NIST Special Publication 800-207

제로 트러스트 아키텍처

Zero Trust Architecture

2021.07.19.

권 리

• 저자
  - Scott Rose, NIST
  - Oliver Borchert, NIST
  - Stu Mitchell, Stu2Labs
  - Sean Connelly, Department of Homeland Security

• 번역 : Youngeun Moon, Blackfalcon Security

개 요

제로 트러스트zero trust는 고정된 네트워크 경계를 방어하는 것에서 사용자/자산/자원 중심의 방어로 변경하는 발전적인 사이버 보안 패러다임 개념이다. 제로 트러스트 아키텍처는 기업의 인프라스트럭처intrastructure 및 워크플로우workflow를 설계할 때 제로 트러스트 원칙을 사용한 것이다. 제로 트러스트는 물리적 위치, 네트워크 위치(예:LAN/인터넷), 자산 소유권(예:기업 소유/개인 소유)만을 기준으로 자산 또는 사용자 계정에 부여된 암묵적인 트러스트는 없다고 가정한다. 인증과 인가는 별개의 기능이며, 인증/인가를 수행한 이후 기업 자원에 대한 세션을 생성한다. 기업 네트워크 트렌드는 원격 접속, BYOD, 클라우드 등이 포함된다. 이들은 기업 네트워크 외부에 위치한다. 제로 트러스트는 이러한 트렌드에 대한 대응이다. 제로 트러스트는 네트워크를 나누는 것이 아니라, 자원(자산, 서비스, 워크플로우, 네트워크 계정 등)을 보호하는 것에 초점을 맞춘다. 네트워크의 위치는 더 이상 자원의 보안 상태를 결정하는 주요 요소로 볼 수 없다. 이 문서는 제로 트러스트 아키텍처에 대한 개념 정의를 포함하고 있다. 또한, 일반적인 배치 모델과 제로 트러스트를 이용하여 기업의 전반적인 정보 보안 상태를 개선할 수 있는 사례를 제공한다.

독 자

이 문서의 목적은 기업 보안 아키텍처를 위해 제로 트러스트를 설명하는 것이다. 이는 민간 일반 시스템에서 제로 트러스트의 이해를 돕고, 기업 환경에 제로 트러스트 보안 개념을 도입하고 배치하는 로드맵의 제공하다는 것을 의미한다. 보안 담당자, 네트워크 관리자는 이 문서를 통해 제로 트러스트 및 제로 트러스트 아키텍처에 대한 인사이트를 얻을 수 있다. 이 문서에서 제시하는 제로 트러스트 아키텍처에 대한 배치 계획을 모든 기업에 적용할 수 없다. 기업마다 보안 대책을 강구해야 할 비즈니스 영역과 데이터가 다르기 때문이다. 조직의 비즈니스와 데이터를 철저히 이해하는 것이 제로 트러스트에 대한 강력한 접근법이 될 것이다.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

목 차

부록 목차

그림 목차

1. 서 론

기업의 인프라스트럭처는 점점 더 복잡해지고 있다. 기업은 여러 개의 내부 네트워크, 자체 로컬 인프라스트럭처를 갖춘 원격 사무실, 원격 접속, 모바일, 클라우드 서비스를 운영한다. 이러한 복잡성을 경계 기반 네트워크 보안이라는 기존 방법으로 통제할 수 없다. 기업의 경계가 분산되어 있고, 식별도 쉽지 않기 때문이다. 또한, 경계 기반 네트워크 보안으로는 충분하지 않다. 경계 기반 네트워크 보안은 공격자가 경계를 침해한 후 경계 내부에서 이동하는 것에 대응하지 못한다.

이렇게 복잡한 기업은 제로 트러스트라는 새로운 사이버 보안 모델의 개발을 선도했다. 제로 트러스트는 초기에 데이터 및 서비스 보호에 집중했다. 그러나, 제로 트러스트는 기업의 모든 자산(기기, 애플리케이션, 인프라스트럭처/가상화/클라우드 컴포넌트)과 주체(최종 사용자, 애플리케이션, 리소스에 정보를 요청하는 인간이 아닌 객체)를 포함하도록 확장할 수 있고, 확장해야 한다. 이 문서에서 “사용자”는 사람인 경우에만 사용했으며, 그 외에는 “주체”라고 사용했다. 제로 트러스트 보안 모델은 기업 환경에 공격자가 존재하며, 기업 환경은 신뢰성이 전혀 보장되지 않는 환경과 차이가 없다고 가정한다. 이 새로운 패러다임에서 기업은 암묵적인 트러스트는 없다고 상정해야 하며, 자산 및 비즈니스에 대한 위험을 지속적으로 분석/평가해야 하고, 위험을 완화하기 위한 보안 대책을 마련해야 한다. 제로 트러스트는 액세스 최소화(액세스가 필요한 주체/자산에게만 리소스에 대한 액세스를 허용) 및 지속적 인증/인가(모든 액세스 요청의 아이덴티티 및 보안 상태에 대한)라는 보안 대책이 기본적으로 포함된다.

제로 트러스트 아키텍처는 제로 트러스트 원칙을 기반으로 데이터 유출 사고를 방지하고, 내부 이동을 제한하도록 설계된 기업 사이버 보안 아키텍처이다. 이 문서에서는 제로 트러스트 아키텍처, 논리 컴포넌트, 배치 시나리오, 위협을 다룬다. 또한, 제로 트러스트를 도입하고자 하는 조직을 위한 일반적인 로드맵을 제공하며, 제로 트러스트 아키텍처에 영향을 줄 수 있는 법령에 대해 언급한다.

제로 트러스트는 하나의 아키텍처가 아니다. 제로 트러스트는 보안 상태(비밀등급 및 민감도) 개선에 사용할 수 있는 워크플로우, 시스템 설계, 운영에 대한 가이드라인의 모음이다. 제로 트러스트 아키텍처로의 전환은 조직의 미션을 달성하는데 발생하는 위험을 어떻게 평가할 것인지와 관련된 여정이며, 대규모 기술 교체만으로는 달성할 수 없다. 바꿔 말하면, 오늘날 다수의 조직은 자신들의 인프라스럭처에 제로 트러스트 아키텍처의 요소들을 이미 가지고 있다는 의미이다. 조직은 제로 트러스트 원칙, 프로세스 변경, 기술 솔루션을 점진적으로 구현하기 위해 애써야 한다. 대부분의 기업은 제로 트러스트로 전환(IT 최신화, 비즈니스 프로세스 개선)하는 동안, 제로 트러스트와 경계 기반 모드를 하이브리드로 운영할 것이다.

조직에서 제로 트러스트가 효과적이려면, 종합적인 정보 보안 및 복구 계획을 실행할 필요가 있다. 기존의 사이버 보안 정책/가이드, 식별/접근 관리, 지속적인 모니터링, 모범 사례가 균형을 이룰 때, 제로 트러스트 아키텍처는 위험 관리를 통해 위협을 방어하고, 조직의 보안 상태를 개선할 수 있다.

1.1. 제로 트러스트에 대한 美연방 기관의 기여

제로 트러스트라는 개념은 “제로 트러스트”라는 용어가 만들어지기 이전부터 사이버 보안에 존재했다. 국방정보체계국DISA[1] 및 국방부는 “블랙코어BCORE”라는 더 안전한 기업 전략에 관련된 연구 결과를 발표했다. 블랙코어에는 경계 기반 보안 모델에서 개별 트랜잭션 보안에 중점을 둔 모델로 전환하는 것이 포함되었다. 2004년 예리코Jerico 포럼에서는 네트워크 위치에 따른 암묵적인 트러스트를 제한해야 한다는 탈脫경계화deperimeterization의 개념과, 네트워크를 크게 분리한 후 단일 지점에서 정적으로 방어하는 것에 한계가 있음을 발표하였다. 탈경계화는 제로 트러스트라는 더 넓은 개념으로 진화하게 되었다. 제로 트러스트는 네트워크 위치 기반의 암묵적인 트러스트에서 벗어나, 트랜잭션 단위로 트러스트를 평가하는데 초점을 맞춘 다양한 사이버 보안 솔루션을 설명하는 용어가 되었다. 또한, 민간 및 교육 영역에서도 이러한 진화(경계 기반 보안 → 제로 트러스트 원칙 기반 보안 전략)가 진행되었다.

연방 기관들은 10년 이상 제로 트러스트 원칙에 기반한 보안으로의 전환을 권고 받았다. 이와 동시에 연방 정보 보안 현대화에 관한 법률FISMA[2]에 의거하여 위험 관리 프레임워크RMF[3], 연방 아이덴티티/크리덴셜/액세스 관리FICAM[4], 신뢰 인터넷 커넥션TIC[5], 상시 진단/완화CDM[6] 프로그램과 같은 역량 및 정책을 구축하였다. 이런 프로그램들은 인가자에 대한 데이터 및 리소스 액세스를 제한하는 것을 목표로 한다. 이런 프로그램들을 시작했을 때는, 정보시스템의 기술적 한계로 인해 제약이 존재했다. 보안 정책은 대부분 정적이며, 기업은 효과를 최대화할 수 있는 넓은 초크choke 포인트에서 보안 정책을 집행한다. 기술이 성숙함에 따라 액세스 요청을 지속적으로 분석하고, 액세스 필요성의 원칙에 따라 동적/세밀한 방법으로 평가하는 것이 가능하게 되었다. 이로 인해 침해된 계정, 네트워크 감시 등의 위협으로 데이터가 유출되는 것을 완화할 수 있다.

1 DISA : Defense Information System Agency
2 FISMA : Federal Information Security Modernization Act
3 RMF : Risk Management Framework
4 FICAM : Federal Identity, Credential, and Access Management
5 TIC : Trusted Internet Connections
6 CDM : Continuous Diagnostics and Mitigation

1.2. 문서 구조

문서는 다음과 같은 구성된다.

- 섹션 2 : 제로 트러스트 및 제로 트러스트 아키텍처를 정의한다. 또한, 기업이 제로 트러스트 아키텍처를 설계할 때 가정하는 사항을 나열한다.
- 섹션 3 : 제로 트러스트의 논리 컴포넌트(또는 빌딩 블록)에 대해 설명한다. 동일한 논리적 기능을 제공하면서도, 제로 트러스트 아키텍처 컴포넌트를 다르게 구성하도록 독특하게 구현할 수 있다.
- 섹션 4 : 기업 환경을 더 안전하게 할 수 있는 제로 트러스트 아키텍처의 유스케이스를 몇 가지 보인다. 이런 유스케이스에는 원격 근무, 클라우드 서비스, 게스트 네트워크를 보유한 기업이 포함된다.
- 섹션 5 : 제로 트러스트 아키텍처를 사용하는 기업이 처할 수 있는 위협에 대해 언급한다. 이런 위협의 다수는 다른 모든 구조화된 네트워크와 비슷하지만, 다른 완화 기술이 필요할 수 있다.
- 섹션 6 : 제로 트러스트 아키텍처 원리를 기존 지침에 적합하게 하거나 보완하는 방법에 대해 다룬다.
- 섹션 7 : 기업을 제로 트러스트 아키텍처로 전환하기 위한 출발선을 명시한다. 여기에는 제로 트러스트 원리가 적용된 애플리케이션 및 기업 인프라스트럭처를 계획/배치하는데 필요한 일반적인 단계에 대한 설명이 포함되어 있다.

2. 제로 트러스트의 기초

제로 트러스트는 트러스트를 암묵적으로 승인하지 않으며, 지속적으로 평가해야 한다는 것을 전제로 리소스 보호에 초점을 맞춘 사이버 보안 패러다임이다. 제로 트러스트 아키텍처는 기업의 리소스/데이터를 보호하기 위한 E2E[End-to-End] 접근법이다. 아이덴티티(사람, 사람이 아닌 개체), 크리덴셜, 접근 관리, 운영, 엔드포인트, 호스팅 환경, 내부 연결 인프라스트럭처를 포함한다. 초기에는 접근이 필요한 사람만으로 리소스를 제한하고, 업무 수행에 필요한 최소한의 권한(예 : 읽기, 쓰기, 삭제)만 부여하는 것에 집중해야 한다. 지금까지 정부 기관 및 일반 기업의 네트워크는 내·외부 경계의 보안에 집중했고, 인증된 주체에게는 내부 네트워크의 자원 대부분에 대한 접근 권한을 부여했다. 그 결과, 승인되지 않은 내부 이동은 정부 기관에게 가장 해결하기 어려운 문제가 되고 있다.

신뢰 인터넷 커넥션 및 경계 방화벽은 강력한 인터넷 게이트웨이를 이룬다. 이는 인터넷에서 침투하려는 공격자를 막는데 도움이 된다. 그러나, 신뢰 인터넷 커넥션 및 경계 방화벽은 네트워크 내부에서 발생하는 공격을 탐지하고 차단하는데는 큰 도움이 되지 않으며, 기업 네트워크의 외부에 위치한 주체(예: 원격 근무자, 클라우드 기반 서비스, 에지 디바이스 등)를 보호할 수 없다.

제로 트러스트와 제로 트러스트 아키텍처의 정의는 다음과 같다.

> 제로 트러스트란, 네트워크가 침해된 상황에서 정보 시스템 및 서비스가 각각의 요청에 대한 접근 권한을 정확하고 최소한으로 판단하려고 할 때 불확실성을 최소화하기 위한 개념과 발상의 모음이다. 제로 트러스트 아키텍처란, 제로 트러스트 개념을 사용한 기업 사이버 보안 계획이며, 컴포넌트간 관계, 워크플로우 설계, 액세스 정책이 포함된다. 따라서, 제로 트러스트 엔터프라이즈란, 제로 트러스트 아키텍처를 실행함으로써 기업에 존재하는 네트워크 인프라스트럭처(물리/가상) 및 정책을 말한다.

제로 트러스트를 기업의 핵심 전략으로 채택한다면, 기업은 제로 트러스트 원칙(섹션 2.1 참조)에 따라 작성한 계획, 즉 제로 트러스트 아키텍처를 만든다. 이 계획은 기업에 제로 트러스트 환경을 구축하기 위해 배포된다.

이 정의는 접근 통제를 가능한 한 세밀하게 하여, 데이터 및 서비스에 대한 비인가된 접근을 방지하는 것을 목적으로 한다. 즉, 인가된 주체(사용자, 애플리케이션/서비스, 디바이스의 조합)는 데이터에 액세스할 수 있으나, 다른 모든 주체(즉, 공격자)를 데이터에 액세스할 수 없다. 더 나아가, “데이터”를 “리소스”로 치환할 수 있다. 이 경우, 제로 트러스트 및 제로 트러스트 아키텍처는 단순히 데이터 액세스가 아니라 리소스 액세스(예: 프린터, 컴퓨터 리소스, IoT 액추에이터)에 대한 것이다.

불확실성을 줄이기 위해(불확실성은 제거될 수 없다), 인증/인가 및 암묵적 트러스트 구역 축소에 초점을 맞춘다. 이와 동시에 가용성을 유지하면서, 인증 메커니즘의 지연 시간을 최소화한다. 요청을 수행하는데 필요한 권한을 최소화하기 위해 액세스 규칙을 가능한 한 세밀하게 만든다.

그림 1은 액세스에 대한 개념적인 모델로 주체는 기업의 리소스에 접근할 필요가 있다. 액세스는 정책 결정 포인트PDP[1] 및 정책 집행 포인트PEP[2] 를 통해 허가된다.

그림 1 : 제로 트러스트 액세스

시스템은 주체가 확실하고 요청이 유효하다는 것을 반드시 보증해야 한다. 정책 결정 포인트 및 정책 집행 포인트는 적절한 판단을 내려, 주체가 리소스에 액세스하는 것을 허가한다. 이는 제로 트러스트가 인증 및 인가라는 두 가지 기본적인 영역에 적용된다는 것을 의미한다. 이렇게 독특한 요청을 보낸 주체의 신원을 어느 정도 신뢰할 수 있는가? 주체의 신원에 대한 현재 신뢰도로 자원에 대한 액세스를 허용할 수 있는가? 요청에 사용된 디바이스는 보안이 적절한 상태인가? 고려해야 하는 다른 요인이나, 신뢰도를 수정해야 하는 요인(예: 시간, 주체의 위치, 주체의 보안 상태)이 있는가? 기업은 리소스 액세스를 위해 동적 위험 기반 정책을 개발할 필요가 있다. 또한, 각 리소스 액세스 요청에 대해 이 정책이 올바르고 일관되게 시행되는 것을 보증하기 위한 시스템을 구축할 필요도 있다. 즉, 기업은 주체가 기본적인 인증 수준을 만족했기 때문에 이후 모든 리소스 요청이 타당하다고 가정(암묵적 신뢰)하면 안된다.

“암묵적 트러스트 구역”이란, 모든 개체가 적어도 마지막 PDP/PEP의 레벨 정도로 신뢰받는 구역이다. 공항의 탑승객 검열 모델을 예로 들 수 있다. 모든 탑승객은 공항 보안 검색대(PDP/PEP)를 통과하여 탑승구로 들어간다. 탑승 구역에 있는 탑승객, 공항 직원, 승무원 등은 신뢰가 부여된 것으로 본다. 여기서 암묵적 트러스트 구역은 탑승 구역이 된다.

PDP/PEP는 PEP를 통과하는 모든 트래픽이 동일한 트러스트 레벨을 갖도록 다수의 통제를 적용한다. PDP/PEP는 자신을 통과한 트래픽에 추가적인 정책을 적용할 수 없다. PDP/PEP를 세분화하려면, 암묵적 트러스트 구역을 작게 만들어야 한다.

제로 트러스트는 PDP/PEP를 리소스에 더 가깝게 위치시키기 위한 원칙 및 개념을 제공한다. 이는 기업을 구성하는 모든 주체/자산/워크플로우를 명확하게 인증하고 인가하는 것이다.

1 PDP : Policy Decision Point
2 PEP : Policy Enforcement Point

2.1. 제로 트러스트의 원리

제로 트러스트에 대한 다수의 정의/논의에서 광범위한 경계 방어(예: 방화벽)를 제거하는 개념을 강조하고 있다. 그러나, 모순적이게도 대부분의 정의/논의에서 제로 트러스트 아키텍처가 가져야 할 기능으로써 경계를 어떤 방법으로든(마이크로 세그멘테이션, 마이크로 페리미터 등, 섹션 3.1 참조) 정의하고 있다. 아래에서는 제로 트러스트 및 제로 트러스트 아키텍처를 정의함에 있어 "무엇을 제외해야 하는가?"보다 "포함해야 하는 기본 원리가 무엇인가?"라는 관점에서 정의하려고 한다. 이런 원리은 이상적인 목표일 뿐이다. 모든 원리를 변경 없이 완전하게 구현할 수 있지는 않다.

제로 트러스트 아키텍처는 다음의 제로 트러스트 기본 원리를 준수하여 설계하고 배포한다.

1. 모든 데이터 소스 및 서비스를 리소스로 간주한다. 네트워크는 여러 종류의 디바이스로 구성될 수 있다. 네트워크에는 데이터를 애그리게이터aggregator, 스토리지, SaaS software as a service 등으로 송신하는 소형 디바이스가 있을 수도 있다. 또한, 개인 소유의 디바이스가 기업이 소유하고 있는 리소스에 접근할 수 있다면, 개인 소유의 디바이스 또한 리소스로 분류할 수 있다.

2. 네트워크 위치에 관계없이 모든 통신을 보호해야 한다. 네트워크 위치가 신뢰를 시사하지 않는다. 기업 네트워크 인프라스트럭처 내부의 자산에서 발생한 액세스 요청과 그 외 모든 네트워크에서 발생한 접근 요청은 동일한 요구사항을 충족해야 한다. 즉, 디바이스가 기업 네트워크 인프라스럭처 내부에 있다고 해서 자동으로 신뢰를 부여해서는 안된다. 모든 통신은 가장 안전한 방법으로 수행되어야 하고, 기밀성과 무결성을 보호해야 하며, 소스를 인증해야 한다.

3. 기업 리소스에 대한 액세스를 세션 단위로 허가한다. 요청자에 대한 신뢰를 평가한 후 액세스를 허가한다. 또한, 작업을 완료하는데 필요한 최소한의 권한으로 접근을 허가해야 한다. 이는 특정 트랜잭션에 대해 신속하게 이루어져야 함을 의미하지만, 그 시점을 세션을 초기화하거나 리소스와 트랜잭션을 수행하기 이전으로 지정하지는 않는다. 다만, 한 리소스에 인증/인가되었다고 해서 다른 리소스에 자동으로 접근을 허용하는 것은 아니다.

4. 동적 정책으로 리소스에 대한 접근을 결정한다. 동적 정책에는 클라이언트의 아이덴티티, 애플리케이션/서비스, 요청을 보낸 자산을 관찰한 상태가 포함되며, 행동 속성 및 환경 속성도 포함될 수 있다. 조직은 "어떤 리소스를 가지고 있는지?", "조직의 사용자는 누구인지?", "리소스 액세스에 어떤 권한이 필요한지?"를 정의함으로써 리소스를 보호한다. 제로 트러스트에서 클라이언트의 아이덴티티란, 사용자 계정(또는 서비스 계정)과 자동화된 태스크를 인증하기 위해 기업이 계정/서비스에 할당한 모든 속성이 포함된다. 요청을 보낸 자산의 상태에는 설치된 소프트웨어 버전, 네트워크

위치, 요청 시일, 이전에 관찰된 행위, 설치된 크리덴셜과 같은 디바이스 특성이 포함될 수 있다. 행동 속성에는 주체 자동 분석, 디바이스 분석, 관찰된 사용 패턴 대비 편차가 포함되며, 다른 사항들도 포함될 수 있다. 정책이란, 조직이 주체/데이터 자산/애플리케이션에 할당하는 속성에 기반한 액세스 룰rule을 모아 놓은 것이다. 환경 속성에는 요청자의 네트워크 위치, 시간, 보고된 공격 등의 요인이 포함된다. 이런 룰/속성은 비즈니스 프로세스의 니즈, 수용 가능한 위험 레벨에 기반하여 작성된다. 리소스 액세스와 액션 퍼미션permission 정책은 리소스/데이터의 민감도에 근거하여 변경될 수 있다. 가시성과 접근성을 제한하기 위해, 최소 권한 원칙을 적용한다.

