제로 트러스트 적용 전략에 관한 연구

이대성

부산가톨릭대학교

A Study on Strategies for Applying Zero Trust

Daesung Lee

Catholic University of Pusan

E-mail : dslee@cup.ac.kr

요 약

최근 네트워크 확장 및 클라우드 인프라 확장, 재택근무로 인한 원격접속의 증가로 외부의 접근뿐만이 아니라 내부에서의 접근을 경계해야 할 필요성이 증가하고 있다. 이로 인해 제로 트러스트라는 새로운 네트워크 보안 모델이 주목받고 있다. 본 논문에서는 제로 트러스트의 개념을 간단히 소개하고 다양한 기업환경에 따른 제로 트러스트 적용 전략에 대해 살펴보고자 한다.

ABSTRACT

With the recent increase in remote access due to network expansion, cloud infrastructure expansion, and telecommuting, the need to be vigilant not only from external access but also from internal access is increasing. Because of this, a new network security model called zero trust is attracting attention. In this paper, we will briefly introduce the concept of zero trust and examine strategies for applying zero trust according to various business environments.

키워드

Zero Trust, Network Security, Architecture, Security Strategies

Ⅰ. 서 론

제로 트러스트는 신뢰할 수 있는 네트워크는 존재하지 않는다는 핵심원칙을 가지고 있으며 모든 네트워크 트랜잭션이 이루어지려면 먼저 인증을 받아야 하며 인증되고 권한이 부여된 사용자와 장치만을 애플리케이션 및 데이터에 접속을 허용한다[1]. 클라우드 인프라가 확대되면서 애플리케이션의 위치에 상관없이 내부 및 외부 관계자들은 언제든지 접속해 필요한 작업을 진행할 수 있게 되었다. 또한, 최근 코로나로 인해 재택근무 등의 원격접속이 새로운 근무 형태로 자리 잡고 있다. 제로 트러스트의 개념은 모든 기업 환경에 적용하여 설계할 수 있다. 특히 제로 트러스트 아키텍처는 지역적으로 분산된 기업이나 업무 이동성이 높은 직원들을 많이 보유한 기업들이 상대적으로 높은 편익을 얻을 수 있다. 본 논문에서는 제로 트러스트의 개념을 적용할 수 있는 여러 기업 환경을 살펴보고 그에 따른 적용 전략을 살펴보고자 한다[2].

Ⅱ. 제로 트러스트 적용 전략

1. 그룹 기업

본사의 네트워크와 분산되어있는 지사가 물리적으로 연결되지 않은 환경의 경우, 지사의 직원들이 업무를 위해 기업 리소스에 접근하는 경우가 자주 발생한다. 이 때문에 지사와 본사의 네트워크를 연결하기 위해서 다중 프로토콜 레이블 스위치(MPLS)를 활용하기도 하지만, 이는 모든 트래픽을 수용하기에는 대역폭이 부족하다. 또한, 직원들이 기업 소유의 디바이스나 개인 소유의 디바이스를 이용하여 집 또는 지점에서 근무할 경우, 일정표나 이메일 같은 일부 리소스에만 액세스가 가능하고, 민감한 데이터베이스에 대해서는 액세스가 제한되

거나 거부될 수 있다. 이러한 경우, 정책 엔진 및 정책 관리자를 기업 네트워크에 직접 호스팅 하면 모든 트래픽을 로컬 네트워크로 재전송해야 하므로 응답률 손실이 생기므로, 정책 엔진 및 정책 관리자를 클라우드 서비스에 호스팅 하고, 기업 자산에 에이전트를 설치하거나 리소스 포털에 액세스한다.

