로 감지하고 대응함.

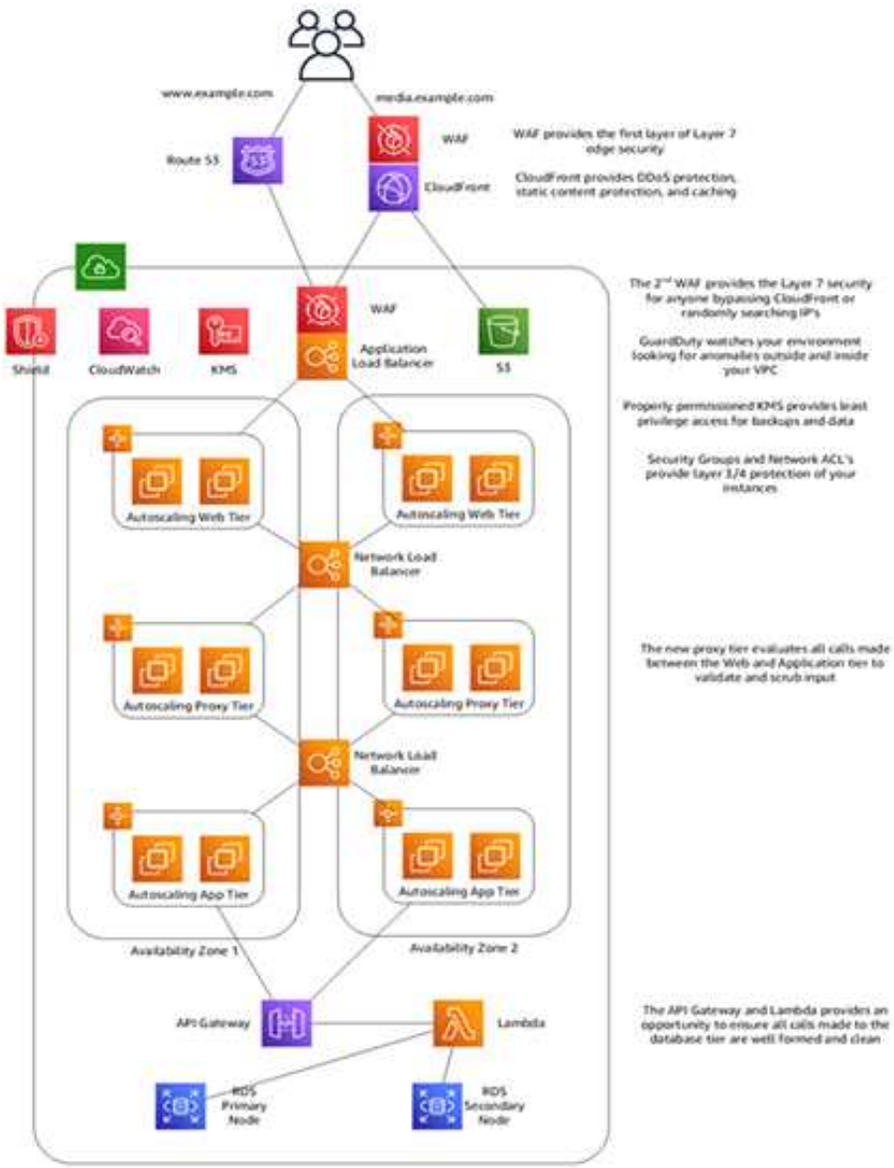


〈그림 11〉 MS의 Azure Active Directory

자료: 마이크로소프트

○ AWS에서는 클라우드 환경에서의 제로 트러스트 보안이 적용된 아키텍처를 설계하였으며, 주요 기능은 다음과 같음.

- 각 모델에서 일관된 트래픽 흐름을 제공하도록 구현 필요함.
- Amazon CloudWatch Anomaly Detection을 구현하여 머신 러닝(ML) 알고리즘을 사용해 비정상적으로 많은 네트워크 트래픽을 생성하는 특정 리소스에 대한 탐지를 수행함.
- Amazon SNS(Simple Notification Service)를 사용해 대상 항목에 자동으로 위협을 알림.
- 위협이 발생한 리소스를 제거하고 동작을 중지한 다음, 그룹으로부터 분리하여 추가 분석을 수행할 수 있는 Amazon Lambda 기능을 구현함.
- AWS KMS(Key Management Service)를 활용하여 정보 노출, 변조 및 거부를 방지하기 위해 암호화 및 최소한의 권한을 부여하여 제어함.