5. 기업은 모든 자산의 무결성/보안 상태를 감시하고 조치해야 한다. 기본적으로 자산을 신뢰하지 않는다. 기업은 리소스에 대한 요청을 평가할 때 자산의 보안 상태를 평가한다. 제로 트러스트 아키텍처를 실행하고 있는 기업은 CDM 또는 유사한 시스템을 구축하여 디바이스/애플리케이션의 상태를 감시해야 하고, 필요에 따라 패치/픽스를 적용해야 한다. 침해가 발견된 자산, 알려진 취약점을 가지고 있는 자산, 조직에서 관리하지 않는 자산은 가장 안전한 상태라고 여겨지는 디바이스와 다르게 처리(기업 리소스에 대한 모든 접속이 거부되는 것을 포함)할 수 있다. 또한, 일부 리소스에는 액세스가 허용되지만 다른 리소스에는 액세스가 허용되지 않는 디바이스(예: 개인 소유 디바이스)도 다르게 처리될 수 있다. 이 경우에도 기업 리소스의 현 상태에 대한 실용적인 데이터를 제공하기 위해 강력한 모니터링 및 리포팅 시스템이 필요하다.

6. 모든 리소스의 인증/인가를 동적으로 강력하게 실시한 후 접근을 허용한다. 이는 커뮤니케이션을 진행하면서, 접근 획득→위협 스캔/평가→조정→지속적인 신뢰 재평가라는 일정한 사이클이다. 제로 트러스트 아키텍처를 실행하고 있는 기업은 ICAMIdentity, Credential, and Access Management 및 자산 관리 시스템 도입이 권장된다. 여기에는 일부(또는 모든) 기업 리소스에 접근하기 위해 다중 인증을 사용하는 것도 포함된다. 보안, 가용성, 유용성, 가성비, 비용 효율성 사이의 균형을 고려하여 정책을 작성(예 : 시간 기반, 신규 리소스 요청, 리소스 변조, 주체의 비정상 행위 탐지)하고, 정책에서 정의한 대로 사용자 트랜잭션 전체를 모니터링하고 재인증/재인가한다.

7. 기업은 자산, 네트워크 인프라스트럭처, 커뮤니케이션의 현 상태에 대해 가능한 한 많은 정보를 수집한다. 그리고, 보안 상태를 개선하기 위해 수집한 정보를 사용한다. 기업은 자산의 보안 상태, 네트워크 트래픽, 액세스 요청과 관련한 데이터를 수집해야 한다. 그 데이터를 처리하여 획득한 지식을 정책을 개선하기 위해 사용해야 한다. 또한, 이 데이터는 주체가 액세스를 요청하게 된 맥락을 파악하기 위해 사용할 수 있다.(섹션 3.3.1 참조)

상기 원리는 기술에 구애받지 않는다. 예를 들어, “사용자 식별”은 ID/비밀번호, 인증서, OTP One Time Password와 같은 요소를 포함할 수 있다. 이 원리는 조직 내부의 작업이나, 다수 파트너와 협업해야 하는 작업에 적용할 수 있다. 그러나, 공공 또는 고객을 상대로 하는 비즈니스 프로세스에는 적용할 수 없다. 외부 인원(예: 고객, 일반적인 인터넷 사용자)에게 내부 정책 준수를 강요할 수 없기 때문이다. 그러나, 특별한 관계에 있는 외부 사용자(예: 등록된 고객, 임직원의 가족)에게는 제로 트러스트 기반 정책의 일부를 적용할 수 있다.

2.2. 네트워크에서 제로 트러스트의 관점

네트워크 계획/배치에 제로 트러스트 아키텍처를 이용하는 조직은 네트워크 연결에 대해 기본적으로 가정하는 것이 몇 가지 있다. 이 가정 가운데 일부는 기업 소유 네트워크 인프라스트럭처에 적용되며, 일부는 기업 외부의 네트워크 인프라스트럭처(예: 공개 와이파이, 공용 클라우드)에서 운영 중인 기업 소유 리소스에 적용된다. 이러한 가정은 제로 트러스트 아키텍처를 어디에 배치할 것인지 결정하기 위해 사용된다. 제로 트러스트 아키텍처를 실행하고 있는 기업은 위에서 언급한 제로 트러스트 아키텍처 원리, 아래 언급할 가정에 따라 네트워크를 구성해야 한다.

1. 기업의 프라이빗 네트워크 전체를 암묵적 트러스트 존으로 간주하지 않는다. 자산은 항상 기업 네트워크에 공격자가 존재하고 있음을 가정하여 행동해야 하며, 가장 안전한 방법으로 통신해야 한다.(원리 2 참조) 여기에는 모든 접속을 인증하고 모든 트래픽을 암호화하는 것이 포함된다.

2. 네트워크에 연결된 디바이스는 기업 소유가 아닐 수도, 기업이 설정할 수 없을 수도 있다. 방문자 및 외부 계약 서비스는 자신의 역할 수행을 위해 네트워크 접속이 필요할 수 있고, 네트워크에 접속되는 자산은 기업 소유가 아닐 수 있다. 여기에는 BYOD bring-your-own-device 정책이 포함된다. BYOD 정책은 기업 주체가 기업 리소스에 접근하기 위해 기업 소유가 아닌 디바이스를 사용할 수 있게 해준다.

3. 본질적으로 신뢰할 수 있는 리소스는 없다. 모든 자산은 PEP로 보안 상태를 평가해야 하며, 그 이후 기업 소유의 리소스에 대한 요청을 허가해야 한다.(자산과 주체에 대해서는 원리 6과 유사) 보안 상태 평가는 세션이 계속되는 한 지속적으로 이루어져야 한다. 기업 소유 디바이스는 인증할 수 있는 아티팩트를 가지고 있을 수 있고, 기업이 소유하지 않은 디바이스에서의 요청보다 더 높은 신뢰도를 가질 수 있다. 기업 리소스를 허가하기 위해 디바이스를 인증할 때, 주체의 크리덴셜만으로는 충분하지 않다.

4. 모든 기업 리소스가 기업 소유 인프라스트럭처에 위치하고 있는 것은 아니다. 리소스에는 클라우드 서비스뿐만 아니라, 기업의 원격 주체도 포함된다. 기업 소유 자산 또는 기업 관리 자산은 기업 소유가 아닌 로컬 네트워크 및 네트워크 서비스(예: DNS)를 사용해야 할 수 있다.

5. 기업의 원격 주체와 자산은 로컬 네트워크 연결을 완전히 신뢰할 수 없다. 원격 주체는 로컬 네트워크(즉, 기업이 소유하지 않은)가 적대적이라고 가정해야 한다. 자산은 모든 트래픽이 모니터링되고 있고, 변조될 수 있다고 가정해야 한다. 모든 연결 요청을 인증하고 인가해야 한다. 그리고, 모든 통신을 가장 안전한 방법(즉, 기밀성, 무결성 보호, 소스 인증)으로 수행해야 한다.(상기 제로 트러스트 아키텍처 원리 참조)

6. 기업-비기업 인프라스트럭처를 오고 가는 자산 및 워크플로우의 보안 정책 및 보안 상태는 일관적이어야 한다. 자산 및 워크로드는 기업 소유 인프라스트럭처를 오갈 때 보안 상태를 유지해야 한다. 여기에는 기업 네트워크에서 비기업 네트워크(즉, 원격 사용자)로 이동하는 디바이스를 포함한다. 또한, 온 프레미스on-premise 데이터 센터에서 비非기업 클라우드 인스턴스로 이전하는 워크로드workload도 포함된다.

3. 제로 트러스트 아키텍처의 논리 컴포넌트

기업에서 제로 트러스트 아키텍처를 실행하기 위해서는 많은 논리 컴포넌트가 필요하다. 이런 컴포넌트는 온 프레미스 서비스로 운영되거나 클라우드 기반 서비스를 통해 운영될 수 있다. 그림 2의 프레임워크 개념 모델은 컴포넌트 및 컴포넌트 사이의 상호작용을 보인다. 물론, 이 개념 모델은 이상적인 모델이다. 정책 결정 포인트(PDP, Policy Decision Point)는 두 개의 논리 컴포넌트, 정책 엔진(PE, Policy Engine)과 정책 관리자(PA, Policy Administrator)로 나눈다. 제로 트러스트 아키텍처의 논리 컴포넌트는 컨트롤 플레인에서 통신한다. 반면, 애플리케이션은 데이터 플레인에서 통신한다.

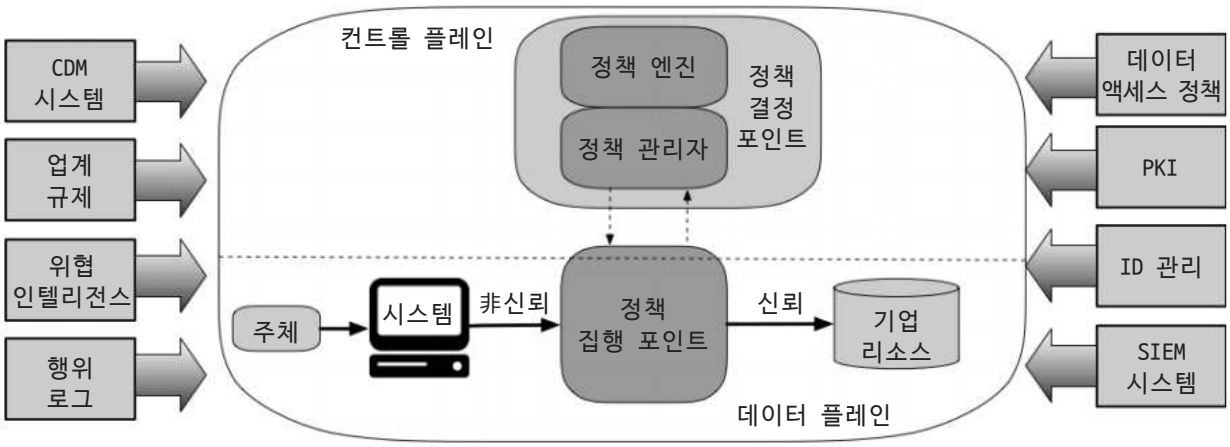

그림 2 : 제로 트러스트 핵심 논리 컴포넌트

- 정책 엔진(PE, Policy Engine) : 정책 엔진은 주체에게 리소스의 액세스를 허가할지 최종적으로 결정한다. 정책 엔진은 트러스트 알고리즘(섹션 3.3 참조)에 대한 입력으로 기업의 정책 및 외부 소스(예 : CDM 시스템, 위협 인텔리전스 서비스)를 사용하여, 리소스의 액세스를 허가/거부/취소한다. 정책 엔진은 정책 관리자와 짝을 이룬다. 정책 엔진은 결정(승인 또는 거부)하고 기록하며, 정책 관리자는 그 결정을 실행한다.

- 정책 관리자(PA, Policy Administrator) : 정책 관리자는 정책 집행 포인트에 명령하여 주체와 리소스 사이의 통신 경로를 설정하거나 폐쇄한다. 정책 관리자는 세션별別 인증/인가 토큰 또는 크리덴셜을 생성하며, 클라이언트는 이를 이용하여 기업 리소스에 액세스한다. 정책 관리자는 정책 엔진과 밀접하게 연관되고, 세션의 허가/거부에 대한 최종적인 결정은 정책 엔진에 의존한다. 세션이 인가되고 요청이 인증되면, 정책 관리자는 세션을 시작할 수 있도록 정책 집행 포인트를 설정한다. 세션이 거부되거나 이전 승인이 철회되면, 정책 관리자는 정책 집행 포인트에게 해당 연결을 끊으라는 신호를 준다. 정책 엔진과 정책 관리자를 하나의 서비스로 취급하여 구현한 경우도 있다. 이 경우, 이 서비스를 두 개의 논리 컴포넌트로 나눈다. 정책 관리자는 통신 경로를 생성할 때, 컨트롤 플레인을 통해서 정책 집행 포인트와 통신한다.

- 정책 집행 포인트(PEP, Policy Enforcement Point) : 정책 집행 포인트는 주체와 기업 리소스 사이를 연결하고, 모니터링하고, 최종적으로 연결을 종료한다. 정책 집행 포인트는 요청을 포워딩하거나, 정책 업데이트를 위해 정책 관리자와 통신한다. 제로 트러스트 아키텍처에서 정책 집행 포인트는 한 개의 논리 컴포넌트지만, 두 개의 다른 컴포넌트로 분리할 수 있다. 즉, 통신 경로에서 골키퍼 같은 역할을 하는 단독 포탈 컴포넌트를 배치하거나, 클라이언트 사이드(예: 노트북 에이전트) 및 리소스 사이드(예 : 리소스 앞에 위치하여 액세스를 컨트롤하는 게이트웨이 컴포넌트)로 분리할 수 있다. 정책 집행 포인트를 통과하면, 기업 리소스를 호스팅하는 트러스트 존이 있다.

제로 트러스트 아키텍처를 실행하고 있는 기업은 몇몇 데이터 소스를 정책 엔진의 입력으로 사용하거나, 정책 규칙으로 사용하여, 액세스를 결정한다. 데이터 소스는 외부 데이터 소스(즉, 기업이 생성하거나 컨트롤하지 않는다.) 뿐만 아니라 로컬 데이터 소스를 포함한다.

- 상시 진단/보완 시스템(Continuous diagnostics and mitigation, CDM) : CDM은 기업 자산의 현재 상태에 대한 정보를 수집하고, 설정 및 소프트웨어 컴포넌트를 업데이트 한다. 기업의 CDM 시스템은 액세스를 요청하는 자산에 대한 정보(적절한게 패치된 OS를 운영중인지, 기업이 승인한 소프트웨어 컴포넌트가 무결성을 유지하고 있는지, 비승인된 컴포넌트가 존재하는지, 자산이 취약점을 가지고 있는지)를 정책 엔진에 제공한다. 또한, CDM 시스템은 기업 인프라에 연결된 非기업 디바이스에 적용할 정책을 식별/집행하는 역할을 한다.

- 업계 컴플라이언스 시스템 : 업계 컴플라이언스 시스템은 기업이 영향을 받는 규제(예: FISMA, 의료 또는 금융 업계의 정보 보안 요구사항)를 준수하고 있음을 보증한다. 여기에는 기업이 컴플라이언스를 보증하기 위해 개발한 모든 정책 규칙이 포함된다.

- 위협 인텔리전스 피드 : 위협 인텔리전스 피드는 내/외부 소스에서 정책 엔진이 액세스를 결정하는 것을 도울 수 있는 정보를 제공한다. 위협 인텔리전스 피드는 복수의 서비스일 수 있으며, 다수의 내/외부 소스에서 데이터를 가져와서 새로 발견된 공격이나 취약점에 대한 정보를 제공한다. 또한 여기에는 새로 발견된 소프트웨어의 결함, 새로 식별된 악성코드, 다른 자산에 대한 보고된 공격(정책 엔진은 기업 자산이 공격을 받은 자산에 액세스하는 것을 거부할 것이다.)을 포함한다.

- 네트워크 및 시스템 액티비티 로그 : 이 시스템은 자산 로그, 네트워크 트래픽, 리소스 액세스 및 다른 이벤트들을 종합한다. 이런 이벤트들은 기업 정보 시스템의 보안 상태에 대한 실시간(또는 실시간에 준하는) 피드백을 제공한다.

- 데이터 액세스 정책 : 데이터 액세스 정책이란, 기업 리소스 액세스와 관련한 속성, 규칙, 정책을 말한다. 규칙은 관리 인터페이스를 통해서 인코딩되거나, 정책 엔진에 의해 동적으로 생성될 수 있다. 정책은 기업의 계정/애플리케이션/서비스에 기본적인 액세스 권한을 제공한다. 즉, 정책은 리소스에 대한 액세스를 인가하는 출발선starting point이다. 정책은 조직에서 정의한 역할 및 필요에 기반해야 한다.

- 기업 공개키 인프라스트럭처(PKI) : 이 시스템은 기업이 리소스/주체/서비스/애플리케이션에 발행한 인증서를 생성하고, 로그를 기록한다. 글로벌 인증 기관 생태계와 공공 PKI도 포함되며, 기업 PKI와 통합할 수도 있다. 또한, X.509 인증서에 기반하지 않은 PKI일 수도 있다.

- ID 관리 시스템 : ID 관리 시스템(예: LDAP 서버)은 기업 사용자 계정 및 식별 기록을 생성/저장/관리한다. ID 관리 시스템은 주체에 대한 필수 정보(예: 이름, 이메일, 인증서)와 기업에서의 특성(역할, 액세스 속성, 할당된 자산 등)을 포함한다. ID 관리 시스템은 사용자 계정과 관련된 아티팩트에 대해서는 다른 시스템(PKI 등)을 이용하는 경우가 많다. ID 관리 시스템은 연합된 커뮤니티의 소유일 수도 있고, 협업을 위해 기업 소속이 아닌 임직원이나 기업 소유가 아닌 자산에 대한 링크가 포함될 수 있다.

- SIEM Security Information and Event Management 시스템 : SIEM은 추후 분석을 위한 보안 중심의 정보를 수집한다. 이 정보는 정책을 개선하고, 기업 자산에 대한 공격 가능성을 경고하기 위해 사용한다.

3.1. 제로 트러스트 아키텍처에 대한 다양한 접근법

기업의 워크플로우에 대해 제로 트러스트 아키텍처를 수립하는 방법은 몇 가지가 있다. 이러한 접근법들은 사용하는 컴포넌트가 다르고, 정책 규칙의 메인 소스가 다르다. 각 접근법은 제로 트러스트의 모든 원리(섹션 2.1 참조)를 실행하지만, 일부 원리에 중점을 두고 정책을 수립할 수 있다. 완전한 제로 트러스트 솔루션은 아래에서 설명할 세 가지 접근법의 모든 요소를 포함할 것이다. 이 접근법들에는 강화된 아이덴티티 거버넌스, 논리적 마이크로 세그멘테이션, 네트워크 기반 세그멘테이션이 포함된다.

일부 유스케이스에 더 적합한 접근법이 있다. 제로 트러스트 아키텍처를 수립하는 조직은 선택한 유스케이스와 기존 정책에 특정 접근법이 더 적합하다는 것을 인지할 것이다. 이는 다른 접근법이 유효하지 않다는 것을 의미하지 않는다. 다만, 다른 접근법은 구현하기 더 어렵고, 기업의 현재 비즈니스 플로우에 근본적인 변화가 필요할 수 있다.

3.1.1. 강화된 아이덴티티 거버넌스를 사용한 제로 트러스트 아키텍처

강화된 아이덴티티 거버넌스 접근 방법은 행위자의 아이덴티티를 핵심 요소로 설정하여 정책을 작성한다. 기업 리소스에 액세스를 요청하는 주체가 없다면, 액세스 정책을 작성할 필요가 없다. 이 접근 방법의 경우, 기업 리소스에 대한 액세스 정책은 아이덴티티와 할당된 속성을 기반으로 한다. 리소스 액세스를 위한 기본 요구사항은 주체에게 부여된 액세스 권한을 기반으로 결정된다. 다른 요소(사용하는 디바이스, 자산 상태, 환경 요소)는 최종 신뢰도 계산에 영향을 주거나, 몇몇 방법(네트워크 위치에 따라 특정 데이터 소스에 대해서는 부분적인 액세스만 허용)으로 결과를 변경한다. 각 리소스 또는 정책 집행 포인트는 요청을 정책 엔진으로 포워딩할 수 있거나, 액세스를 허가하기 전에 주체를 인증하고 요청을 승인할 수 있어야 한다.

개방형 네트워크 모델, 방문객의 액세스를 허용하는 기업 네트워크 모델, 또는 기업 소유가 아닌 디바이스가 자주 연결되는 기업 네트워크 모델을 사용하는 기업은 강화된 아이덴티티 거버넌스 기반 접근법을 채택하는 경우가 많다.(4.3 섹션의 유스케이스 참조) 처음에는 모든 자산에게 네트워크 액세스가 허용된다. 하지만, 기업 리소스에 대한 액세스는 적절한 액세스 권한을 갖는 아이덴티티로 제한된다. 네트워크 연결을 기본적으로 허가하는 것은 악의적인 행위자가 네트워크의 정보를 수집하거나, 내부 또는 서드파티에 대한 DoS 공격에 네트워크가 사용될 수 있다는 단점이 있다. 기업은 이러한 행위가 워크플로우에 영향을 미치기 전에 모니터링하고 지속적으로 대응해야 한다.

아이덴티티 주도 접근법은 리소스 포털 모델(섹션 3.2.3 참조)에 유효하다. 디바이스 아이덴티티 및 상태는 액세스를 결정하는데 참조할 수 있는 부가적인 데이터를 제공하기 때문이다. 다른 모델에서도 유효하지만, 정책에 영향을 받는다. 클라우드 기반 애플리케이션/서비스는 기업이 운영중인 제로 트러스트 컴포넌트를 사용할 수 없을 수 있다. 아이덴티티 주도 접근법은 이러한 클라우드 기반 애플리케이션/서비스를 사용하는 기업에도 유효하다. 기업은 이러한 플랫폼에서 정책을 생성/실행하기 위해 요청자의 아이덴티티를 사용할 수 있다.

3.1.2. 마이크로 세그멘테이션을 사용한 제로 트러스트 아키텍처

기업은 보안 게이트웨이로 보호되는 단독 네트워크 세그먼트에 개별 리소스 또는 리소스 그룹을 배치하는 방식으로 제로 트러스트 아키텍처를 구현할 수 있다. 이 접근법에서 기업은 개별 리소스 또는 관련된 소규모 리소스 그룹을 보호하는 인프라스트럭처 디바이스(인텔리전트 스위치, 라우터, 차세대 방화벽, 특별한 목적의 게이트웨이 디바이스 등)를 배치하며, 이는 정책 집행 포인트 역할을 한다. 대안으로 기업은 호스트 기반 마이크로 세그멘테이션(소프트웨어 에이전트 또는 엔드포인트 자체 방화벽을 사용)을 구현할 수 있다. 이러한 게이트웨이 디바이스는 클라이언트/자산/서비스의 개별 액세스 요청을 동적으로 허용한다. 모델에 따라 게이트웨이는 단독 정책 결정 포인트일 수도 있고, 게이트웨이와 클라이언트 에이전트로 구성된 정책 집행 포인트의 일부분일 수도 있다.

이 접근법은 다양한 유스케이스 및 배치 모델에 적용된다. 보호를 수행하는 디바이스가 정책 집행 포인트 역할을 하고, 정책 엔진 및 정책 관리자는 이런 디바이스를 관리한다. 이 접근법이 완전히 기능하기 위해서는 아이덴티티 거버넌스 프로그램IGP이 필요하다. 하지만, 인가되지 않은 액세스 및 탐색으로부터 리소스를 방어하는 것은 정책 집행 포인트로 기능하는 게이트웨이에 의존한다.

이 접근법은 정책 집행 포인트가 관리되고, 필요(위협 및 워크플로우 변화에 대응)에 따라 정책 집행 포인트가 대응/재구성하는 기능이 필수적이다. 구형 게이트웨이 디바이스 및 스테이트리스stateless 방화벽으로도 이 접근법(micro-segmented enterprise)의 일부 기능을 구현할 수 있다. 하지만, 관리 비용이 높고, 변화에 빠르게 적응하기 어렵기 때문에 매우 좋지 못한 선택이다.

3.1.3. 네트워크 인프라스럭처 및 SDP를 사용한 제로 트러스트 아키텍처

마지막 접근법은 제로 트러스트 아키텍처를 구현하기 위해 네트워크 인프라스트럭처를 사용한다. 제로 트러스트 아키텍처는 오버레이 네트워크(즉, L7, OSI의 하위 계층으로도 설정 가능)를 사용하여 구현할 수 있다. 이런 방식을 소프트웨어 정의 경계SDP[1]라고 부르기도 하며, 소트프웨어 정의 네트워크SDN[2] 및 인텐트 기반 네트워킹IBN[3]의 개념을 주로 포함하고 있다. 이 접근법에서 정책 관리자는 네트워크 컨트롤러로 기능한다. 네트워크 컨트롤러는 정책 엔진의 결정에 따라 네트워크를 구성하고 재구성한다. 클라이언트는 정책 집행 포인트를 통해 액세스를 계속 요청하며, 정책 집행 포인트는 정책 관리자에 의해 관리된다.

애플리케이션 레이어(즉, L7)에서 이 접근법을 구현할 때, 가장 일반적인 모델은 에이전트/게이트웨이이다.(섹션 3.2.1 참조) 에이전트와 리소스 게이트웨이(PEP로 기능하고, 정책 관리자에 의해 설정)는 클라이언트-리소스 사이의 통신에 사용할 보안 채널을 설정한다. 클라우드 가상 네트워크, IP 기반이 아닌 네트워크 등에도 이 모델을 변형하여 사용할 수 있다.

1 SDP : Software Defined Perimeter
2 SDN : Software Defined Network
3 IBN : Intent-Based Networking

3.2. 제로 트러스트 아키텍처의 다양한 배치

위에서 언급한 모든 컴포넌트는 논리 컴포넌트이다. 이 컴포넌트가 반드시 단독 시스템일 필요는 없다. 자산 하나가 다수 논리 컴포넌트의 역할을 수행할 수 있다. 마찬가지로, 논리 컴포넌트 하나가 태스크를 실행하기 위해 다수의 하드웨어/소프트웨어로 구성될 수 있다. 예를 들어, 기업 PKI는 디바이스에 인증서를 발행하는 컴포넌트와 엔드 유저에게 인증서를 발행하는 컴포넌트가 다르다. 그러나, 두 컴포넌트는 동일한 중간 인증서(루트 인증서 인증 기관에서 발급)를 사용한다. 현재 마켓에서 구입할 수 있는 제로 트러스트 제품 중에서 일부는 정책 엔진과 정책 관리자를 하나의 서비스로 제공한다.

선택된 아키텍처의 컴포넌트를 배치하는 형태에는 몇 가지 변형이 있다. 기업 네트워크가 구축된 상황에 따라, 한 기업에서도 서로 다른 비즈니스 프로세스에 다양한 제로 트러스트 아키텍처 배치 모델이 사용될 수 있다.

3.2.1. 디바이스 에이전트-게이트웨이 기반 배치

이 배치 모델에서는 정책 집행 포인트를 두 개의 컴포넌트(리소스에 상주하는 컴포넌트, 리소스의 바로 앞에 위치한 컴포넌트)로 분리한다. 예를 들어, 기업이 지급한 자산에는 연결을 제어하는 디바이스 에이전트가 설치된다. 리소스 바로 앞에는 게이트웨이를 설치하여, 리소스가 게이트웨이와만 통신하게 한다. 게이트웨이는 기본적으로 리소스의 프록시로 기능한다. 에이전트는 소프트웨어 컴포넌트이다. 이 소프트웨어 컴포넌트는 요청을 평가하기 위해 일부(또는 모든) 트래픽을 적절한 정책 집행 포인트로 보낸다. 게이트웨이는 정책 관리자와 통신하여, 정책 관리자에 의해 승인된 통신 경로만 허용하는 역할을 한다.(그림 3 참조)

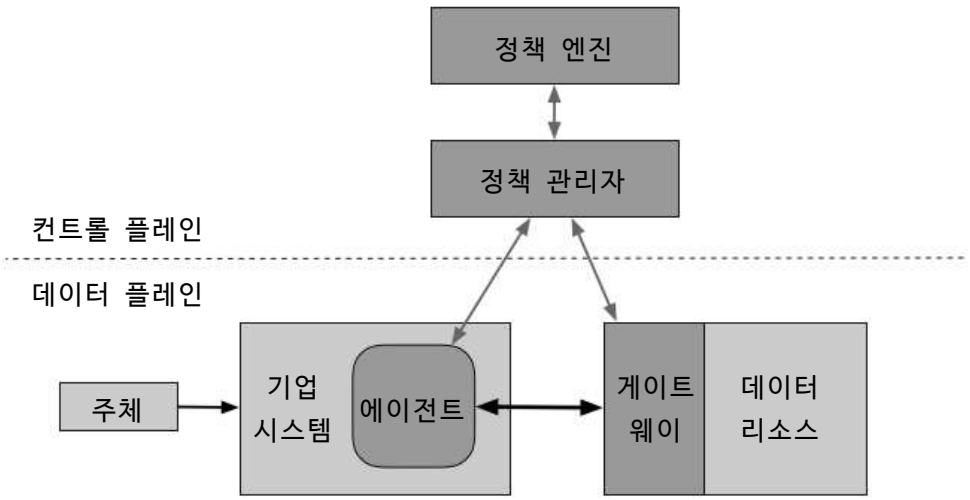

그림 3 : 디바이스 에이전트-게이트웨이 모델

일반적으로 기업에서 지급한 노트북을 소지한 주체가 기업 리소스(예: 인사 애플리케이션/데이터베이스)에 접속한다. 로컬 에이전트는 액세스 요청을 받고, 요청을 정책 관리자로 포워딩한다. 정책 관리자와 정책 엔진은 기업의 로컬 자산이거나, 클라우드 서비스일 수 있다. 정책 관리자는 요청을 평가하기 위해 요청을 정책 엔진으로 포워딩한다. 요청이 인가되면, 정책 관리자는 데이터 플레인에서 디바이스 에이전트와 관련된 리소스 게이트웨이 사이의 통신 채널을 설정한다. 여기에는 IP 주소, 포트, 세션, 또는 이와 유사한 보안 아티팩트 등의 정보가 포함된다. 디바이스 에이전트와 게이트웨이가 연결되면, 암호화된 애플리케이션/서비스 데이터 플로우가 시작된다. 워크플로우가 완료되거나, 보안 이벤트(예: 세션 타임아웃, 재인증 실패)로 정책 관리자가 종료를 트리거하면, 디바이스 에이전트와 리소스 게이트웨이 사이의 연결을 종료한다.

이 모델은 개별 리소스가 게이트웨이와 통신할 수 있고, 강력한 디바이스 관리 프로그램을 보유한 기업에 최적이다. 클라우드 서비스를 많이 사용하는 기업의 경우, 이 모델은 클라우드 보안 연합 소프트웨어 정의 경계CSA-SDP[1]의 클라이언트-서버를 구현한다. 또한, 이 모델은 BYOD 정책을 도입하지 않는 기업에 적합하다. 디바이스 에이전트를 통해서만 액세스할 수 있고, 디바이스 에이전트는 기업 소유의 자산에 설치할 수 있다.

3.2.2. 소규모 집합 기반 배치

소규모 집합 기반 배치 모델은 위에서 언급한 디바이스 에이전트/게이트웨이 모델의 변형이다. 이 모델에서는 게이트웨이가 모든 리소스의 앞에 위치하지 않는다. 대신, 소규모 리소스 집합의 경계(예: 데이터 센터)에 위치한다.(그림 4 참조) 이러한 리소스들은 하나의 비즈니스 기능을 제공하거나, 또는 게이트웨이와 직접 통신할 수 없을 수도 있다. 게이트웨이와 통신하기 위한 API를 가지고 있지 않은 레거시 데이터베이스 시스템이 이 사례이다. 이 배치 모델은 하나의 비즈니스 프로세스(예: 사용자 알림, 데이터베이스 검색, 급여 지급)를 위해 클라우드 기반 마이크로서비스를 사용하는 기업에도 유용할 수 있다. 이 모델에서 프라이빗 클라우드는 모두 게이트웨이 뒤에 위치한다.

이 모델은 디바이스 에이전트-게이트웨이 모델과 하이브리드로 적용하는 것도 가능하다. 이 하이브리드 모델에서 기업 자산은 디바이스 에이전트를 갖는다. 디바이스 에이전트는 소규모 집합 게이트웨이와 통신하는데 사용되지만, 디바이스 에이전트-게이트웨이 모델과 동일한 프로세스를 사용하여 연결된다.

하이브리드 모델은 개별적으로 게이트웨이를 가질 수 없는 레거시 애플리케이션 또는 데이터 센터를 보유한 기업에 유용하다. 기업은 디바이스 에이전트를 설치/설정하기 위해, 견고한 자산 관리 프로그램 및 형상 관리 프로그램이 필요하다. 단점으로는 각각의 리소스를 보호할 수 없으며, 주체가 액세스 권한이 없더라도 리소스를 볼 수는 있다는 것이다.

1 CSA-SDP : the Cloud Security Alliance Software Defined Perimeter

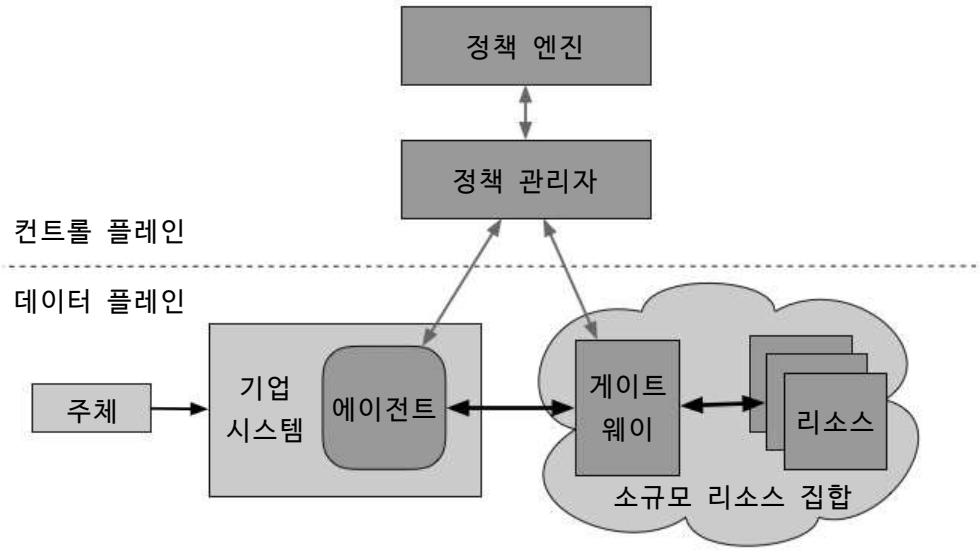

그림 4 : 소규모 집합 게이트웨이 모델

3.2.3. 리소스 포털 기반 배치

리소스 포털 기반 배치 모델에서 정책 집행 포인트는 주체 요청에 대한 게이트웨이로 동작한다. 게이트웨이 포털은 각 리소스별로 배치하거나, 하나의 비즈니스 기능을 위해 사용되는 소규모 보안 리소스 집합에 배치할 수 있다. 프라이빗 클라우드 또는 레거시 애플리케이션을 보유한 데이터 센터를 예로 들 수 있다.(그림 5 참조)

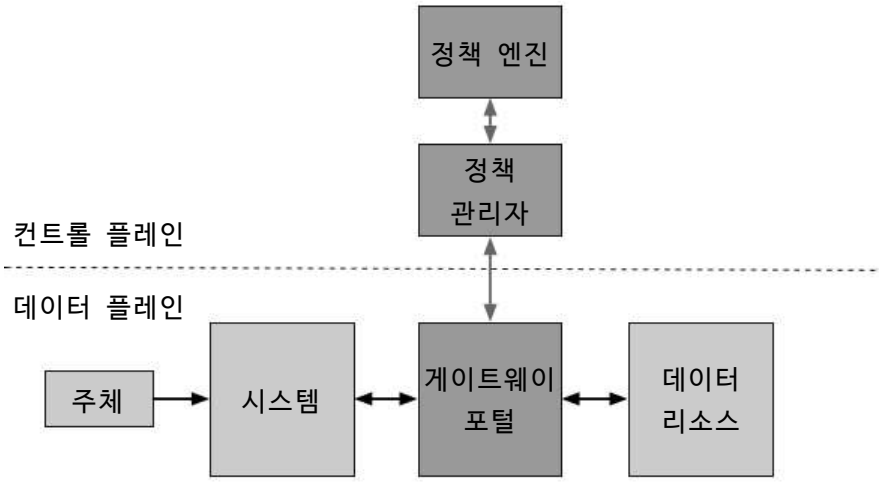

그림 5 : 리소스 포털 모델

이 모델의 주요한 장점은 모든 클라이언트 디바이스에 소프트웨어 컴포넌트를 설치할 필요가 없다는 것이다. 또한, 이 모델은 BYOD 정책 및 조직간 협업 프로젝트에도 유연하게 적용할 수 있다. 기업 관리자는 각 디바이스에 적절한 에이전트가 설치되어 있는지 확인할 필요가 없다. 하지만, 액세스를 요청하는 디바이스로부터 제한된 정보만 추측할 수 있다. 이 모델은 자산/디바이스가 게이트웨이 포털에 접속할 때에만 자산/디바이스를 스캔하고 분석할 수 있다. 이 모델은 자산/디바이스에 악성코드가 있는지, 패치되지 않은 취약점이 있는지, 적절하게 설정되었는지 지속적으로 모니터링할 수 없을 것이다.

이 모델의 주요한 차이점은 요청을 처리하는 로컬 에이전트가 없다는 것이다. 기업은 자산이 포털에 접속했을 때에만 자산을 확인/스캔할 수 있다. 따라서, 자산에 대해 완전한 가시성을 가질 수 없고, 임의로 통제할 수도 없을 것이다. 기업은 이를 완화하거나 보상하기 위해 브라우저 격리와 같은 대책을 채택할 수 있지만, 자산을 확인할 수 없을지도 모른다. 또한, 이 모델은 공격자가 포털을 검색하여 액세스하거나, DoS 공격을 시도할 수 있다. 포털 시스템은 DoS 공격 또는 네트워크 장애에 대한 가용성을 갖도록 잘 준비되어야 한다.

3.2.4. 디바이스 애플리케이션 샌드박싱

디바이스 에이전트-게이트웨이 배치 모델의 또 다른 변형으로 심사된 애플리케이션/프로세스를 자산에서 격리하여 실행하는 모델이 있다. 이러한 격리는 가상 머신, 컨테이너 등이 있지만, 목적은 동일하다. 자산에서 실행 중인 다른 애플리케이션 및 침해 가능성이 있는 호스트로부터 애플리케이션 또는 애플리케이션 인스턴스를 보호하는 것이다.

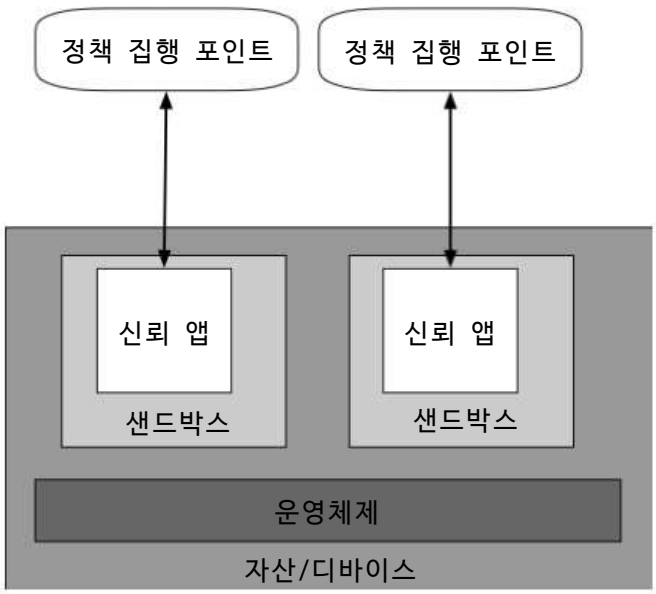

그림 6 : 애플리케이션 샌드박스

그림 6에서, 디바이스(주체)는 심사되고 승인된 애플리케이션을 샌드박스에서 실행한다. 애플리케이션은 정책 집행 포인트와 통신하여, 리소스에 대한 액세스를 요청한다. 정책 집행 포인트는 자산에 있는 다른 애플리케이션의 요청은 거부한다. 이 모델에서 정책 집행 포인트는 기업의 로컬 서비스 또는 클라우드 서비스일 수 있다.

이 모델의 주요한 장점은 애플리케이션이 자산 내에서 분리된다는 것이다. 자산의 취약점을 스캔할 수 없더라도, 샌드박싱된 애플리케이션이 악성코드에 감염되지 않도록 보호할 수 있을 것이다. 이 모델의 단점은 기업이 모든 자산의 샌드박싱된 애플리케이션을 관리해야 한다는 것이다. 그리고, 클라이언트 자산에 대한 완전한 가시성을 가질 수 없을지도 모른다. 또한, 기업은 각 샌드박싱된 애플리케이션이 안전하다는 것을 확인할 필요가 있다. 이는 단순히 디바이스를 모니터링하는 것보다 더 많은 노력이 필요할지도 모른다.

3.3. 트러스트 알고리즘

제로 트러스트 아키텍처를 실시한 기업의 경우, 정책 엔진을 두뇌로, 정책 엔진의 트러스트 알고리즘[TA[1]]을 주요한 사고 프로세스로 간주할 수 있다. 트러스트 알고리즘은 리소스에 대한 액세스를 최종적으로 허가/거부하기 위해 정책 엔진이 사용하는 프로세스이다. 정책 엔진은 다양한 소스(섹션 3 참조)에서 입력(주체, 주체의 속성/역할, 주체의 행동 패턴, 위협 인텔리전스, 그 외 메타데이터)을 가져온다. 이 프로세스는 그림 7과 같이 개략적인 카테고리로 나눌 수 있다.

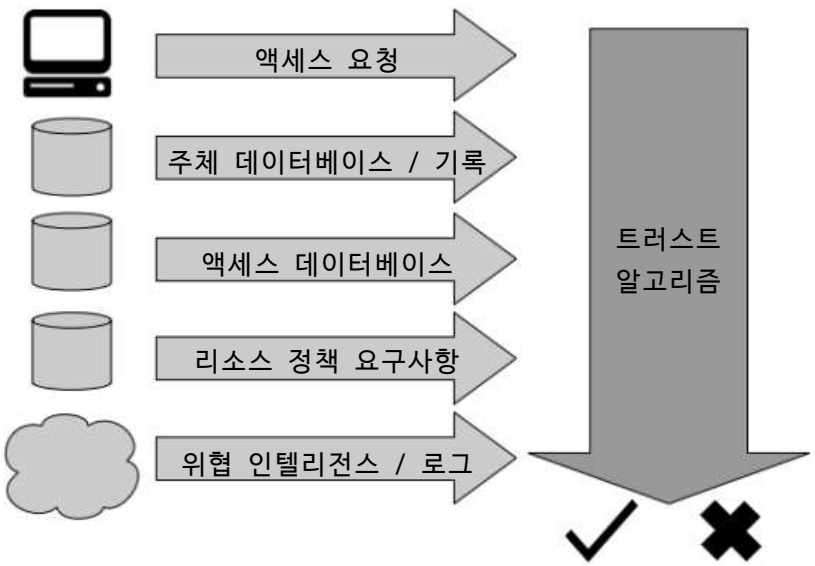

그림 7 : 트러스트 알고리즘의 입력

[1] TA : Trust Algorithm

이 그림에서, 입력은 트러스트 알고리즘에 무엇을 제공하는지에 따라 나눌 수 있다.

- 액세스 요청 : 액세스 요청이란, 주체의 실제 요청이다. 액세스 요청에서 사용되는 주요 정보는 요청된 리소스지만, 요청자에 대한 정보도 사용된다. 요청자에 대한 정보에는 OS 버전, 사용 중인 소프트웨어(예: 요청에 사용된 애플리케이션이 승인된 애플리케이션인가?), 패치 정보를 포함될 수 있다. 이러한 정보와 자산의 보안 상태에 따라, 자산에 대한 액세스를 제한하거나 거부할 수 있다.