〈그림 12〉 AWS에서 제로 트러스트 웹 호스팅 아키텍처의 예

자료: Amazon

Ⅲ. 제로 트러스트 적용방안

○ 제로 트러스트는 기존에 사이버보안에서 보호하는 중점인 '데이터'에서 사용자, 디지털기기, 네트워크, 워크로드까지 개념을 확장하여 보호하고 또한 전 영역에 걸친 가시성 확보 기능을 추가하고, 보안 위협 분석과 통합 기능까지 포함하는 전사적인 개념으로 인식됨.

○ 이에 따라, 각 기관 및 기업에서는 제로 트러스트 기반의 구성의 범위와 대상을 지정하고 단계적으로 시행하는 전략을 수립하는데 많은 부담과 어려움이 따름.

- 대부분의 보안전문기업 Aruba, Cisco, MS, Okta, Akamai, Ctrix 등 각 기업의 대표 주력 분야를 확장하여 전사적인 제로 트러스트로 응용하여 제안하고 있음.
- SDN, NAC, EDR, SIEM 등 기존 출시된 기술을 기반으로 통제 및 검증 기능을 확대하는 것으로 제로트러스트 기술을 제시하는 것이 대부분이므로 기술 차별성, 투자 대비 효과성 등에 대해 담보하기 어려움.

○ 美 NSTAC(국가안보통신자문위원회)는 Zero Trust Implementation Plan을 발표하여 구현계획을 발표하였으며, 특히 제로 트러스트를 구현하기 위해 아주 느린속도로 실행하라고 제시함.

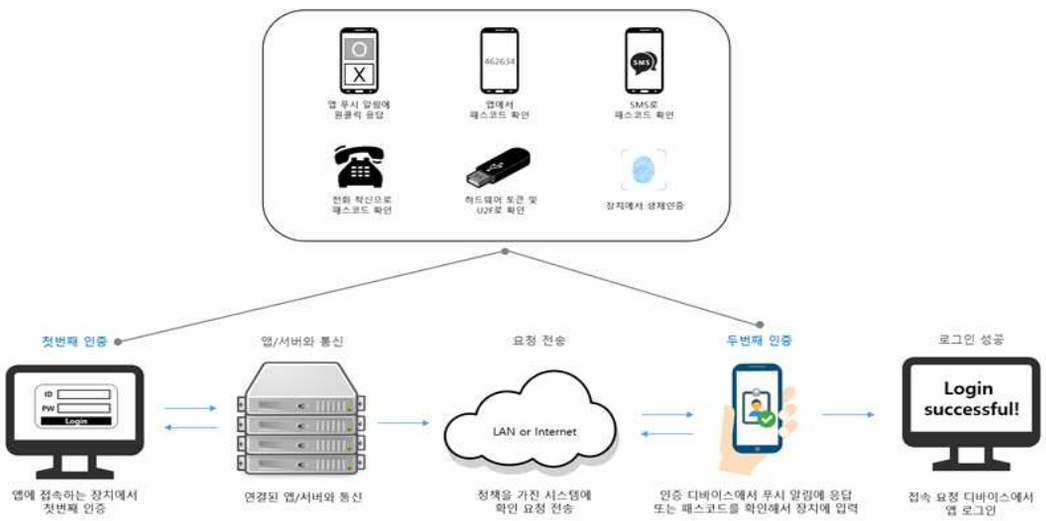
- 제로 트러스트는 장기적, 변화 혁신적인 노력이다.
- 제로 트러스트 지침을 활용하라.
- 제로 트러스트 프로그램을 구현할 사무소(부서)를 구성하라.
- 클라우드서비스 사용 도입을 가속화하라.
- 성공을 위해서는 효과적인 신원관리가 필요하다.

○ 이러한 이유는 제로 트러스트 기반 기술은 단순한 솔루션, 제품의 도입으로 단기간 구현할 수 있는 기술이 아니라, 전사적인 구현계획 수립과 전사적인 정보공유를 통해 전략과 규정의 준수 요건을 지속적으로 맞춰가는 장기적인 노력임을 강조함.

○ 따라서, 제로 트러스트 핵심 원리 7가지는 다단계인증, 장치엑세스 제어, 최소권한 정책의 3가지 기능의 강화로 미세분할에 해당되는 워크로드인 승인 세그먼트 엑세스에 대한 구체성을 확보할 수 있으며, 미세분할에 따른 지속적인 모니터링 및 검증은 대부분의 기업과 기관이 구성되어 있는

로그의 수집과 모니터링의 확대로 구체성을 확보할 수 있음.