- 주체 데이터베이스 : 주체 데이터베이스는 누가 리소스에 액세스를 요청하는지에 대한 것이다.[SP800-63] 주체 데이터베이스는 기업 또는 협력사의 주체(사람/프로세스), 주체에 할당된 속성/권한의 모음이다. 이러한 주체 및 속성/권한은 리소스 액세스를 위한 정책 기준을 형성한다.[SP800-162][NISTIR 7987] 사용자 아이덴티티는 논리 아이덴티티(예: 계정 ID)의 조합, 정책 집행 포인트가 수행한 인증 확인 결과가 포함될 수 있다. 신뢰도를 도출할 때 고려할 수 있는 아이덴티티 속성은 시간과 지리적 위치가 포함된다. 다수 주체에게 부여된 권한들을 역할로 생각할 수 있다. 하지만, 개인별로 권한을 할당해야 한다. 이러한 권한들은 특정 역할에 적합할지도 모르기 때문이다. 이 권한들을 인코딩해서 ID 관리 시스템 및 정책 데이터베이스에 저장해야 한다. 일부 변형된 트러스트 알고리즘에는 과거에 관측된 주체 행위에 대한 데이터도 포함할 수 있다.(섹션 3.3.1 참조)

- 자산 데이터베이스 : 자산 데이터베이스는 기업 소유(및 인지할 수 있는 기업 소유가 아닌 자산, BYOD) 자산(물리/가상/기타)의 상태를 포함하는 데이터베이스이다. 자산 데이터베이스와 요청한 자산의 상태를 비교한다. 자산 데이터베이스에는 OS 버전, 설치된 소프트웨어, 무결성, 위치(네트워크 위치 및 지리적 위치), 패치 정보가 포함될 수 있다. 자산 데이터베이스와 자산 상태를 비교하여, 자산에 대한 액세스를 제한하거나 거부할 수 있다.

- 리소스 요구사항 : 리소스 요구사항은 사용자 ID 및 속성 데이터베이스[SP800-63]를 보완하고, 리소스에 액세스하기 위한 최소한의 요구사항을 정의한다. 리소스 요구사항에는 네트워크 위치(예 : 해외 IP 액세스 거부) 및 데이터 민감도 등의 인증 보증 레벨AAL[1]이 포함될 수 있고, 자산 설정에 대한 요구사항도 포함될 수 있다. 이러한 요구사항은 데이터 관리자 및 데이터를 사용하는 비즈니스 프로세스 책임자 양쪽에서 개발되어야 한다.

1 AAL : Authenticator Assurance Level

- 위협 인텔리전스 : 위협 인텔리전스는 일반적인 위협 및 유행하는 악성코드에 대한 정보 피드이다. 위협 인텔리전스는 의심스러운 디바이스로부터의 통신(악성코드 C&C일 수도 있는 노드의 쿼리)과 관련된 특정 정보를 포함할 수 있다. 위협 인텔리전스는 외부 서비스를 이용할 수도 있고, 내부의 스캔 및 탐지 결과를 이용할 수도 있다. 또한, 공격 패턴이나 보완 대책을 포함할 수 있다. 위협 인텐리전스는 기업이 통제하지 않고, 서비스가 통제하고 있을 가능성이 높은 유일한 컴포넌트이다.

각 데이터 소스의 중요성에 대한 가중치는 외부 개발 알고리즘을 사용할 수 있고, 기업이 설정할 수도 있다. 데이터 소스가 기업에게 얼마나 중요한지를 가중치에 반영할 수도 있다.

실행에 대한 최종 결정은 정책 관리자에게 넘어간다. 정책 관리자는 필요한 정책 집행 포인트를 설정하여 승인된 통신을 가능하게 한다. 제로 트러스트 아키텍처가 어떻게 배치되었는지에 따라, 정책 집행 포인트(게이트웨이, 에이전트, 리소스 포털)를 설정하기 위해 인증 결과 및 연결 설정 정보를 정책 집행 포인트로 보낼 수 있다. 정책 관리자는 정책 요구사항에 따라 연결을 재인증/재인가하기 위해 통신 세션을 보류하거나 잠시 멈출 수도 있다. 또한, 정책 관리자는 정책에 따라 연결을 종료(예 : 타임아웃, 워크플로우 완료, 보안 알림)하기 위한 명령을 내린다.

3.3.1. 트러스트 알고리즘의 변형

트러스트 알고리즘을 구현하는 방법은 다양하다. 위에서 언급한 입력들의 중요성을 어떻게 인식하는지에 따라 가중치를 다르게 주어 구현하고 싶을지도 모른다. 트러스트 알고리즘을 차별화하려면, 크게 두 가지 특징을 사용할 수 있다. 첫 번째는 입력을 평가하는 방법이다. 이는 이진 판단, 가중치를 적용한 총점/신뢰도의 등이다. 두 번째는 같은 주체, 같은 애플리케이션/서비스, 같은 디바이스에서의 다른 요청과 비교하여 요청을 평가하는 방법이다.

- 기준 기반 vs 점수 기반 : 기준 기반의 트러스트 알고리즘은 리소스에 대한 액세스를 승인하거나, 액션(예 : 읽고/쓰기)을 허가하기 전에 반드시 만족해야 하는 속성들을 검증한다. 이러한 기준은 기업이 설정하며, 모든 리소스에 대해 독립적으로 설정해야 한다. 모든 기준을 만족한 경우에만 액세스를 허가하거나, 리소스에 대한 액션을 적용한다. 점수 기반의 트러스트 알고리즘은 모든 데이터 소스에 대한 가치와 기업이 설정한 가중치에 기반하여 신뢰도를 계산한다. 점수가 설정된 경계값보다 크면, 액세스를 허가하거나 액션을 수행한다. 점수가 설정된 경계값보다 작으면, 요청이 거부되거나 액세스 권한이 줄어든다.(예 : 파일에 대한 읽기는 허가하지만, 쓰기는 허가하지 않음)

- 단독 vs 맥락 : 단독 트러스트 알고리즘은 각 요청을 개별적으로 다룬다. 그리고, 평가할 때 주체의 이력을 고려하지 않는다. 이는 평가의 속도를 빠르게 할 수 있다. 하지만, 공격이 주체에게 허용된 역할 내에서 이루어지면, 공격이 탐지되지 않을 수 있다. 맥락 트러스트 알고리즘은 액세스 요청을 평가할 때 주체 또는 네트워크 에이전트의 최근 이력을 고려한다. 이는 정책 엔진이 모든 주체/애플리케이션에 대한 상태 정보 일부를 유지해야 한다는 것을 의미한다. 또한, 정책 엔진이 주체와 상호작용하는 PA/PEP에 사용자의 행위를 알려야 한다는 것을 의미한다. 주체 행위 분석을 사용하여 허용 가능한 사용 모델을 만들 수 있고, 이 행위와의 편차를 통해 추가적인 인증 검사 또는 리소스 요청 거부를 트리거할 수 있다.

위에서 언급한 두 가지 특징이 서로에게 항상 의존하지는 않는다. 모든 주체/디바이스에 신뢰도가 할당되고, 모든 액세스 요청을 독립적으로(즉, 단수로) 판단하는 트러스트 알고리즘을 가질 수도 있다. 하지만, 맥락, 점수 기반 트러스트 알고리즘은 더욱 동적이고 세밀하게 액세스를 통제할 수 있다. 점수는 요청자의 현재 신뢰도를 제공하고, 관리자가 정책을 수정하는 것 보다 입력 변화에 더 빠르게 적응하기 때문이다.

이상적으로 트러스트 알고리즘은 문맥적이어야 한다. 하지만, 문맥적 트러스트 알고리즘은 기업의 인프라스트럭처에 항상 적용할 수 있지는 않다. 문맥적 트러스트 알고리즘은 공격자가 정상적인 액세스를 요청할 수 있는 장소 근처에 머무르며 주체를 침해하거나 내부를 공격하는 위협을 완화할 수 있다. 트러스트 알고리즘을 정의하고 구현할 때, 보안-사용성-비용 대비 효과의 균형을 이루는 것이 중요하다. 조직 내부의 관습적/일반적인 행위에 대해 지속적으로 재인증을 요구하면, 사용성에 이슈가 생길 수 있다. 예를 들어, 인사팀 직원이 하루에 직원 20~30명에 대한 기록에 액세스하는 것이 일반적이라면, 맥락적 트러스트 알고리즘은 하루에 100명에 대한 기록에 액세스하면 경고를 보낼 수도 있다. 또한, 맥락적 트러스트 알고리즘은 누군가가 일반적인 근무 시간 후에 액세스하면 경고를 보낼 수도 있다. 이 사람이 침해된 인사 계정을 사용하여 기록을 유출하려는 공격자일 수 있기 때문이다. 이런 예에서 문맥적 트러스트 알고리즘은 공격자를 탐지할 수 있지만, 단독 트러스트 알고리즘은 새로운 행위를 탐지하지 못할 수 있다. 또 다른 예로, 일반적인 근무시간에 재무 시스템에 접속하는 컨설턴트가 알 수 없는 장소에서 한밤 중에 시스템에 액세스하려는 경우, 맥락적 트러스트 알고리즘은 경고를 발령하고, 주체에게 더 높은 신뢰도나 NIST SP 800-63A에 명시된 다른 기준을 만족하도록 요구할 수 있다.

각 리소스에 대한 기준 또는 가중치/경계값을 설정할 때는 계획과 테스트가 필요하다. 기업 관리자는 제로 트러스트 아키텍처의 실행 초기에 잘못된 설정으로 승인되어야 할 액세스 요청이 거부되는 문제에 직면할 수 있다. 이러한 상황은 실행 초기의 튜닝 단계에서 발생할 것이다. 기업의 비즈니스 프로세스가 기능하면서 정책이 확실히 적용되도록 기준 또는 점수의 가중치를 조정해야 할 수도 있다. 이 튜닝 단계가 얼마나 지속될지는 진행현황에 대해 기업이 정의한 지표 및 워크플로우에 사용되는 리소스에 대한 잘못된 액세스 승인/거부를 얼마나 허용하는지에 달려있다.

3.4. 네트워크/환경 컴포넌트

제로 트러스트 환경에서는 네트워크를 제어/설정하는데 사용되는 커뮤니케이션 플로우와 조직에서 실무를 수행하기 위해 사용되는 애플리케이션/서비스 커뮤니케이션 플로우가 논리적 또는 물리적으로 분리되어야 한다. 보통 네트워크 제어 커뮤니케이션 플로우를 위한 컨트롤 플레인과 애플리케이션/서비스 커뮤니케이션 플로우를 위한 데이터 플레인으로 분리한다.[Gilman]

컨트롤 플레인은 다양한 인프라스트럭처 컴포넌트(기업 소유, 서비스 제공자 소유)에서 자산을 유지/설정하고, 리소스에 대한 액세스를 판단/허가/거부하며, 리소스 사이의 커뮤니케이션 경로를 설정하기 위해 필요한 모든 작업을 수행하기 위해 사용된다. 데이터 플레인은 소프트웨어 컴포넌트 사이의 커뮤니케이션을 위해 사용된다. 이 커뮤니케이션 채널은 컨트롤 플레인을 통해 경로가 설정되기 전까지 사용하지 못할 수도 있다. 즉, 정책 관리자 및 정책 집행 포인트가 주체와 기업 리소스 사이의 커뮤니케이션 경로를 설정하기 위해 컨트롤 플레인을 사용할 수 있다. 그 후 애플리케이션/서비스 워크로드가 설정된 데이터 플레인 경로를 사용한다.

3.4.1. 제로 트러스트 아키텍처를 지원하기 위한 네트워크 요구사항

1. 기업 자산은 기본적으로 네트워크에 연결된다. LAN은 기업의 통제 여부와 관계없이 기본 라우팅과 인프라스트럭처(예 : DNS)를 제공해야 한다. 원격 자산은 인프라스트럭처의 모든 서비스를 반드시 사용하지 않을 수 있다.

2. 기업은 기업이 소유하거나 관리하는 자산을 구별할 수 있어야 하고, 디바이스의 현재 보안 상태를 구별할 수 있어야 한다. 이는 기업이 발행한 크리덴셜로 결정해야 하며, 인증할 수 없는 정보(예 : MAC 주소, 스푸핑 가능)는 사용해서는 안된다.

3. 기업은 모든 네트워크 트래픽을 감시할 수 있어야 한다. 기업은 데이터 플레인에서 검출된 패킷을 기록해야 한다. 애플리케이션 레이어(즉, OSI 7번째 레이어)에서 검사를 수행할 수 없더라도 패킷을 기록해야 한다. 기업은 액세스 요청을 평가할 때 커넥션 관련 메타데이터(예: 목적지, 시간, 디바이스 아이덴티티)를 필터링하여, 정책을 동적으로 업데이트하고, 정책 엔진에 전달해야 한다.

4. 정책 집행 포인트에 액세스하지 않고, 기업 리소스에 접근할 수 없어야 한다. 기업 리소스는 인터넷으로부터 임의의 연결을 받아들이지 않아야 한다. 리소스는 클라이언트가 승인/인가된 후에만 연결을 받아들인다. 통신 경로는 정책 집행 포인트에 의해 설정된다. 심지어 정책 집행 포인트에 액세스하지 않으면, 리소스를 발견할 수 없을 수도 있다. 이는 공격자가 스캐닝을 통해 타겟을 식별할 수 없게 하고, 정책 집행 포인트 뒤에 위치한 리소스에 대해 DoS 공격을 할 수 없게 한다. 모든 리소스

를 이러한 방법으로 감추어서는 안된다. 일부 네트워크 인프라스트럭처 컴포넌트(예: DNS 서버)는 반드시 접근할 수 있어야 한다.

5. 데이터 플레인과 컨트롤 플레인은 논리적으로 분리해야 한다. 정책 엔진, 정책 관리자, 정책 집행 포인트는 논리적으로 분리되어, 기업 자산/리소스가 직접 액세스할 수 없는 네트워크에서 통신한다. 데이터 플레인은 애플리케이션/서비스 데이터 트래픽에 사용된다. 정책 엔진, 정책 관리자, 정책 집행 포인트는 컨트롤 플레인을 사용하여 자산 사이의 통신 경로를 관리하고 통신한다. 정책 집행 포인트는 데이터 플레인과 컨트롤 플레인으로 메시지를 보내고 받을 수 있어야 한다.

6. 기업 자산은 정책 집행 포인트에 접근할 수 있어야 한다. 기업 주체는 리소스에 액세스하기 위해 반드시 정책 집행 포인트에 액세스할 수 있어야 한다. 이는 웹 포털, 네트워크 디바이스 또는 소프트웨어 에이전트의 형태를 취할 수 있다.

7. 정책 집행 포인트는 비즈니스 플로우에서 정책 관리자에 접근하는 유일한 컴포넌트이다. 기업 네트워크에서 각 정책 집행 포인트는 통신 경로(클라이언트 → 리소스)를 설정하기 위해 정책 관리자와 연결된다. 기업 비즈니스 프로세스의 모든 트래픽은 한 개 이상의 정책 집행 포인트를 통과한다.

8. 원격 기업 자산은 기업 네트워크 인프라스트럭처를 통과하지 않고 기업 리소스에 액세스할 수 있어야 한다. 예를 들어, 기업에서 퍼블릭 클라우드 제공자가 제공하는 서비스(예: 이메일)를 이용하는 경우, 원격 주체에게 기업 네트워크(즉, VPN) 사용을 요구하지 않아야 한다.

9. 제로 트러스트 아키텍처의 액세스 결정 프로세스에 사용되는 인프라스트럭처는 프로세스 부하의 변화를 고려하여 확장할 수 있어야 한다. 제로 트러스트 아키텍처에서 사용되는 정책 엔진, 정책 관리자, 정책 집행 포인트는 모든 비즈니스 프로세스에서 핵심 컴포넌트이다. 정책 집행 포인트로 연결이 지연/중단되거나, 정책 집행 포인트가 정책 엔진/정책 관리자에 연결할 수 없다면, 워크플로우를 수행하는 능력에 부정적인 영향을 미친다. 제로 트러스트 아키텍처를 시행하는 기업은 워크로드를 예상하여 컴포넌트를 마련하거나, 증가된 사용량을 처리할 수 있도록 인프라스트럭처를 신속히 확장할 수 있어야 한다.

10. 정책 또는 식별할 수 있는 요소에 의해, 기업 자산이 특정 정책 집행 포인트에 연결되는 것을 제한할 수 있어야 한다. 예를 들어, 해외의 모바일 자산은 특정 리소스에 연결할 수 없다고 명시한 정책이 있을지도 모른다. 식별할 수 있는 요소로는 위치(지리적 위치 또는 네트워크의 위치), 디바이스 종류 등의 기준을 사용할 수 있다.

4. 배치 시나리오 / 유스케이스

모든 기업 환경은 제로 트러스트 원리를 고려하여 설계할 수 있다. 대부분의 조직은 인프라스트럭처에 제로 트러스트의 일부 요소를 이미 가지고 있거나, 정보 보안/복구 정책/모범 사례를 시행하는 중이다. 일부 배치 시나리오 및 유스케이스는 제로 트러스트 아키텍처에 매우 적합하다. 예를 들어, 제로 트러스트 아키텍처는 지역적으로 분산되어 있는 기업이나, 이동이 많은 직원을 보유한 기업에서 시작되었다. 즉, 모든 기업은 제로 트러스트 아키텍처에서 이익을 얻을 수 있다.

아래 유스케이스에서 제로 트러스트 아키텍처를 분명하게 명시하지 않았다. 기업은 경계 기반 인프라스트럭처와 제로 트러스트 아키텍처를 모두 가지고 있을 수 있기 때문이다. 섹션 7.2에서 설명하겠지만, 제로 트러스트 아키텍처 컴포넌트와 경계 기반 네트워크 인프라스트럭처가 동시에 운영될 기간이 있을 것이다.

4.1. 위성 시설을 보유한 기업

본사와 복수의 지사(기업이 소유한 물리적 네트워크로 연결되지 않음)로 구성된 기업이 가장 일반적인 시나리오이다.(그림 8) 지사의 네트워크는 기업 소유가 아닐 수도 있다. 하지만, 지사의 직원들은 임수를 수행하기 위해 기업 리소스에 액세스할 필요가 있다. 기업은 본사 네트워크에 연결하기 위해 다중 프로토콜 레이블 스위치MPLS[1]를 가지고 있을지도 모른다. 하지만, 모든 트래픽을 수용하기에 대역폭이 충분하지 않거나, 클라우드 기반 애플리케이션/서비스를 목적지로 하는 트래픽이 본사 네트워크를 통과하는 것을 원하지 않을 수도 있다. 마찬가지로, 직원들이 기업 소유의 디바이스나 본인 소유의 디바이스를 이용하여, 집이나 지점에서 근무할 수 있다. 이러한 경우, 기업은 일부 리소스(예 : 일정표, 이메일)에 대해서는 액세스를 허용하지만, 민감한 리소스(예: 인사 데이터베이스)에 대해서는 액션을 제한하거나 액세스를 거부하기를 원할지도 모른다.

이 유스케이스에서는 정책 엔진/정책 관리자를 클라우드 서비스에 호스팅[2]하고, 자산에 에이전트를 설치(섹션 3.2.1 참조)하거나 리소스 포털에 액세스(섹션 3.2.3 참조)한다. 정책 엔진/정책 관리자를 기업 네트워크에 호스팅하면 응답성에 손해를 볼 수 있다. 집이나 지사에서 클라우드에 호스팅된 애플리케이션/서비스에 연결하려면, 모든 트래픽을 기업의 로컬 네트워크로 다시 보내야 하기 때문이다.

1 MLPS : Multiprotocol Label Switch
2 가용성이 우수하고, 원격 근무자가 리소스에 액세스하기 위해 기업 인프라스트럭처에 의존하지 않음

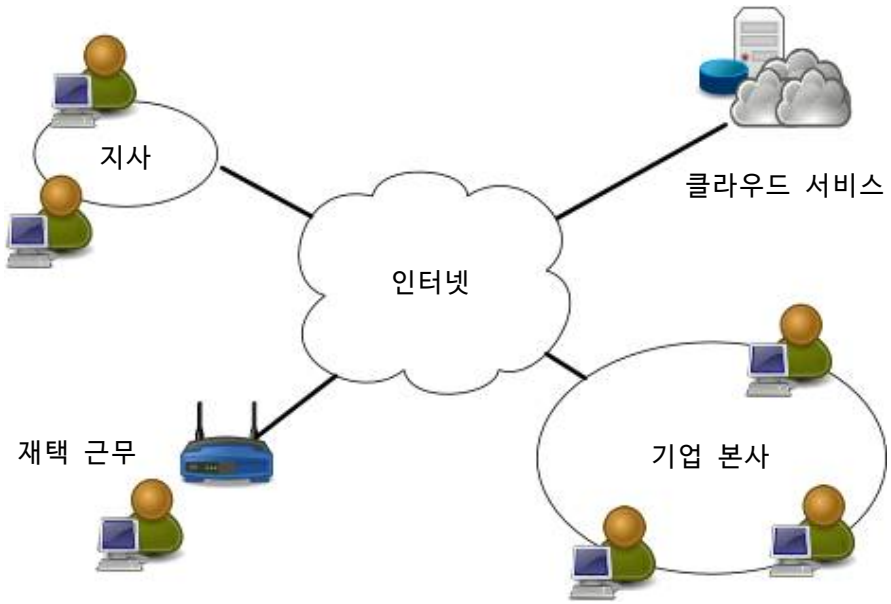

그림 8 : 원격 근무

4.2. 멀티 클라우드 및 C2C[cloud-to-cloud]를 이용하는 기업

제로 트러스트 아키텍처의 대표적인 유스케이스 중 하나로 다수의 클라우드 서비스 제공자를 사용하는 기업이 있다. 이 유스케이스에서 기업은 로컬 네트워크를 가지고 있지만, 두 개 이상의 클라우드 서비스 제공자를 사용하여 애플리케이션/서비스 및 데이터를 호스팅한다. 애플리케이션/서비스 중에는 데이터 소스가 다른 클라우드 서비스에 호스팅되는 경우도 있다. 성능과 관리 용이성을 위해, 애플리케이션이 기업 네트워크로 터널링하여 다시 보내는 것 보다는 클라우드 A에 호스팅된 애플리케이션은 클라우드 B에 호스팅된 데이터 소스에 직접 연결할 수 있어야 한다.

이 유스케이스는 CSA-SDP의 서버-서버 배치 모델을 구현한 것이다. 기업이 클라우드 호스팅 더 많은 애플리케이션/서비스을 클라우드 서비스에 호스팅함에 따라, 기업이 보안을 경계에 의지하는 것은 부채가 될 것이 분명해진다. 섹션 2.2에서 언급한 것처럼, 제로 트러스트 원칙에서는 기업이 소유/운영하는 네트워크 인프라스트럭처와 다른 서비스 제공자가 소유/운영하는 인프라스트럭처 사이에는 차이가 없다고 본다. 멀티 클라우드 사용과 관련하여, 제로 트러스트는 각 애플리케이션/서비스 및 데이터 소스의 액세스 포인트에 어떻게 정책 집행 포인트를 설치할 것인지로 접근한다. 정책 엔진과 정책 관리자는 멀티 클라우드 중 어떤 클라우드에라도 호스팅될 수 있고, 심지어 다른 서비스 제공자의 클라우드라도 관계없다. 클라이언트는 (포털 또는 에이전트가 설치된 로컬 시스템을 통해서) 정책 집행 포인트에 직접 접속한다. 이런 방법으로 기업은 리소스가 외부에 호스팅된 경우에도 리소스에 대한 액세스를 관리할 수 있다. 한 가지 문제점은 클라우드 제공자별로 동일한 기능을 서로 다른 방법으로 실행한는 것이다. 기업은 클라우드 서비스 제공자가 기업의 제로 트러스트 아키텍처를 어떻게 시행하는지 알아야 할 필요가 있다.

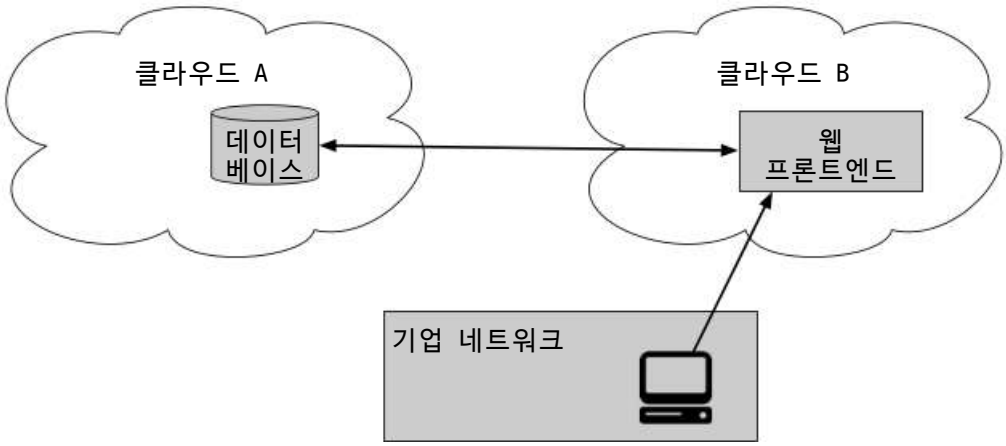

그림 9 : 멀티 클라우드 유스케이스

4.3. 외부 서비스 계약 등 외부 인원의 액세스가 필요한 기업

업무를 위해 기업 리소스에 제한된 액세스가 필요한 계약 서비스 제공자 및 현장 방문객이 있는 기업이다.(그림 10 참조) 예를 들어, 기업은 내부 애플리케이션/서비스, 데이터베이스, 자산을 가지고 있다. 여기에는 유지보수를 위해 계약된 서비스도 포함되며, 가끔씩 현장을 방문한다. (예: 외부 제공자가 소유하고 관리하는 난방 및 조명 시스템) 이러한 방문객 및 서비스 제공자는 임무를 수행하기 위해 네트워크에 연결이 필요하다. 제로 트러스트 기업은 기업 리소스를 차폐하면서, 방문 서비스 기술자 및 관련 디바이스는 인터넷에 액세스할 수 있도록 허가할 수 있다.

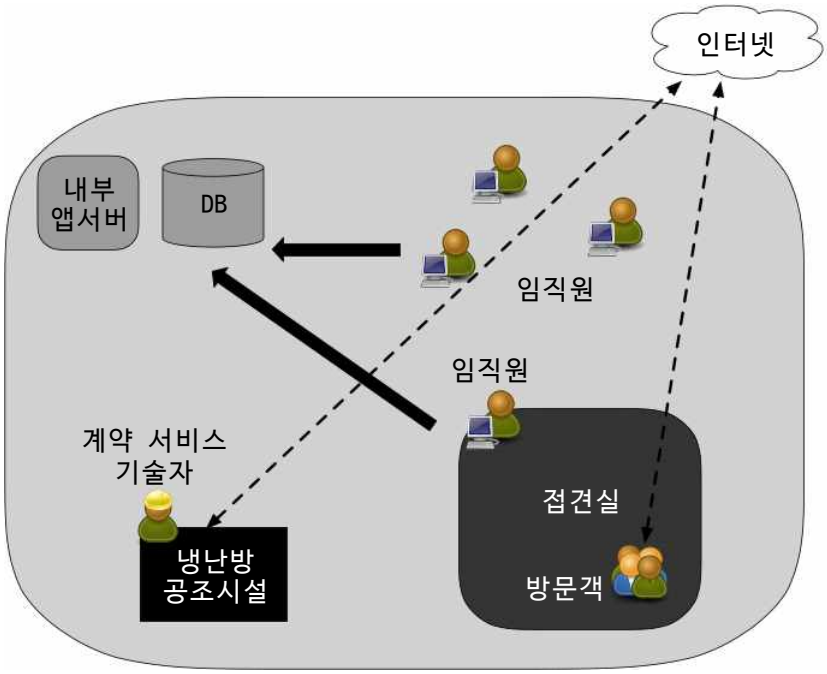

그림 10 : 외부 인원의 액세스가 필요한 기업

이 사례에서 조직은 직원과 방문객이 교류하는 접견실도 가지고 있다. 제로 트러스트 아키텍처를 시행하면, 접견실에 있는 직원과 방문객을 구분한다. 직원은 적절한 기업 리소스에 액세스할 수 있다. 반면, 방문객은 인터넷에 액세스할 수 있지만, 기업 리소스에는 액세스할 수 없다. 심지어 방문객은 네트워크 스캔을 통해 기업 서비스를 탐색할 수도 없을 것이다. 즉, 네크워크 정보 수집 및 내부 이동을 방어한다.

이 유스케이스에서 정책 엔진과 정책 관리자를 클라우드 서비스 또는 LAN에 호스팅할 수 있다. 기업 자산은 에이전트가 설치(섹션 3.2.1 참조)되거나, 포털을 통해 리소스에 액세스(섹션 3.2.3 참조)할 것이다. 정책 관리자는 모든 외부 자산(에이전트가 설치되지 않았거나 포털에 접속할 수 없음)의 로컬 리소스 액세스는 막으면서, 인터넷에는 액세스할 수 있게 한다.

4.4. 기업 間 협업

네 번째 유스케이스는 기업 간 협업이다. 예를 들어, 기업 A와 기업 B의 직원이 관여하는 프로젝트가 있다.(그림 11 참조) 두 기업은 정부 기관이 될 수도 있고, 정부 기관 대 민간 기업이 될 수도 있다. 기업 A에서 프로젝트를 위한 데이터베이스를 운영한다. 하지만, 기업 B의 특정 직원은 데이터에 액세스할 수 있어야 한다. 기업 A는 기업 B의 직원을 위해 특별한 계정을 설정하여, 필요한 데이터에 대해서는 액세스를 허가하고 다른 리소스에 대해서는 액세스를 거부한다. 그러나, 이 방법은 관리가 어려울 수 있다. 연합 ID 관리 시스템에 두 조직이 모두 등록되어 있다면, 두 조직의 정책 집행 포인트는 연합 ID 관리 시스템에서 주체를 인증할 수 있어 빠르게 이러한 관계를 설정할 수 있다.

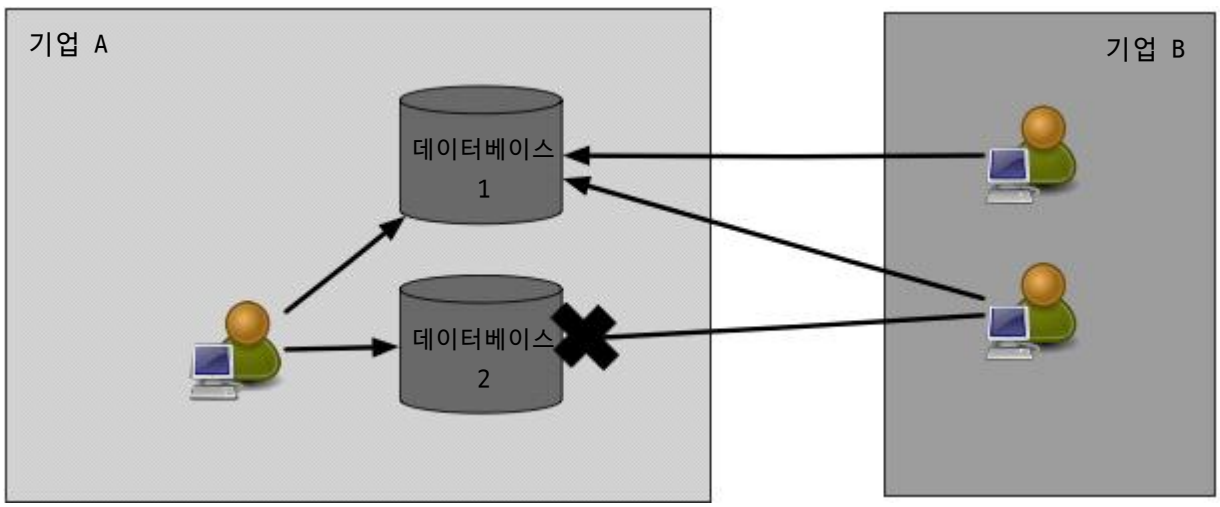

그림 11 : 기업 間 협업

이 시나리오는 두 기업의 직원이 조직의 네트워크 인프라스트럭처에 위치하지 않을 수 있고, 직원들이 액세스하는 리소스가 기업 내부 또는 클라우드에 호스팅 될 수 있다는 점에서 첫 번째 유스케이스(섹션 4.1)와 유사점이 있다. 이는 기업 B의 특정 IP 주소가 기업 A의 액세스 정책에 기반하여 기업 A의 리소스에 액세스할 수 있게 하기 위해, 방화벽 룰 또는 ACL을 복잡하게 설정할 필요가 없다는 의미이다. 이 액세스를 실현하는 방법은 사용중인 기술에 따라 다르다. 첫 번째 유스케이스와 유사하게 정책 엔진과 정책 관리자가 클라우드 서비스에 호스팅되면, VPN 등을 이용하지 않고 모든 관계자가 사용할 수 있다. 기업 B의 직원은 자산에 소프트웨어 에이전트를 설치하거나, 웹 게이트웨이를 통해 필요한 데이터 리소스에 액세스할 수 있다.(섹션 3.2.3 참조)

4.5. 공개 서비스 또는 고객 서비스를 제공하는 기업

공개 서비스는 많은 기업이 공통적으로 제공하는 기능이다. 공개 서비스는 사용자를 등록(즉, 사용자는 로그인 크리덴셜을 작성하고, 사용자에게 로그인 크리덴셜이 발행됨)하거나, 등록하지 않을 수 있다. 공개 서비스는 일반인, 비즈니스 관계가 있는 고객, 또는 임직원 가족과 같은 특별한 사용자를 위한 것일 수 있다. 어떤 경우든 요청하는 자산은 기업 소유가 아닐 가능성이 높고, 기업은 내부 사이버 보안 정책 적용에 제약을 받는다.

액세스를 위해 로그인 크리덴셜을 요구하지 않는 공개 리소스에 대해서는 제로 트러스트 아키텍처의 원리를 직접 적용하지 않는다. 기업은 요청하는 자산의 상태를 엄격하게 통제할 수 없고, 공개 리소스(예 : 공개 웹 페이지)를 액세스하기 위해 크리덴셜이 필요하지 않다.

기업은 고객(즉, 비즈니스 관계가 있는), 특수한 사용자(예 : 임직원 가족)와 같은 등록된 사용자를 위한 정책을 설정할 수 있다. 사용자가 크리덴셜을 생성하거나 발급받아야 하는 경우, 기업은 패스워드의 길이, 라이프 사이클 및 기타 세부적인 사항에 대한 정책을 수립할 수 있고, 옵션 또는 요구사항으로 다중 인증을 제공할 수 있다. 그러나, 기업이 이러한 유형의 사용자를 위해 구현할 수 있는 정책은 한계가 있다. 요청에 포함된 정보는 공개 서비스의 상태를 결정하고, 정상적인 사용자를 가장한 공격을 탐지하는데 도움이 될지도 모른다. 예를 들어, 등록된 고객이 일반적인 웹 브라우저 중 하나를 이용하여 사용자 포털에 액세스한다는 것을 알고 있다면, 불분명하거나 구버전의 브라우저에서 액세스 요청이 갑자기 증가하는 것은 일종의 자동화된 공격을 의심할 수 있고, 기업은 식별된 클라이언트의 요청을 제한하는 조치를 취할 수 있다. 기업은 사용자 및 자산에 대해 어떤 정보를 수집하고 기록할 수 있는지에 관련한 법령 및 규제에 주의해야 한다.

5. 제로 트러스트 아키텍처 관련 위협

어떤 기업도 사이버 보안 위험을 제거할 수 없다. 기존 사이버 보안 정책/지침, 아이덴티티/자산 관리, 상시 모니터링, 일반적 사이버 보안으로 보완하고, 제로 트러스트 아키텍처를 적절하게 시행/관리하면 전반적인 위험을 줄일 수 있고, 일반적인 위협으로부터 보호할 수 있다. 그러나, 제로 트러스트 아키텍처를 구현했을 때, 독특한 특징을 갖는 위협들이 있다.

5.1. 제로 트러스트 아키텍처의 결정 프로세스 무력화

제로 트러스트 아키텍처에서 정책 엔진 및 정책 관리자는 핵심 컴포넌트이다. 정책 엔진 및 정책 관리자가 승인/설정하지 않으면, 기업 리소스 사이의 어떠한 커뮤니케이션도 이루어질 수 없다. 이는 반드시 정책 엔진 및 정책 관리자를 적절하게 설정/관리해야 한다는 것을 의미한다. 정책 엔진의 룰을 설정할 수 있는 기업 관리자는 승인없이 룰을 변경하거나, 기업 운영에 지장을 주는 실수를 할 수 있다. 마찬가지로, 정책 관리자가 침해되면, 승인되지 않은 리소스에 대한 액세스를 허용할 것이다. 관련된 위험을 완화한다는 것은 정책 엔진 및 정책 관리자를 적절하게 설정/모니터링하고, 모든 설정 변경을 반드시 기록/감사해야 한다는 것을 의미한다.

5.2. DoS 또는 네트워크 장애

제로 트러스트 아키텍처에서 정책 관리자는 리소스 액세스에 대한 핵심 컴포넌트이다. 정책 관리자가 허가/설정하지 않으면, 기업 리소스는 서로 연결할 수 없다. 공격자가 정책 집행 포인트, 정책 엔진 또는 정책 관리자에 대한 액세스를 방해/거부하면(즉, DoS 공격 또는 라우팅 하이재킹), 기업의 운영에 부정적인 영향을 미칠 수 있다. 기업은 이들을 적절하게 보호되는 클라우드 환경에 두거나, 사이버 내성cyber resiliency에 관한 지침[SP 800-160 v2]에 따라 몇몇 위치에 복제하여, 이 위협을 완화할 수 있다.

이를 통해 위험을 완화할 수 있지만, 제거하지는 못한다. 미라이Mirai같은 봇넷은 핵심 인터넷 서비스 제공자에 대한 대규모 DoS 공격으로 수많은 인터넷 사용자에 대한 서비스를 방해할 수 있다. 공격자는 일부 또는 모든 사용자 계정(예 : 지사 또는 원격 근무자)에서 정책 집행 포인트 또는 정책 관리자로 가는 트래픽을 가로채거나 가로막을 수 있다. 이러한 경우, 조직 주체의 일부만 영향을 받는다. 이는 기존 VPN에서도 발생할 수 있으며, 제로 트러스트 아키텍처에서만 발생하는 것은 아니다.

호스팅 제공자가 실수로 클라우드 기반 정책 엔진 또는 정책 관리자를 오프라인[offline]할 수도 있다. 과거에 클라우드 서비스, IaaS 및 SaaS에서 장애가 발생한 사례가 있다. 운영 실수로 정책 엔진 또는 정책 관리자를 네트워크에서 액세스할 수 없게 되면, 전체 기업의 기능을 마비시킬 수 있다.

정책 관리자가 기업 리소스에 연결하지 못하는 위험도 있다. 이 경우, 주체에게 액세스가 허용되어 있어도, 정책 관리자는 커뮤니케이션 경로를 설정할 수 없다. 이는 DDoS 공격 때문일 수도 있고, 단순히 과도한 사용량 때문일 수도 있다. 이는 어떤 이유로 리소스를 사용할 수 없기 때문에 일부 또는 모든 기업 주체가 특정 리소스에 액세스할 수 없다는 점에서 다른 네트워크 장애와 유사하다.

5.3. 크리덴셜 도용 및 내부자 위협

제로 트러스트, 정보 보안, 복구 정책, 모범 사례를 적절하게 시행하면, 크리덴셜 도용 또는 내부자 위협을 통해 공격자가 광범위한 액세스를 얻는 위험을 줄일 수 있다. '네트워크 위치에 기반한 암묵적 트러스트는 없다'는 제로 트러스트 원칙으로 인해, 공격자가 기업에 발판을 마련하려면 계정 또는 디바이스를 침해할 필요가 있다. 제로 트러스트 아키텍처는 침해된 계정 또는 자산이 일반적인 권한 또는 액세스 패턴과 다르게 리소스에 액세스하는 것을 방지해야 한다. 공격자가 노리는 리소스에 액세스할 수 있는 계정이 공격자의 주요 타켓이 될 것이다.

공격자는 중요한 계정의 크리덴셜을 획득하기 위해 피싱, 사회 공학, 또는 이러한 공격을 조합하여 사용할 수 있다. "중요한"이라는 의미는 공격자의 동기에 따라 달라질 수 있다. 예를 들어, 기업 관리자 계정은 중요하다. 하지만, 금전적 이득을 노리는 공격자는 재정 또는 결재 리소스에 액세스할 수 있는 계정을 관리자 계정과 동등한 가치가 있다고 생각할 수 있다. 액세스 요청을 위해 다중 인증을 구현하면, 침해된 계정으로 정보가 유출되는 위험을 줄일 수 있다. 그러나, 유효한 크리덴셜(또는 악의적인 내부자)을 가진 공격자는 여전히 리소스에 액세스할 수 있다. 예를 들어, 공격자 또는 악의를 가진 임직원이 인사담당자의 유효한 크리덴셜과 기업 소유 자산을 갖게 되면, 인사 데이터베이스에 계속 액세스할 수 있다.

제로 트러스트 아키텍처는 위험을 줄이고, 모든 침해된 계정 또는 자산을 이용하여 네트워크 내부에서 이동하는 것을 방지한다. 침해된 크리덴셜이 특정 리소스에 액세스하는 것을 인가하지 않으면, 침해된 크리덴셜이 그 리소스에 액세스하는 것은 지속 거부될 것이다. 추가적으로, 맥락적 트러스트 알고리즘(섹션 3.3.1 참조)은 이 공격이 레거시한 경계 기반 네트워크에서 일어났을 때보다 탐지하고 빠르게 대응할 가능성이 높다. 맥락적 트러스트 알고리즘은 일반적인 행위와 다른 액세스 패턴을 탐지하기 때문에, 침해된 계정 또는 악의적인 내부자가 민감한 리소스에 액세스하는 것을 거부할 수 있다.

5.4. 네트워크 가시성

섹션 3.4.1에서 언급한 것처럼, 네트워크의 모든 트래픽을 검사/기록하고, 기업에 대한 잠재적인 공격을 식별/대응하기 위해 분석한다. 그러나, 기업 네트워크의 일부 트래픽은 3계층 네트워크 분석 도구로는 잘 보이지 않는다. 이러한 트래픽은 기업이 소유하지 않은 자산(예 : 인터넷에 액세스하기 위해 기업 인프라스트럭처를 사용하는 계약된 서비스)이 원인이거나, 수동 모니터링에 내성이 있는 애플리케이션/서비스이 원인이 될 수 있다. 패킷 심층 검사를 수행할 수 없거나, 암호화된 트래픽을 조사할 수 없는 기업의 경우, 네트워크에서 공격자가 존재할 가능성을 평가하기 위해 다른 방법을 사용해야만 한다.

하지만, 기업이 네트워크의 암호화된 트래픽을 분석할 수 없다는 것은 아니다. 기업은 암호화된 트래픽에 대한 메타 데이터(예 : 출발지 및 목적지 IP 주소 등)를 수집하여, 네트워크에서 커뮤니케이션하고 있는 공격자 또는 악성코드를 탐지하는데 사용할 수 있다. 복호화/검사할 수 없는 트래픽을 분석하기 위해 머신러닝[Anderson]을 사용할 수 있다. 이런 유형의 머신러닝을 도입하면, 기업은 유효한 트래픽과 악의적일 수 있어 대응이 필요한 트래픽으로 분류할 수 있다.