- 다단계 인증(MFA)를 통해 정보시스템 접속의 인증을 강화하는 것이 중요하나, 단순히 기술적인 인증이 아닌 **정보시스템의 중요도를 구분하여 침해사고가 발생할 시 파장이 높은 서버 위주로 인증 강화 필요**
- 중요도가 낮거나 보통인 시스템은 싱글사인온(SSO)의 기능을 확장하여 사용성, 가용성이 저하되지 않은 상태로 보안이 강화되도록 함.



〈그림 13〉 다단계 인증 예시

- 정보시스템에 접속할 디지털기기 엑세스 제어를 위해 기기의 관리 상태(소유자, 백신, 패치 업데이터, 공유폴더, 접속 히스토리 유무 등)을 다각도로 점검하여 접근 성공 여부를 구분할 수 있도록 방안을 수립
- 기존에 활용하던 EDR, EPP, 내PC지킴이 등을 응용하여 최소필요 보안수준을 제시하여 그것을 연계한 디지털기기 접속 방안 연구 필요
- 전사적, 에플리케이션별, 그룹별 접속 정책 등은 정보시스템에 접근 여부를 결정할 최소 권한 엑세스로 세분화할 필요가 있으며, 장기적인 계획을 세워서 실행하는 것이 필요함.

○ 따라서, 제로 트러스트 기술 적용은 기존 정보시스템의 중요도 식별 기반의 MFA인증 강화, 접속 기기 보안강화 수립, 접근권한 수립, 모니터링 확대가 주안점이며, 이는 솔루션을 구축하거나, 확대하여 구성되는 것이 아닌 기존 기술을 활용하여 장기적인 계획의 수립과 실행으로 해결 가능한 전략이므로, 단순히 관련 제품의 추가 도입 등은 업무가 가중되고 가용성이 오히려 저하되며 특정 벤더의 종속적인 현상이 발생하여 제로 트러스트 기술의 적용 실패를 불러올 수 있음.

Ⅳ. 결론

○ 현재 제로 트러스트 보안 기술로 전환한다는 계획 등은 다수 확인할 수 있으나, 제로 트러스트 관련된 구체화된 모델을 찾기 어려우며, 실제로 적용하여 사용되는 사례도 찾아 볼 수 없음.

○ 제로 트러스트용 보안 솔루션이 다수 출시되고 있지만, 기존 기술을 확대하여 적용 범위를 확대할 수 있도록 응용하고 통합한 것이 대부분이므로 단순한 장비의 도입으로 해결하기 어려움.

○ 제로 트러스트의 기술 적용의 핵심요소인 다단계 인증, 장치엑세스 제어, 최소권한 정책을 수행할 수 있는 부서와 인력을 확대하여 장기적인 관점으로 단계별 제로 트러스트 기반 보안 전략 수립이 필요.

○ 특히, 최근에 문화체육관광 분야에 다양한 디지털기기가 활용됨에 따라 제로 트러스트 기술 적용의 핵심요소를 반영한 보안 기술 강화 필요.

- 키오스크, 가상현실기기 등 무인자동화기기는 관공서, 대중교통, 병원 등 생활 필수 시설에 다양하게 설치되어있으며, 특히 문화체육관광시설인 미술관, 박물관, 도서관, 영화관, 스포츠 경기장 등에 중요하게 설치되어 운영 중
- 그러나, 키오스크, 가상현실기기 등의 관리 권한 등이 탈취되는 것에 대비하여 보안을 강화할 필요성이 있음에도, 해당 기기들은 임베디드 운영체제 기술 등이 적용되어 장치제어엑세스가 적용되기에 일부 어려움 존재함.

○ 다단계인증(MFA) 기술을 활용한 무인자동화 디지털기기 보호 적합함.

- 무인자동화 디지털기기 도입시 필수적으로 다단계인증(MFA) 기능을 자체적으로 혹은 응용적으로 적용하여 보안 강화 추진 필요.

- 문화체육관광분야의 기관은 정보시스템 중요도 산정시에 시민을 안내하거나 활용하기 위해 접속하는 등의 다양한 문화행사에 활용되는 디지털 기기 보호의 중요도를 검토하여 다단계인증이 적용되도록 방안의 수립과 실행 필요.