5.5. 시스템/네트워크 정보 스토리지

모니터링 및 네트워크 트래픽 분석에 관련된 위협은 분석 컴포넌트 그 자체에 있다. 모니터링, 네트워크 트래픽, 메타 데이터를 맥락적 정책, 포렌식, 사후 분석을 위해 저장하고 있다면, 이 데이터는 공격자의 타겟이 된다. 네트워크 다이어그램, 설정 파일, 기타 네트워크 아키텍처 문서와 마찬가지로, 이런 리소스는 보호되어야 한다. 공격자가 이런 정보를 얻는데 성공하면, 공격자는 기업 아키텍처에 대한 지식을 얻을 수 있고, 다음으로 어떤 자산에 대한 정보를 수집하고 공격해야 하는지 식별할 수 있다.

공격자는 액세스 정책을 인코딩하기 위해 사용하는 관리 도구에서도 정보를 수집할 수 있다. 저장된 트래픽과 마찬가지로, 이 관리 도구는 리소스에 대한 액세스 정책을 포함하고 있어, 공격자는 침해를 위해 어떤 계정이 가장 가치가 있는지에 대한 정보를 얻을 수 있다. (예 : 원하는 데이터 리소스에 액세스할 수 있는 계정)

모든 중요한 기업 데이터는 인가되지 않은 액세스 및 액세스 시도를 예방하기 위해 적절히 보호되어야 한다. 이런 리소스는 보안에 필수적이기 때문에 가장 제한이 엄격한 액세스 정책을 설정하여, 지정된 관리자 계정만 액세스하게 해야 한다.

5.6. 전용 데이터 포맷 또는 솔루션에 대한 의존

제로 트러스트 아키텍처는 몇몇 데이터 소스에 의존하여 액세스를 결정한다. 여기에는 요청하는 주체, 사용된 자산, 기업 인텔리전스, 외부 인텔리전스, 위협 분석에 관한 정보 등이 포함된다. 이러한 정보를 저장/처리하는데 사용되는 자산은 상호 작용 및 정보 교환에 대한 공통의 개방적인 표준이 없는 경우가 많다. 이러한 상황은 상호 운용성 문제로 기업이 일부 제공자에게 종속되는 결과를 초래할 수 있다. 만약 한 제공자에게 보안 이슈 및 장애가 생기면, 기업은 막대한 금액(예: 일부만 세트로 교체)을 들이거나, 장기간의 이전 프로그램(예 : 정책 룰을 다른 포맷으로 변환)을 거치지 않고는 새로운 제공자로 옮길 수 없을 것이다. DoS 공격처럼, 이러한 위험은 제로 트러스트 아키텍처에만 발생하는 것은 아니다. 하지만, 제로 트러스트 아키텍처는 정보의 동적 액세스(기업과 서비스 제공자)에 크게 의존하기 때문에, 장애가 발생하면 기업의 핵심 비즈니스 기능에 영향을 미칠 수 있다. 관련된 위험을 완화하기 위해, 기업은 벤더의 보안 통제, 교체 비용, 공급망 위험 관리, 성능, 안전성과 같은 요소를 고려하여 서비스 제공자를 종합적으로 평가해야 한다.

5.7. 非인간 객체NPE[1]에 의한 제로 트러스트 아키텍처 관리

기업 네트워크에서 발생하는 보안 문제를 관리하기 위해 인공지능 또는 소프트웨어 기반 에이전트를 배치하고 있다. 이런 컴포넌트는 인간 관리자를 대신하여, 제로 트러스트 아키텍처의 관리 컴포넌트(예 : 정책 엔진, 정책 관리자)와 상호작용해야 한다. 제로 트러스트 아키텍처에서 이러한 컴포넌트들이 어떻게 서로를 인증할 것인지는 아직 해결되지 않은 문제이다. 대부분의 자동화된 기술 시스템은 API를 사용하여 리소스 컴포넌트에 접근할 때, 인증을 위해 몇 가지 방법을 사용할 것이라고 가정한다.

설정 및 정책 집행에 자동화된 기술을 사용할 때 발생하는 가장 큰 위험은 기업의 보안 상태에 영향을 줄 수 있는 오탐(무해한 행위를 공격으로 판단)과 미탐(공격을 일반적인 행위로 판단)의 가능성이다. 이는 잘못된 판단을 바로 잡고, 결정 프로세스를 개선하기 위한 정기적인 분석 튜닝을 통해 줄일 수 있다.

제로 트러스트 아키텍처와 관련된 위험은 공격자가 수행할 권한이 없는 몇몇 태스크를 非인간 객체가 수행하도록 유도하거나 강요할 수 있다는 것이다. 소프트웨어 에이전트는 인간 사용자 대비 더 낮은 강도의 인증(예 : API 키 vs 다중 인증)으로 관리 또는 보안 관련 태스크를 수행할 수 있을 지도 모른다. 만약 공격자가 에이전트와 상호작용할 수 있다면, 이론적으로 에이전트를 속여 공격자에게 더 높은 액세스를 허가하거나, 공격자를 대신하여 몇몇 태스크를 수행하게 할 수 있다. 또한, 공격자가 소프트웨어 에이전트의 크리덴셜을 획득하여, 에이전트 행세를 하며 태스크를 수행할 수 있는 위험도 있다.

1 NPE : Non-Person Entities

6. 제로 트러스트 아키텍처와 기존 가이드라인의 연계 가능성

기존 정책/가이드라인 중 일부는 제로 트러스트 아키텍처의 계획/전개/운영과 접점이 있다. 이러한 정책들이 제로 트러스트 아키텍처를 도입하는 것을 가로막지 않지만, 제로 트러스트 전략을 수립하는데 영향을 미칠 수 있다. 기존 사이버 보안 정책/가이드라인, ICAM[Identity, Credential, and Access Management], 지속적인 모니터링, 일반적인 사이버 보안은 보완이 필요하다. 이를 보완했을 때, 비로소 제로 트러스트 아키텍처는 조직의 보안 상태를 강화할 수 있고, 일반적인 위협으로부터 보호할 수 있다.

6.1. 제로 트러스트 아키텍처와 NIST 위험 관리 프레임워크

제로 트러스트 아키텍처를 전개하는 것은 지정된 미션 또는 비즈니스 프로세스에 대한 수용 가능한 위험을 중심으로 액세스 정책을 수립하는 것이 포함된다.(섹션 7.3.3 참조) 리소스에 대한 모든 네트워크 액세스를 거부할 수 있고, 접속된 터미널에서만 액세스를 허용할 수 있다. 그러나, 대부분의 상황에서 이러한 정책은 지나치게 제한적이어서 업무의 목표 달성을 저해할 수 있다. 미션을 수행하기 위해 수용할 수 있는 위험 수준이 있다. 미션 수행과 관련된 위험을 식별하고 평가하고, 받아들이거나 완화해야 한다. 이를 돕기 위해, NIST 위험 관리 프레임워크RMF[1]가 개발되었다.[SP800-37]

제로 트러스트 아키텍처를 계획하고 시행하면, 기업에서 설정한 인가의 한계가 변할 수 있다. 이는 새로운 컴포넌트(예 : 정책 엔진, 정책 관리자, 정책 집행 포인트)가 추가되고, 네트워크 경계 방어에 대한 의존성이 감소했기 때문이다. 그러나, 위험 관리 프레임워크의 전반적인 프로세스는 제로 트러스트 아키텍처에서도 변하지 않을 것이다.

6.2. 제로 트러스트 아키텍처와 NIST 개인정보보호 프레임워크

사용자의 개인 정보(예 : 개인 식별 정보)를 보호하는 것은 조직의 가장 중요한 관심사이다. 연방 정보 보안 현대화에 관련 법률FISMA[2], 의료보험 양도 및 책임에 관한 법률HIPAA[3]와 같은 컴플라이언스 프로그램은 프라이버시/데이터 보호를 포함한다. 이에 따라, NIST는 조직에서 사용하기 위해 개인정보보호 프레임워크[NISTPRIV]를 만들었다. 이 문서에는 조직에서 저장/처리하는 사용자의 개인 정보에 대한 위험을 식별/평가/완화하는 프로세스, 개인 정보 위험과 완화 전략을 설명하는 프레임워크를 제공한다. 여기에는 제로 트러스트 아키텍처를 운영하기 위해 기업이 사용하는 개인 정보 및 액세스 요청 평가에 사용되는 모든 바이오 정보가 포함된다.

1 RMF : Risk Management Framework
2 FISMA : Federal Information Security Modernization Act
3 HIPAA : Heath Insurance Portability and Accountability Act

제로 트러스트의 핵심 요구사항에는 환경 내부의 트래픽을 검사하고 기록하는 것(모니터링 시스템이 트래픽을 복호화할 수 없는 경우에는 최소한 메타 데이터를 검사하고 기록)이 포함된다. 일부 트래픽에는 개인 정보가 포함되어 있거나, 프라이버시와 관련된 위험이 있을 수 있다. 조직은 네트워크 트래픽의 인터셉트/스캔/로깅과 관련하여 발생할 수 있는 모든 위험을 식별할 필요가 있다.[NISTIR 8062] 여기에는 사용자 고지, 로그인 페이지 및 배너 등을 통한 동의 획득, 기업 사용자 교육 등의 액션이 포함될 수 있다. NIST 프라이버시 프레임워크[NISTPRIV]는 제로 트러스트 아키텍처를 개발하고 있는 기업이 프라이버시와 관련된 위험을 식별/완화하는 공식적인 프로세스를 개선하는 데 도움을 줄 수 있다.

6.3. 제로 트러스트 아키텍처와 FICAM[1] 아키텍처

주체 프로비저닝은 제로 트러스트 아키텍처의 핵심 컴포넌트이다. 정책 엔진이 주체 및 리소스를 식별하기 위한 정보를 충분히 획득할 수 없다면, 정책 엔진은 리소스에 연결하기 위한 커넥션 시도를 인가할 것인지 결정할 수 없다. 제로 트러스트 전개를 진행하기 전에 강력한 주체 프로비저닝 및 인증 정책을 마련해야 한다. 기업은 액세스 요청을 평가하기 위해 정책 엔진이 사용할 수 있는 명확한 주체 속성 및 정책이 필요하다.

美 관리예산실OMB[2]은 연방 정부의 아이덴티티 관리 개선에 관련한 정책(M-19-17)을 발표한다. 이 정책의 목적은 “국가 임무 수행/신뢰/안전의 조력자로서 아이덴티티를 위한 공통의 비전”이다.[M-19-17] 이 정책에서는 모든 연방 기관에 ICAMIdentity, Credential, and Access Management 부서를 조직하여, 아이덴티티 발행 및 관리와 관련된 활동을 관리할 것을 요구한다. 이러한 관리 정책의 대부분은 NIST SP 800-63-3, 디지털 아이덴티티 가이드라인[SP800-63]의 권고사항을 사용해야 한다. 제로 트러스트 아키텍처는 정확한 아이덴티티 관리에 크게 의존하기 때문에, 모든 제로 트러스트 아키텍처 활동은 기관의 ICAM 정책과 통합할 필요가 있다.

6.4. 제로 트러스트 아키텍처와 TIC 3.0

TIC는 연방 사이버 보안 이니셔티브이며, 美 관리예산실OMB, 美 국토안보부DHS[3], 美 연방총무청GSA[4]에서 공동으로 관리한다. TIC는 연방 정부 전체의 네트워크 보안 베이스라인 수립을 목적으로 한다. 역사적으로 TIC는 경계 기반 사이버 보안 전략이었고, 기관들이 외부 네트워크 연결을 통합하고 모니터링할 것을 요구했다. TIC 1.0 및 TIC 2.0은 경계의 내부를 “신뢰”한다는 가정이 내재되어 있다. 반면 제로 트러스트 아키텍처는 네트워크의 위치로 “신뢰”를 추론하지 않는다. 즉, 기관의 내부 네트워크는 “신뢰”가 없다. TIC 2.0는 기관 경계의 TIC 액

1 FICAM : Federal Identity, Credential, and Access Management
2 OMB : The Office of Management and Budget
3 DHS : The Department of Homeland Security
4 GSA : The General Services Administration

세스 포인트가 보유해야 할 네트워크 기반 보안 기능(예 : 콘텐츠 필터링, 모니터링, 인증 등)의 목록을 제공한다. 이런 기능의 다수는 제로 트러스트 원칙과 일치한다.

TIC 3.0은 클라우드 서비스 및 모바일 디바이스를 추가하기 위해 업데이트 되었다.[M-19-26] TIC 3.0에서는 “신뢰”가 특정 컴퓨팅 맥락에 따라 다르게 정의될 수 있고, 기관들이 트러스트 존을 정의하기 위한 위험 수용 수준이 다르다는 것을 인정하고 있다. 추가적으로 TIC 3.0은 TIC 보안 기능 핸드북을 업데이트했다. TIC 보안 기능 핸드북에서는 두 가지 형태의 보안 기능을 정의했다. ① 일반적인 보안 기능(기업 레벨에 적용) 및 ② PEP 보안 기능(다수의 PEP에 적용되는 네트워크 레벨의 기능)으로 TIC 유스케이스에 정의되어 있다. PEP 보안 기능은 기관의 경계에 위치한 PEP 한 개에 적용하기 보다, 데이터 플로우에 위치한 모든 PEP에 적용할 수 있다. 이런 TIC 3.0 보안 기능의 다수(예 : 트래픽 암호화, 강력한 인증, 마이크로 세그멘테이션, 네트워크 및 시스템 인벤토리 등)는 제로 트러스트 아키텍처를 직접적으로 지원한다. TIC 3.0은 특정 애플리케이션, 서비스, 환경에서 트러스트 존 및 보안 기능의 구현에 대해 설명하는 구체적인 유스 케이스를 정의한다.

TIC 3.0은 네트워크 기반 보안에 초점을 맞추고 있다. 반면, 제로 트러스트 아키텍처는 더 포괄적인 아키텍처로, 애플리케이션/사용자/데이터를 보호한다. TIC 3.0의 유스 케이스가 발전함에 따라, PEP가 배치된 네트워크 보호를 정의하기 위해 제로 트러스트 아키텍처에서의 TIC 유스 케이스가 개발될 가능성이 높다.

6.5. 제로 트러스트 아키텍처와 EINSTEIN

EINSTEIN으로 더 많이 알려진 국가 사이버 보안 보호 시스템NCPS[1]은 여러 시스템을 통합한 시스템으로, 사이버 위협으로부터 연방 정부를 보호하기 위해 침입 탐지, 고급 분석, 정보 공유 및 침입 차단 기능을 제공한다. NCPS의 목적은 사이버 위험을 관리하고, 사이버 보호를 개선하고, 사이버 공간을 보호하기 위해 파트너에게 권한을 부여하는 것으로 제로 트러스트의 전반적인 목표와 일치한다. EINSTEIN 센서는 사이버 보안 및 인프라 보안국CISA[2]의 국가 사이버 보 보안 및 커뮤니케이션 통합 센터NCCIC[3]가 연방 네트워크를 보호하고, 연방 기관의 중대한 사고에 대응할 수 있게 해준다.

EINSTEIN 센서는 연방 정부의 네트워크 경계 보호에 기초를 둔다. 반면, 제로 트러스트 아키텍처는 자산, 데이터 및 다른 모든 리소스를 더 가까이에서 보호한다. EINSTEIN은 클라우드 기반 트래픽에 대한 보안 정보를 사용하는 방향으로 발전하고 있으며, 이는 제로 트러스트 아키텍처로부터 확장된 상황 인식의 기초를 수립하는데 도움을 준다. EINSTEIN의 침입 차단 기능은 제로 트러스트 아키텍처에 정책 집행을 알릴 수 있도록 발전이 필요하다. 연방 정부에서 제로 트러스트 아키텍처를 채택함에 따라 EINSTEIN은 지속적으로 발전할 필요가 있다. 제로 트러스트 아키텍처를 구현한 연방 기관의 사고 대응 담당자는 인증, 트래픽 검사, 로그에서

1 NCPS : National Cybersecurity Protection System
2 CISA : Cybersecurity & Infrastructure Security Agency
3 NCCIC : National Cybersecurity and Communications Integration Center

정보를 얻을 수 있다. 제로 트러스트 아키텍처에서 생성된 정보는 이벤트의 영향을 정량화하는데 더 적합하다. 머신러닝 도구는 탐지 성능을 개선하기 위해 제로 트러스트 아키텍처의 데이터를 사용한다. 사고 대응 담당자는 사후 분석을 위해 제로 트러스트 아키텍처로부터 추가적인 로그를 저장할 수 있다.

6.6. 제로 트러스트 아키텍처와 美 국토안보부 상시 진단/완화 프로그램

美 국토안보부DHS의 상시 진단/완화CDM[1] 프로그램은 연방 기관의 IT 기술을 개선하기 위한 것이다. 이를 위해 가장 중요한 것은 기관들이 자신의 자산, 설정, 주체를 잘 파악하는 것이다. 시스템 보호를 위해 기관들은 자신의 인프라에 존재하는 기본적인 컴포넌트 및 액터를 발견/이해하기 위한 프로세스를 수립할 필요가 있다.

- 무엇이 연결되어 있나? 조직이 어떤 디바이스/애플리케이션/서비스를 사용하는가? 여기에는 취약점/위협을 발견했을 때, 디바이스/애플리케이션/서비스의 보안 상태를 관찰/개선하는 것이 포함된다.

- 누가 네트워크를 사용하고 있나? 조직에 속한 사용자인가? 외부 사용자인가? 기업 리소스에 액세스가 허용된 사용자인가? 여기에는 자동화된 NPENon-Person Entities도 포함된다.

- 네트워크에서 무슨 일이 벌어지고 있나? 기업은 시스템 사이의 트래픽 패턴과 메시지를 파악해야 한다.

- 데이터를 어떻게 보호하고 있나? 기업은 저장/전송/사용 시 데이터 보호에 대한 정책이 필요하다.

강력한 CDM 프로그램을 구현하는 것은 제로 트러스트 아키텍처의 성공을 위해 가장 중요하다. 예를 들어, 제로 트러스트 아키텍처로 전환할 때, 기업은 사용 가능한 인벤토리를 작성하기 위해 물리/가상 자산을 발견/기록하기 위한 시스템을 갖추어야 한다. 美 국토안보부의 CDM 프로그램은 연방 기관이 제로 트러스트 아키텍처 전환 초기에 필요한 몇몇 역량을 포함하고 있다. 예를 들어, 美 국토안보부의 하드웨어 자산 관리HWAM[2],[HWAM] 프로그램은 기관들이 자신들의 네트워크 인프라에서 디바이스를 식별하여 보안을 설정하는데 도움을 준다. 이는 제로 트러스트 아키텍처 로드맵을 개발할 때의 첫 단계와 비슷하다. 기관들은 네트워크 활동을 분류/설정/감시하기 위해 네트워크에서 자산의 액티브 여부를 반드시 확인(또는 원격으로 그 리소스에 액세스) 할 수 있어야 한다.

1 CDM : Continuous Diagnostics and Mitigations
2 HWAM : Hardware Asset Management

6.7. 제로 트러스트 아키텍처, 클라우드 스마트 전략, 연방 데이터 전략

클라우드 스마트 전략, 업데이트된 데이터 센터 최적화 이니셔티브[M-19-19] 정책, 연방 데이터 전략은 기관이 제로 트러스트 아키텍처를 계획할 때 일부 요구사항에 영향을 준다. 이런 정책들은 기관들이 온 프레미스 및 클라우드에서 데이터를 수집/저장/액세스하는 방법을 목록화하고 평가할 것을 요구한다.

어떤 비즈니스 프로세스 및 리소스에 제로 트러스트 아키텍처를 시행하는 것이 유리한지 결정하는데 이 목록은 매우 중요하다. 데이터 리소스/애플리케이션/서비스가 대부분 클라우드 기반이거나 원격 근무자가 주로 사용한다면, 제로 트러스트 아키텍처 도입을 고려해 볼 만하다. (섹션 7.3.3 참조) 주체와 리소스가 기업 네트워크 경계 외부에 위치해 있고, 사용/확장성/보안에서 최대의 이익을 얻을 가능성이 높기 때문이다.

연방 데이터 전략에서 한 가지 추가적인 고려사항은 기관이 데이터 자산을 다른 기관이나 대중들에게 액세스할 수 있게 하는 방법이다. 이는 제로 트러스트 아키텍처의 기업 간 협업 유스 케이스에 부합한다.(섹션 4.4 참조) 이런 자산에 제로 트러스트 아키텍처를 사용하는 기관들은 전략을 수립할 때 협업이나 공개 요구를 고려할 필요가 있을지도 모른다.

7. 제로 트러스트 아키텍처로의 전환

제로 트러스트 아키텍처를 시행하는 것은 인프라 또는 프로세스의 전면적인 교체보다는 여행에 가깝다. 조직은 가장 높은 가치의 데이터를 보호하기 위해 점진적으로 제로 트러스트 원칙 구현하고, 프로세스를 변화시키고, 기술 솔루션 도입해야 한다. 대부분의 기업은 최신 IT 이니셔티브에 지속 투자하면서, 상당 기간 동안 하이브리드(제로 트러스트 + 경계 기반) 모드로 운영할 것이다. 제로 트러스트 아키텍처로의 전환이 포함된 IT 최신화 계획을 수립하였다면, 기업이 작은 규모의 워크플로우를 전환하기 위한 로드맵을 형성하는데 도움이 될 것이다.

기업이 어떠한 전략으로 전환할 것인지는 기업의 현재 사이버 보안 상태 및 운영에 달려있다. 기업의 역량이 베이스라인에 도달해야 한다. 그 이후 중요한 제로 트러스트 중심 환경[ACT-IAC]을 전개하는 것이 가능하다. 이 베이스라인에는 기업이 자산, 주체, 비즈니스 프로세스, 트래픽 플로우, 의존성을 식별/분류하여 매핑하는 것이 포함된다. 기업은 이 정보를 이용하여, 비즈니스 프로세스 후보 및 이 프로세스에 속하는 주체/자산의 목록을 작성한다.

7.1. 순수 제로 트러스트 아키텍처

그린필드greenfield 접근법을 선택하면, 제로 트러스트 아키텍처를 처음부터 구축할 수 있다. 기업이 업무에 사용하고 싶은 애플리케이션/서비스/워크플로우를 있다면, 그 워크플로우를 위한 아키텍처를 제로 트러스트 원칙에 근거하여 만들 수 있다. 워크플로우를 식별하면, 기업은 필요한 컴포넌트를 최소화할 수 있고, 각 컴포넌트가 어떻게 상호 작용할지 매핑할 수 있다. 이 시점부터 인프라를 구축하고 컴포넌트를 설정하는 것은 엔지니어링 및 훈련의 영역이다. 기업이 어떻게 설립되어 운영 중인지에 따라 조직에도 변화가 필요할 수 있다.

이는 네트워크가 이미 구축되어 있는 조직에서 실행할 수 있는 옵션이 아니다. 그러나, 조직이 자체적으로 인프라를 구축해야 하는 경우가 있을 수 있다. 이 경우, 제로 트러스트 개념을 어느 정도 도입하는 것이 가능할 수도 있다. 예를 들어, 기관에서 새로운 애플리케이션, 서비스 또는 데이터베이스를 구축해야 한다고 하자. 기관은 주체의 트러스트를 평가한 후 액세스를 허가하고, 신규 리소스 주위에 마이크로 페리미터micro-perimeter를 형성하는 등 제로 트러스트 원칙 및 시큐어 시스템 엔지니어링[SP800-160v1]에 필요한 새로운 인프라를 설계할 수 있다. 성공 여부는 이 새로운 인프라가 기존 리소스(예 : ID 관리 시스템)에 얼마나 의존하는지에 달려있다.

7.2. 하이브리드 아키텍처

주요 기업이 한 차례의 기술 교체 주기로 제로 트러스트로 전환할 수 있는 가능성은 낮다. 기업에서 제로 트러스트 아키텍처 워크플로우와 제로 트러스트 아키텍처가 아닌 워크플로우가 상존하는 시기는 명확히 규정할 수 없다. 한 번에 한 개의 비즈니스 프로세스가 제로 트러스트 아키텍처로 전환될 것이다. 기업은 공통 요소(예 : ID 관리, 디바이스 관리, 이벤트 로깅)에 대해 제로 트러스트 및 경계 기반 하이브리드 아키텍처에서 운영할 수 있을 정도의 충분한 유연성을 확보해야 한다. 기업은 제로 트러스트 아키텍처 솔루션 후보를 기존 컴포넌트와 인터페이스할 수 있는 것들로 제한할 수도 있다.

기존 워크플로우를 제로 트러스트 아키텍처로 전환할 때, 조금이나마 부분적인 재설계가 필요할 수 있다. 이런 상황은 기업에게 시큐어 시스템 엔지니어링[SP800-160v1] 사례를 채택할 기회가 될 수 있다.

7.3. 제로 트러스트 아키텍처 전환 단계

제로 트러스트 아키텍처로 전환하려면, 조직은 자신의 물리/가상 자산에 대한 상세한 지식을 가지고 있어야 한다. 정책 엔진은 리소스의 요청을 평가할 때 이 지식에 액세스한다. 지식이 완전하지 않으면, 정책 엔진은 정보가 충분하지 않기 때문에 요청을 거부하게 되고, 이는 비즈니스 프로세스 실패로 이어진다. 조직 내부에 인지하지 못한 “섀도우shadow IT”가 운영되고 있다면, 이는 특별한 이슈이다.

기업이 제로 트러스트 아키텍처 도입에 착수하기 전에, 자산/주체/데이터플로우/워크플로우를 조사해야 한다. 이는 제로 트러스트 아키텍처를 전개하기 전에 반드시 인지해야 하는 기초를 형성한다. 현 운영 상태에 대한 지식이 없다면, 기업은 어떤 신규 프로세스/시스템 필요한지 결정할 수 없다. 이런 조사는 병렬적으로 수행할 수 있다. 하지만, 모두 조직의 비즈니스 프로세스 조사와 연결된다. 제로 트러스트 아키텍처로 전환하는 단계를 위험 관리 프레임워크[SP800-37]의 단계와 매핑할 수 있다. 제로 트러스트 아키텍처를 채택하는 것이 기관의 비즈니스 기능에 대한 위험을 줄이기 위한 프로세스이기 때문이다. 제로 트러스트 아키텍처를 시행하기까지의 경로는 그림 12와 같이 도식화할 수 있다.

인벤토리 생성부터 유지보수 및 업데이트를 위한 정기적인 주기가 있다. 업데이트는 비즈니스 프로세스를 변경할 수도, 영향이 없을 수도 있다. 하지만, 비즈니스 프로세스에 대한 평가를 수행해야 한다. 예를 들어, 디지털 인증서 제공자를 변경하는 것은 중대한 영향이 없는 것으로 보일 수 있다. 하지만, 인증서 루트 스토어 관리, 인증서 투명성 로그 모니터링 등이 포함되어 있을 수 있다.

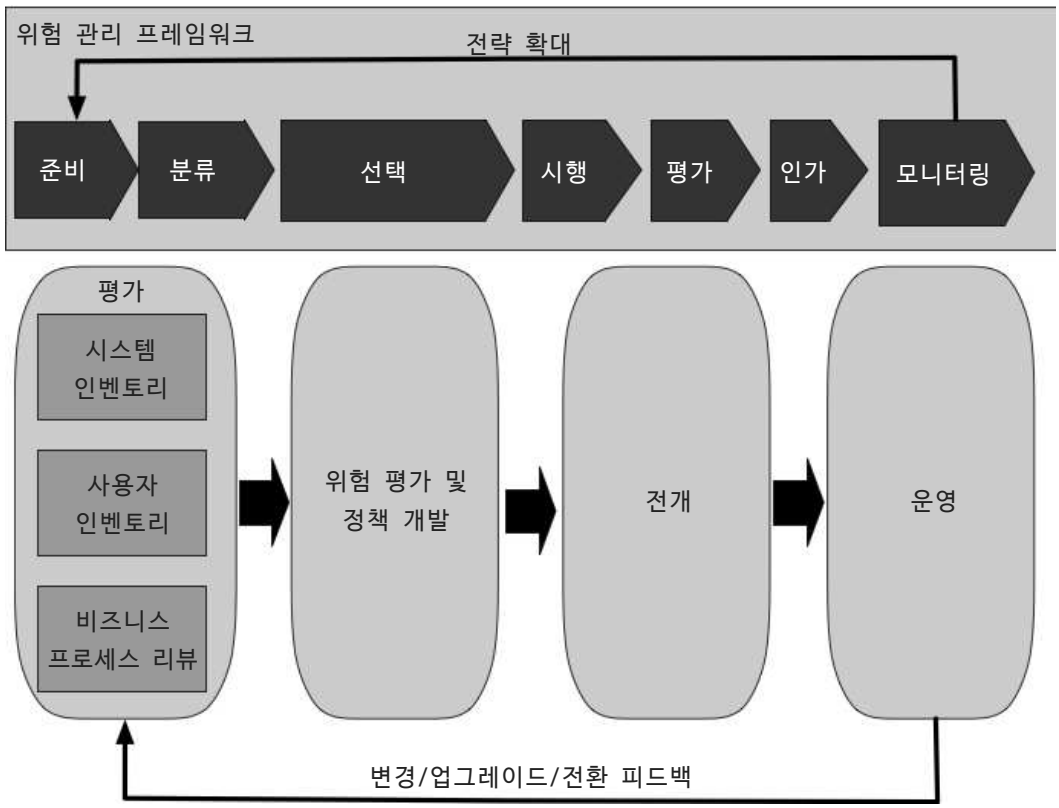

그림 12 : 제로 트러스트 아키텍처의 전개 사이클

7.3.1. 주체 식별

기업에서 제로 트러스트를 운영하려면, 정책 엔진은 기업 주체에 대한 지식을 갖춰야 한다. 주체는 사람과 NPE(리소스와 상호작용하는 서비스 계정 등)를 모두 아우른다.

개발자 및 시스템 관리자 등 특수 권한을 가진 사용자에게 속성/역할을 할당할 때는 추가적인 정밀 조사가 필요하다. 다수 레거시 보안 아키텍처에서 이러한 계정은 모든 기업 리소스에 액세스할 수 있는 포괄적인 퍼미션을 가질 수 있다. 제로 트러스트 아키텍처는 개발자 및 관리자가 자신들의 비즈니스 요구사항을 만족하도록 충분한 유연성을 허용해야 한다. 이와 동시에 로그 및 감사를 통해 액세스 패턴을 식별해야 한다. 제로 트러스트 아키텍처를 전개할 때, 관리자는 NIST 800-63A의 섹션 5[SP800-63A]에 명시되어 있는 더 높은 신뢰 수준/기준을 만족해야 한다.

7.3.2. 기업 소유 자산 식별

섹션 2.1에서 언급한 것처럼, 제로 트러스트 아키텍처의 핵심 요구사항 중 하나는 디바이스를 식별/관리하는 능력이다. 또한, 제로 트러스트 아키텍처는 기업이 소유한 네트워크 인프라에 연결되어 있거나 기업 리소스에 액세스하는 디바이스 중에서 기업 소유가 아닌 디바이스를 식별/모니터링하는 능력이 필요하다. 기업 자산을 관리하는 능력은 제로 트러스트 아키텍처 전개에 성공하기 위한 핵심이다. 기업 자산에는 하드웨어 컴포넌트(예: 노트북, 핸드폰, IoT 디바이스) 및 디지털 아티팩트(예 : 사용자 계정, 애플리케이션, 디지털 인증서)가 포함된다. 기업이 소유한 모든 자산을 완벽하게 조사하는 것이 불가능할 수도 있다. 따라서, 기업은 기업 소유 인프라에서 새롭게 발견된 자산을 빠르게 식별/구분/액세스하는 능력을 갖추는 것을 고려해야 한다.

이는 단순히 기업 자산 데이터베이스를 구분/관리하는 것 이외에, 설정 관리 및 모니터링도 포함된다. 자산의 현 상태를 관찰하는 능력은 액세스 요청을 평가하는 프로세스의 일부분이다.(섹션 2.1 참조) 이는 기업이 자산(가상 자산 및 컨테이너 등)을 설정/조사/업데이트할 수 있어야 한다는 것을 의미한다. 물리적 위치 및 네트워크 위치도 모두 포함된다. 이 정보는 정책 엔진이 리소스에 대한 액세스를 결정할 때 정책 엔진에게 전달되어야 한다.

또한, 기업 소유가 아닌 자산과 기업 소유의 “섀도우 IT”를 가능한 한 구분해야 한다. 이를 위해, 기업이 확인할 수 있는 것(예 : MAC 주소, 네트워크 위치)과 관리자가 추가로 입력한 것을 사용할 수 있다. 이 정보는 액세스 결정을 위해 사용될 뿐만 아니라, 모니터링 및 포렌식을 위해서도 사용된다. 섀도우 IT는 특수한 문제를 일으킨다. 섀도우 IT는 기업 소유지만, 관리되지 않기 때문이다. 특정 제로 트러스트 아키텍처 접근법, 주로 네트워크 기반 접근법에서 섀도우 IT 컴포넌트를 사용할 수 없을 수 있다. 섀도우 IT 컴포넌트는 인지되지 않았는데, 네트워크 액세스가 필요할 수 있기 때문이다.

많은 기관들이 이미 자신들의 자산을 식별하기 시작했다. 하드웨어 자산 관리[HWAM[1]] 및 소프트웨어 자산 관리[SWAM[2]],[SWAM]와 같은 CDM 프로그램의 기능을 도입한 기관은 제로 트러스트 아키텍처를 시행할 때 사용할 수 있는 풍부한 데이터 세트를 갖는다. 또한, 기관들은 미션을 달성하는데 핵심이라고 식별된 고高가치 자산[HVA[3]],[M-19-03]이 포함된 제로 트러스트 아키텍처의 후보 프로세스의 목록을 가지고 있을 수 있다. 이 작업은 기업 전체 또는 기관 전체에 대해 수행할 필요가 있다. 그 후에 해당 비즈니스 프로세스를 제로 트러스트 아키텍처로 설계할 수 있다. 이런 프로그램은 기업의 변화에 확장/적응할 수 있게 설계되어야 한다.

1 HWAM : Hardware Asset Management
2 SWAM : Software Asset Management
3 HVA : High Value Asset

7.3.3. 핵심 프로세스 식별 및 위험 평가

기관이 수행해야 하는 세 번째 인벤토리는 비즈니스 프로세스 및 데이터 플로우, 이들의 관계를 식별하고 순위를 매기는 것이다. 비즈니스 프로세스는 리소스에 대한 액세스 요청을 허가/거부하는 상황을 알려야 한다. 기업은 위험이 낮은 비즈니스 프로세스를 가장 먼저 제로 트러스트 아키텍처로 전환하고 싶을 수 있다. 장애가 발생하였을 때, 조직 전체에 좋지 않은 영향을 미칠 가능성이 낮기 때문이다. 충분한 경험이 쌓이면, 더 중요한 비즈니스 프로세스도 후보가 될 수 있다.

클라우드 기반 리소스를 사용하거나 원격 근무자가 사용하는 비즈니스 프로세스는 제로 트러스트 아키텍처를 적용하기에 적합한 경우가 많다. 이런 비즈니스 프로세스는 가용성 및 보안이 개선될 가능성이 있다. 기업 경계를 클라우드에 옮기거나 클라이언트가 VPN을 통해 기업 네트워크를 사용하는 것이 아니라, 기업의 클라이언트가 클라우드 서비스를 직접 요청할 수 있다. 기업의 정책 집행 포인트는 클라이언트에게 리소스에 대한 액세스를 허가하기 전에 클라이언트가 기업 정책을 따른다는 것을 보증한다. 또한, 제로 트러스트 아키텍처를 수립할 때, 성능, 사용자 경험, 워크플로우 취약점 증가 가능성 사이의 균형을 고려해야 한다.

7.3.4. 제로 트러스트 아키텍처 후보에 대한 정책 수립

후보 서비스/워크플로우는 몇 가지 요인으로 결정된다. 이 요인이란, 프로세스의 중요성, 영향을 받는 주체, 워크플로우에 사용되는 리소스의 현재 상태이다. NIST 위험 관리 프레임워크 [SP800-37]를 사용하면, 위험을 기반으로 자산/워크플로우의 가치를 평가할 수 있다.

자산/워크플로우를 식별한 후, 워크플로우가 사용하거나 영향을 주는 모든 업스트림 리소스(예 : ID 관리 시스템, 데이터베이스, 마이크로서비스), 다운스트림 리소스(예 : 로깅, 보안 모니터링), 엔티티(예 : 주체, 서비스 계정)를 식별해야 한다. 이는 제로 트러스트 아키텍처로 전환하기 위한 후보 선택에 가장 먼저 영향을 준다. 기업의 모든 주체에게 필수적인 애플리케이션/서비스(예 : 이메일)보다 기업의 일부 주체가 사용하는 애플리케이션/서비스(예 : 구매 시스템)를 후보로 선택할 것이다.

기업 관리자는 후보 비즈니스 프로세스가 사용하는 리소스에 대해 기준들을 결정(기준 기반 트러스트 알고리즘 사용 時)하거나, 중요도에 따른 가중치를 결정(점수 기반 트러스트 알고리즘 사용 時)해야 한다.(섹션 3.3.1 참조) 관리자는 튜닝 단계에서 이런 기준/가중치를 조정해야 할 수도 있다. 이러한 조정은 정책이 효과적이고, 리소스에 대한 액세스를 방해하지 않는다는 것을 보증하기 위해 필요하다.

7.3.5. 솔루션 후보 식별

비즈니스 프로세스 후보 목록이 작성되면, 기업 설계자는 솔루션 후보 목록을 작성할 수 있다. 특정 워크플로우 및 현재 기업 생태계에 더 적합한 배치 모델(섹션 3.1 참조)이 있다. 마찬가지로, 특정 유스 케이스에 더 적합한 솔루션이 있다. 여기에는 몇 가지 고려할 요인이 있다.

- 이 솔루션은 클라이언트에 컴포넌트를 설치해야 하는가? 이 솔루션은 기업 소유가 아닌 자산(BYOD 또는 기관 간 협업 등)을 사용하는 비즈니스 프로세스에 적용이 제한된다.

- 이 솔루션은 비즈니스 프로세스 리소스가 모두 온 프레미스인 경우에도 동작하는가? 일부 솔루션은 요청된 리소스가 클라우드(위-아래 트래픽)에 있고 기업 경계 내부(좌-우 트래픽)에 있지 않는다고 가정한다. 후보 비즈니스 프로세스의 리소스 위치는 제로 트러스트 아키텍처에도 후보 솔루션에도 영향을 줄 것이다.

- 이 솔루션은 분석을 위해 로그 상호작용에 대한 방법을 제공하는가? 제로 트러스트의 핵심 컴포넌트는 액세스 결정 시 정책 엔진으로 피드백되는 프로세스 플로우 관련 데이터를 수집하고 사용하는 것이다.

- 이 솔루션은 다양한 애플리케이션, 서비스, 프로토콜을 지원하는가? 프로토콜(웹, SSH 등) 및 전송(IPv4, IPv6)을 광범위하게 지원하는 솔루션도 있지만, 웹/이메일처럼 좁은 범위에서만 동작하는 솔루션도 있다.

- 이 솔루션은 주체의 행위에 변경이 필요한가? 일부 솔루션은 특정 워크플로우를 수행하려면, 추가적인 단계가 필요할 수 있다. 이는 기업 주체가 워크플로우를 수행하는 방법을 변화시킬 것이다.

한 가지 해결책은 기존 비즈니스 프로세스를 그저 교체만 하기보다 파일럿pilot 프로그램으로 만들어 보는 것이다. 이런 파일럿 프로그램은 다수 비즈니스 프로세스에 적용할 수 있도록 일반화할 수도, 한 가지 유스 케이스에만 구체화할 수 있다. 파일럿 프로그램은 제로 트러스트 아키텍처로 전환하기 위한 시험대로 사용될 수 있다.

7.3.6. 최초 전개 및 모니터링

후보 워크플로우 및 제로 트러스트 아키텍처 컴포넌트를 선택하면, 최초 전개를 시작할 수 있다. 기업 관리자는 선택된 컴포넌트를 사용하여, 수립한 정책을 시행해야 한다. 하지만, 처음에는 모니터링 모드로 운영하기를 원할 수 있다. 한 번의 반복으로 완료할 수 있는 정책은 거의 없다. 중요한 사용자 계정(예 : 관리자 계정)이 필요한 리소스에 대한 액세스가 거부되거나, 할당된 액세스 권한이 과도할 수 있기 때문이다.

새로운 제로 트러스트 비즈니스 워크플로우에 대해 정책이 효과적이고 운영 가능한지 확인할 때까지 레포팅만 수행하는 모드reporting-only mode로 운영할 수 있다. 이를 통해 기업은 자산/리소스에 대한 액세스 요청/행위/통신 패턴의 베이스라인을 인식할 수 있다. 보고만 수행한다는 것은 대부분의 요청에 대해 액세스를 허가하며, 접속 로그/트레이스를 최초 작성된 정책과 비교하는 것을 의미한다. 기본적인 정책(다중 인증에 실패하는 요청, 공격자가 침해한 것으로 알려진 IP 주소 거부 등)을 실행하고 로그를 기록해야 한다. 하지만, 최초 전개 이후에는 액세스 정책이 관대하게 적용하여, 제로 트러스트 워크플로우의 실제 상호작용으로부터 데이터를 수집해야 한다. 워크플로우에 대한 액티비티 패턴 베이스라인이 설정되면, 비정상 행위를 쉽게 식별할 수 있다. 관대하게 운영하는 것이 가능하지 않다면, 기업 네트워크 운영자는 로그를 주의 깊게 모니터링해야 한다. 그리고, 운영 경험을 기반으로 액세스 정책을 수정할 수 있도록 준비해야 한다.

7.3.7. 제로 트러스트 아키텍처 확대

충분한 자신감을 얻고, 워크플로우 정책을 개선하였다면, 기업은 정상적인 운영 단계에 돌입한다. 네트워크/자산을 지속적으로 모니터링하고, 트래픽을 로그에 기록한다.(섹션 2.1 참조) 그러나, 대응 및 정책 변경 속도를 늦추어, 심각한 상황에 빠지지 않도록 해야 한다. 또한, 주체 및 리소스/프로세스의 이해 관계자는 운영 개선을 위한 피드백을 제공해야 한다. 이 단계에서 기업 관리자는 제로 트러스트의 다음 전개를 계획할 수 있다. 최초 전개와 마찬가지로 워크플로우 및 솔루션 후보를 식별하고, 초기 정책을 작성할 필요가 있다.

그러나, 워크플로우에 변화가 생겼다면, 제로 트러스트 아키텍처 운영에 대한 재평가가 필요하다. 신규 디바이스, 소프트웨어(특히 제로 트러스트 논리 컴포넌트)의 중요 업데이트, 조직 구조의 이동과 같은 시스템의 중요한 변화는 워크플로우 또는 정책의 변화를 초래할 수 있다. 실제로 일부 작업이 이미 수행되었다고 가정하여, 전체 프로세스를 다시 검토해야 한다. 예를 들어, 신규 디바이스를 구매하였으나, 아직 신규 사용자 계정을 하나도 생성하지 않았다면, 디바이스 인벤토리만 업데이트하면 된다.

참고 문헌

[ACT-IAC] American Council for Technology and Industry Advisory Council (2019) Zero Trust Cybersecurity Current Trends. Available at https://www.actiac.org/zero-trust-cybersecurity-current-trends

[Anderson] Anderson B, McGrew D (2017) Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and NonStationarity. Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (ACM, Halifax, Nova Scotia, Canada), pp 1723-1732. https://doi.org/10.1145/3097983.3098163

[BCORE] Department of Defense CIO (2007). Department of Defense Global Information Grid Architecture Vision Version 1.0 June 2007. Available at http://www.acqnotes.com/Attachments/DoD%20GIG%20Architectural%20Vision,%20June%2007.pdf

[CSA-SDP] Cloud Security Alliance (2015) SDP Specification 1.0. Available at https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/

[FIPS199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems.(U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[Gilman] Gilman E, Barth D (2017) Zero Trust Networks: Building Secure Systems in Untrusted Networks (O'Reilly Media, Inc., Sebastopol, CA), 1st Ed.

[HWAM] Department of Homeland Security (2015) Hardware Asset Management(HWAM) Capability Description. Available at https://www.uscert.gov/sites/default/files/cdm_files/HWAM_CapabilityDescription.pdf

[IBNVN] Cohen R, Barabash K, Rochwerger B, Schour L, Crisan D, Birke R, Minkenberg C, Gusat M, Recio R, Jain V (2013) An Intent-based Approach for Network Virtualization. 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013). (IEEE, Ghent, Belgium), pp 42-50. Available at https://ieeexplore.ieee.org/document/6572968

[JERICHO] The Jericho Forum (2007) Jericho Forum Commandments, version 1.2. Available at https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf

[M-19-03] Office of Management and Budget (2018) Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program. (The White House, Washington, DC), OMB Memorandum M19-03,December 10, 2018. Available at https://www.whitehouse.gov/wpcontent/uploads/2018/12/M-19-03.pdf

[M-19-17] Office of Management and Budget (2019) Enabling Mission Delivery through Improved Identity, Credential, and Access Management. (The White House, Washington, DC), OMB Memorandum M-19-17, May 21, 2019. Available at https://www.whitehouse.gov/wpcontent/uploads/2019/05/M-19-17.pdf

[M-19-19] Office of Management and Budget (2019) Update on Data Center Optimization Initiative (DCOI). (The White House, Washington, DC), OMB Memorandum M-19-19, June 25, 2019. Available at https://datacenters.cio.gov/assets/files/m_19_19.pdf

[M-19-26] Office of Management and Budget (2019) Update to the Trusted Internet Connections (TIC) Initiative. (The White House, Washington, DC), OMB Memorandum M-19-26, September 12, 2019. Available at https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf

[NISTIR 7987] Ferraiolo DF, Gavrila S, Jansen W (2015) Policy Machine: Features, Architecture, and Specification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7987, Rev. 1. https://doi.org/10.6028/NIST.IR.7987r1

[NISTIR 8062] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062

[NISTPRIV] National Institute of Standards and Technology (2020) Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01162020

[SDNBOOK] Nadeau T, Gray K (2013) SDN: Software Defined Networks: An Authoritative Review of Network Programmability Technologies. (O'Reilly) 1st Ed.

[SP800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP800-63] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. NIST Special Publication (SP) 800-63-3, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[SP800-63A] Grassi PA, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Enrollment and Identity Proofing. NIST Special Publication (SP) 800-63A, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63A

[SP800-160v1] Ross R, McEvilley M, Oren JC (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[SP800-160v2] Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R (2019) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication (SP) 800-160, Vol. 2. https://doi.org/10.6028/NIST.SP.800-160v2

[SP800-162] Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication (SP) 800-162, Includes updates as of August 2, 2019. https://doi.org/10.6028/NIST.SP.800-162

[SWAM] Department of Homeland Security (2015) Software Asset Management (SWAM) Capability Description. Available at https://www.uscert.gov/sites/default/files/cdm_files/SWAM_CapabilityDescription.pdf

부록 A - 약어

API	Application Programming Interface
BYOD	Bring Your Own Device
CDM	Continuous Diagnostics and Mitigation
DHS	Department of Homeland Security
DoS	Denial of Service
G2B	Government to Business (private industry)
G2G	Government to Government
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
PA	Policy Administrator
PDP	Policy Decision Point
PE	Policy Engine
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
RMF	NIST Risk Management Framework
SDN	Software Defined Network
SDP	Software Defined Perimeter
SIEM	Security Information and Event Monitoring
TIC	Trusted Internet Connections
VPN	Virtual Private Network
ZT	Zero Trust
ZTA	Zero Trust Architecture

부록 B – 제로 트러스트 아키텍처와 현재 기술 사이의 간극

이 문서를 작성하기 위해 연구하면서, 제로 트러스트 컴포넌트 및 솔루션의 현재 성숙도를 조사하였다. 이 조사에서는 제로 트러스트 아키텍처 생태계의 현재 상태가 널리 채택하기에 충분히 성숙하지 못했다고 결론을 내렸다. 기업 환경에 제로 트러스트 아키텍처 전략을 수립하고 전개하는 것은 가능하지만, 필요한 모든 컴포넌트를 제공하는 단일 솔루션은 존재하지 않는다. 또한, 기업에 존재하는 다양한 워크플로우에 모두 사용할 수 있는 제로 트러스트 아키텍처 컴포넌트는 거의 없다.

제로 트러스트 아키텍처 생태계에서 식별된 간극 및 추가적인 연구가 필요한 영역을 아래에 요약하였다. 추가적인 연구가 필요한 영역의 경우, 제로 트러스트 아키텍처 원칙이 이런 영역을 어떻게 변경시키는지 잘 알려져 있지 않다. 다양한 제로 트러스트 아키텍처 기업 환경에서의 경험이 충분하지 않기 때문이다.

B.1. 기술 조사

다수 벤더가 초대되어, 제로 트러스트 관련 제품 및 관점을 발표했다. 이 조사의 목적은 제로 트러스트 기반 인프라로 전환을 방해하거나, 제로 트러스트 아키텍처가 유지되는 것을 방해하는 요인 중에서 놓친 부분을 식별하기 위한 것이었다. 이런 간극은 전개 임박(즉시 또는 단기), 유지보수 및 운영에 영향을 주는 시스템적 간극(중단기), 미지(향후 연구 영역)로 구분할 수 있다. 이를 표 B-1에 요약하였다.

구분	질의 예시	식별된 간극
전개 임박	• 조달 요구사항은 어떻게 작성해야 하는가? • 제로 트러스트 아키텍처는 TIC, FISMA 등의 요구사항과 어떻게 같이 시행하는가?	• 제로 트러스트 아키텍처에 대한 공통 프레임워크 및 용어 부재 • 제로 트러스트 아키텍처가 기존 정책과 상충된다는 인식
시스템적	• 벤더에 종속되는 것을 어떻게 방지할 수 있는가? • 다른 제로 트러스트 아키텍처 환경과 어떻게 상호작용하는가?	• 벤더 API에 대한 과도한 의존
추가 조사 필요 영역	• 제로 트러스트 아키텍처에서 위협은 어떻게 진화할 것인가? • 제로 트러스트 아키텍처는 비즈니스 프로세스를 어떻게 변화시킬 것인가?	• 제로 트러스트 아키텍처를 시행중인 기업에 대한 공격 성공 사례 • 제로 트러스트 아키텍처를 시행중인 기업에서 최종 사용자 경험을 문서화

표 B-1 : 식별된 전개 간극

B.2. 제로 트러스트 아키텍처로 즉시 전환을 방해하는 간극

현재 제로 트러스트 아키텍처의 채택을 늦추고 있는 이슈가 있다. 이러한 이슈를 당면 문제로 구분할 수 있다. 이 카테고리에서는 향후 유지보수를 고려하지 않았다. 진보적인 기업은 유지보수 카테고리를 제로 트러스트 아키텍처 컴포넌트의 최초 배치를 방해하는 당면 문제로 검토할 수도 있다. 하지만, 여기서는 이런 문제를 다른 카테고리로 생각한다.

B.2.1. 제로 트러스트 아키텍처 설계, 계획, 조달에 대한 공통 용어 부재

기업 인프라의 설계 및 배치를 위한 전략으로서의 제로 트러스트는 여전히 개념을 형성하고 있는 중이다. 업계는 아직까지 제로 트러스트 아키텍처 컴포넌트 및 운영을 설명하기 위한 용어나 개념을 통일하고 있지 않다. 이는 조직이 기업 인프라를 제로 트러스트로 설계하고 컴포넌트를 조달하기 위해 일관된 요구사항 및 정책을 작성하는 것을 어렵게 한다.

섹션 2.1 및 섹션 3.1은 제로 트러스트 아키텍처를 설명하는 용어 및 개념에 대한 중립적인 기반을 형성하기 위한 최초의 시도이다. 개념적인 제로 트러스트 아키텍처 컴포넌트 및 배치 모델은 제로 트러스트 아키텍처에 대한 기본적인 용어 및 방법으로 사용하기 위해 개발되었다. 이는 기업 요구사항 작성 및 시장 조사 시, 제로 트러스트 아키텍처 솔루션을 살펴보고, 모델링하고, 논의하기 위한 공통적인 방법을 제공하는 것을 목적으로 한다. 상기 섹션은 제로 트러스트 아키텍처에 대한 경험이 축적되면서 불완전함이 드러날 수 있다. 그러나, 현재로서는 공통의 개념적 프레임워크를 위한 기반으로 역할을 수행하고 있다.

B.2.2. 기존 사이버 보안 정책과 상충된다는 인식

제로 트러스트 아키텍처는 사이버 보안에 대한 기존 관점과 양립할 수 없는 솔루션들로 구성된 프레임워크라는 오해가 있다. 하지만, 제로 트러스트는 현재 사이버 보안 전략이 진화한 것으로 간주해야 한다. 다수의 개념과 아이디어가 오랫동안 유통되어 왔기 때문이다. 연방 기관들은 기존 지침(섹션 6 참조)를 통해 사이버 보안에 제로 트러스트 접근법을 더 많이 채택하도록 장려해 왔다. 기관이 성숙한 ID 관리 시스템과 견고한 CDM 기능을 갖고 있다면, 제로 트러스트 아키텍처의 길을 걷고 있다고 볼 수 있다.(섹션 7.3 참조) 이런 간극은 제로 트러스트 아키텍처에 대한 오해에 기반한다.

B.3. 제로 트러스트 아키텍처에 영향을 주는 시스템적 간극

이런 간극들은 제로 트러스트 아키텍처의 최초 시행/전개 및 지속적 운영/성숙도에 영향을 주는 것이다. 이런 간극은 기관에서 제로 트러스트 아키텍처의 채택을 늦추거나, 제로 트러스트

아키텍처 컴포넌트 업계의 단편화를 초래할 수 있다. 시스템적 간극은 표준 개발 기구SDO[1] 또는 업계 컨소시엄에서 작성한 개방 표준이 도움이 될 수 있는 영역이다.

B.3.3. 컴포넌트 間 인터페이스 표준화

기술 조사를 통해, 하나의 솔루션으로 제로 트러스트를 제공할 수 있는 벤더는 없다는 것이 명확해 졌다. 더욱이, 제로 트러스트를 달성하기 위해 한 벤더의 솔루션만을 사용하여 벤더에 종속되는 위험에 처하는 것은 바람직하지 않다. 이를 통해, 구매 시부터 지속적으로 컴포넌트 사이의 상호 운용을 유도한다.

기업 내부 컴포넌트의 스펙트럼은 매우 넓다. 많은 제품이 제로 트러스트의 한 가지 특정 분야에 초점을 맞추고 있으며, 데이터나 서비스를 제공하는 것은 다른 제품에 의존한다.(예 : 리소스 접근을 위한 다중 인증의 통합) 벤더는 이런 통합을 이루기 위해 표준화된 API보다 파트너社가 제공하는 독자적인 API에 의존하는 경우가 잦다. 이런 방식의 문제점은 API에 특허가 있고, API가 한 벤더에 의해 좌우된다는 것이다. 벤더가 API를 변경하면, 자신의 제품을 업데이트해야 한다. 따라서, 제품 사이의 호환성에 영향을 미칠 수 있는 API 변경을 조기에 통보하기 위해 벤더 커뮤니티 사이의 긴밀한 파트너쉽이 필요하다. 이는 벤더와 이용자에게 추가적인 부담을 지운다. 제품을 변경하려면, 벤더는 리소스를 소모해야 한다. 한 벤더가 자신의 독자적인 API를 변경하면, 고객은 다수 제품을 업데이트해야 한다. 추가적으로, 벤더는 호환성과 상호 운용성을 최대화하기 위해 각 파트너 컴포넌트를 위한 래퍼wrapper를 구현하고 관리해야 한다. 예를 들어, 많은 다중 인증 제품 벤더는 다른 종류의 클라이언트 조합에 사용할 수 있도록 클라우드 제공자 또는 아이덴티티 관리 시스템 별로 다른 래퍼를 제작해야 한다.

이는 이용자가 제품 구매를 위한 요구사항 작성 시, 추가적인 문제를 발생시킨다. 구매자가 제품 사이의 호환성을 확인하기 위해 사용할 수 있는 표준이 존재하지 않는다. 따라서, 제로 트러스트로 전환하기 위한 다년도 로드맵을 작성하기 어렵다. 컴포넌트 호환성과 관련된 최소한의 요구사항도 식별할 수 없기 때문이다.

B.3.4. 독자적 API에 대한 과도한 의존성 해결을 위한 신규 표준

제로 트러스트 아키텍처를 개발하기 위한 단일 솔루션은 존재하지 않기 때문에, 제로 트러스트 기업을 위한 단일 도구 세트 또는 단일 서비스 세트는 존재하지 않는다. 따라서, 기업이 단일 프로토콜 또는 단일 프레임워크로 제로 트러스트 아키텍처로 전환할 수 없다. 현재, 제로 트러스트 아키텍처에 대한 주도적인 권위를 갖기 위해 애쓰고 있는 다양한 모델 및 시스템이 있다.

1 SDO : Standards Development Organization

이는 제로 트러스트 아키텍처로 전환을 지원하는 개방적 표준 프로토콜 세트가 개발될 기회가 있다는 것을 의미한다. IETF[Internet Engineering Task Force]와 같은 표준 개발 기구는 XMPP-Grid[1]라 불리는 위협 정보 교환에 유용한 프로토콜을 가지고 있다. CSA[Cloud Security Alliance]는 소프트웨어 정의 경계[SDP[1],[2]]를 위한 프레임워크를 만들고 있으며, 이는 제로 트러스트 아키텍처에도 유용할 수 있다. 제로 트러스트 아키텍처와 관련된 프레임워크의 현상태 또는 제로 트러스트 아키텍처에 필요한 프로토콜을 조사하고, 규격을 만들고 개선할 필요가 있는 부분을 식별해야 한다.

B.4. 제로 트러스트 아키텍처에서 지식 격차 및 향후 연구 분야

여기에 나열된 격차들은 기관이 제로 트러스트 아키텍처를 채택하는 것을 방해하지 않는다. 이 격차들은 운영중인 제로 트러스트 아키텍처 환경에 대한 지식의 회색 지대이다. 대부분은 성숙한 제로 트러스트를 배치한 시간과 경험이 없다는 점에 기인하고 있다. 이 격차들은 향후 연구되어야 할 분야이다.

B.4.5. 제로 트러스트 아키텍처에 대한 공격자의 대응

적절하게 구현된 제로 트러스트 아키텍처는 전통적인 네트워크 경계 기반 보안보다 기업의 사이버 보안 상태를 개선할 것이다. 제로 트러스트 아키텍처 원리는 공격자에게 리소스가 노출되는 것을 줄이고, 자산이 침해되었을 때 내부 이동을 최소화하거나 막는 것을 목표로 한다.

그러나, 완강한 공격자들은 제로 트러스트 아키텍처와 마주했을 때 방관하지 않고 행위를 변경할 것이다. 해결되지 않은 이슈는 공격을 어떻게 변화시킬 것인가이다. 한 가지 가능성은 크리덴셜을 훔치던 공격이 다중 인증까지 확장되는 것을 생각할 수 있다.(예 : 피싱, 사회공학) 다른 가능성으로 하이브리드(제로 트러스트 아키텍처 + 경계 기반) 형태의 기업에서 공격자가 제로 트러스트 아키텍처 원리가 적용되지 않은, 즉, 전통적인 네트워크 경계 기반 보안을 따르는 비즈니스 프로세스에 집중하는 것을 생각할 수 있다. 이 경우, 실제로는 제로 트러스트 아키텍처가 적용된 비즈니스 프로세스에 대한 발판을 얻기 위한 시도로 손쉬운 대상을 목표로 하는 것이다. 제로 트러스트 아키텍처가 성숙함에 따라, 더 많이 전개되고, 경험을 얻고, 리소스의 공격 표면이 줄어드는 것에 제로 트러스트 아키텍처의 효과가 명확해질 것이다. 예전 사이버 보안 전략에 대비한 제로 트러스트 아키텍처 성공 지표도 개발할 필요가 있을 것이다.

1 SDP : Software Defined Perimeter

B.4.6. 제로 트러스트 아키텍처 환경에서의 사용자 경험

제로 트러스트 아키텍처를 사용하고 있는 기업에서 최종 사용자가 어떻게 행동하는지에 대해 철저한 조사는 이루어지지 않았다. 이는 분석을 할 수 있을 정도의 대규모 제로 트러스트 아키텍처 유스 케이스가 없다는 것이 주요 이유이다. 하지만, 제로 트러스트 아키텍처 기업에서 사용하는 다중 인증 및 다른 보안 운영과 사용자가 어떻게 반응하는지에 대해서는 지속적으로 연구해 왔다. 이런 연구는 제로 트러스트 아키텍처 워크플로우를 사용할 때, 최종 사용자 경험 및 행동을 예측하는 기초를 형성할 수 있다.

제로 트러스트 아키텍처가 최종 사용자 경험에 어떤 영향을 미칠 것인지를 예측할 수 있는 연구로 기업에서 다중 인증 사용과 보안 피로에 관한 것이 있다. 보안 피로[3]란, 최종 사용자가 많은 보안 정책 및 과제에 직면하여, 생산성에 부정적인 영향을 미치기 시작하는 현상이다. 다른 복수의 연구에서 다중 인증이 사용자 행동을 변화시킬 수 있음을 보였지만, 전체적인 변화는 엇갈린다.[4][5] 일부 사용자는 프로세스가 간소하고, 프로세스에 개인 소유의 디바이스가 포함(예 : 스마트폰 애플리케이션)되면 다중 인증을 쉽게 받아들인다. 하지만, 일부 사용자는 개인 소유의 디바이스를 비즈니스 프로세스에 사용해야 하는 것에 화를 내거나, IT 정책 위반 여부를 지속적으로 감시당한다고 느낀다.

B.4.7. 기업/네트워크 장애에 대한 제로 트러스트 아키텍처의 회복력

제로 트러스트 아키텍처 벤더 생태계 조사에서 제로 트러스트 아키텍처를 도입하는 기업이 검토할 필요가 있는 폭넓은 범위의 인프라를 보였다. 앞서 기술한 것처럼, 현재 완전한 제로 트러스트 솔루션을 단독으로 제공하는 벤더는 존재하지 않는다. 결과적으로 기업은 다수의 다른 서비스와 제품을 구매할 것이고, 이는 컴포넌트 사이의 의존성을 복잡하게 만들 수 있다. 중요한 컴포넌트에 장애가 발생하거나 연결되지 않으면, 하나 이상의 비즈니스 프로세스에 영향을 미치는 장애가 연쇄적으로 발생할 수 있다.

조사한 대부분의 제품 및 서비스는 강인함을 제공하기 위해 클라우드에 의존한다. 하지만, 클라우드 서비스도 공격이나 단순 에러로 연결되지 않을 수 있다. 이런 일이 일어나면, 액세스 결정에 사용되는 핵심 컴포넌트에 연결할 수 없거나, 다른 컴포넌트와 통신할 수 없다. 예를 들어, 클라우드에 위치한 정책 엔진 및 정책 관리자 컴포넌트는 DDoS 공격 중에도 연결할 수 있지만, 리소스에 위치한 모든 정책 집행 포인트에는 연결할 수 없을 수 있다. 제로 트러스트 아키텍처 배치 모델에서 초크 포인트가 될 수 있는 지점을 찾아내는 연구가 필요하다. 또한, 제로 트러스트 아키텍처 컴포넌트에 연결할 수 없거나 연결이 제한될 때, 네트워크 운영에 어떠한 영향을 주는 지에 대한 연구도 필요하다.

제로 트러스트 아키텍처를 채택한 경우, 기능 연속성COOP[1] 계획을 재검토해야 할 필요가 있다. 제로 트러스트 아키텍처는 많은 기능 연속성 요소를 사용하기 편리하게 해준다. 원격 근무자들도 온 프레미스 리소스에 대해 동일한 액세스를 갖기 때문이다. 하지만, 다중 인증 등의 정책은 사용자가 적절하게 훈련되지 못하고 경험이 부족하다면 부정적인 영향을 미칠 수 있다. 긴급 상황에서 사용자는 토큰과 기업 디바이스에 대한 액세스를 잊거나 가지고 있지 않을 수도 있다. 이런 상황은 기업 비즈니스 프로세스의 속도 및 유효성에 영향을 미칠 것이다.

B.5. 참고 문헌

[1] Cam-Winget N (ed.), Appala S, Pope S, Saint-Andre P (2019) Using Extensible Messaging and Presence Protocol (XMPP) for Security Information Exchange. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 8600. https://doi.org/10.17487/RFC8600

[2] Software Defined Perimeter Working Group “SDP Specification 1.0” Cloud Security Alliance. April 2014.

[3] Stanton B, Theofanos MF, Spickard Prettyman S, Furman S (2016) Security Fatigue. IT Professional 18(5):26-32. https://doi.org/10.1109/MITP.2016.84

[4] Strouble D, Shechtman GM, Alsop AS (2009) Productivity and Usability Effects of Using a Two-Factor Security System. SAIS 2009 Proceedings (AIS, Charleston, SC), p 37. Available at http://aisel.aisnet.org/sais2009/37

[5] Weidman J, Grossklags J (2017) I Like It but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017) (ACM, Orlando, FL), pp 212-224. https://doi.org/10.1145/3134600.3134629

1 COOP : Continuity of Operation