2. 멀티 클라우드 및 C2C(Cloud-to-Cloud)를 이용하는 기업

다수의 클라우드 서비스 제공자를 사용하는 기업의 경우 로컬 네트워크를 소유하고 있지만, 두 개 이상의 클라우드 서비스 제공자를 사용하여 애플리케이션, 서비스 및 데이터를 호스팅 한다. 멀티 클라우드 사용자 환경에서는 많은 애플리케이션이나 서비스가 클라우드에 호스팅 되기 때문에 기업의 보안 부담이 커질 수밖에 없다. 하지만 제로 트러스트 개념을 구현한다면 기업이 소유한 네트워크 환경과 다른 서비스 제공자의 네트워크 환경의 차이를 없앨 수 있다고 본다. 멀티 클라우드 사용과 관련하여, 제로 트러스트는 '애플리케이션이나 서비스 및 데이터 소스의 액세스 포인트에 어떻게 정책집행 포인트를 설치할 것인가'로 접근한다. 정책 엔진과 정책 관리자는 멀티 클라우드 중 어떤 클라우드에도 호스팅 될 수 있으며 다른 서비스 제공자의 클라우드에도 호스팅 될 수 있다. 클라이언트는 포털이나 에이전트가 설치된 로컬 시스템을 통해 정책집행 포인트에 직접 액세스한다. 이러한 방법으로 기업은 외부에 호스팅 된 리소스에 액세스와 관리를 할 수 있다. 하지만 한가지 문제점이 있는데 클라우드 제공자별로 같은 기능을 서로 다른 방법으로 실행한다는 것이다. 그러므로 기업은 클라우드 서비스 제공자가 기업의 제로 트러스트 아키텍처를 어떻게 시행하는지 확인해야만 한다.

3. 외부 협력업체 직원의 액세스가 필요한 기업

Supply Chain을 형성하고 있는 기업들은 업무상 협력업체나 현장 방문 직원들에게 기업 리소스에 제한된 액세스를 허용해야 한다. 이러한 리소스에는 내부 애플리케이션, 서비스, 데이터베이스 등이 있다. 또한, 기업의 유지보수 및 난방, 조명 시스템 등의 보수 작업을 위해서 외부 업체에 네트워크 접속을 허용해야 할 때도 있다. 이를 위해서 제로 트러스트 기업은 리소스에 접속을 차단하면서, 방문 서비스 기술자나 관련 디바이스가 인터넷망에 액세스할 수 있도록 허가해야 한다[3]. 또한, 직원과 외부 인력이 접견실에 있는 경우, 제로 트러스트 아키텍처를 실행하여 접견실의 직원과 외부 인력을 구분하고, 직원은 필요한 기업 리소스에 액세스할 수 있지만, 외부 인력은 인터넷에만 액세스할 수 있고 기업 리소스에는 액세스할 수 없게 한다. 즉, 정책 엔진과 정책 관리자를 클라우드 서비스 또는 LAN에 호스팅하여 네트워크 정보수집 및 내부 이동을 차단한다.

4. 기업 간 협업

기업 간 협업 환경하에서는 두 기업의 직원이 같은 네트워크 인프라 스트럭쳐에 위치하지 않을 수 있고, 직원들이 액세스하는 리소스가 기업 내부 또는 클라우드에 호스팅 될 수 있다는 점에서는 그룹 기업 환경과 유사하다고 볼 수 있다. 기업과 기업이 서로 협력이 있는 환경의 경우에 다른 기업의 직원이 협업 기업의 데이터에 액세스할 수 있어야 한다. 그래서 협업 기업은 외부 기업의 직원을 위해 특별 계정을 설정하여, 필요한 데이터에 대해서만 액세스를 허가하는 계정을 제공한다. 하지만 이러한 방법은 협업 기업이 정부 기관이나 공공기관일 경우 계정관리에 더 많은 어려움이 발생할 수 있다. 이 경우, 연합 ID 관리 시스템에 두 기업을 등록하면, 두 기업의 정책집행 포인트는 연합 ID 관리 시스템에서 주체를 인증할 수 있기에 빠르게 관계를 정의할 수 있다. 또한, 정책 엔진과 정책 관리자를 클라우드 서비스에 호스팅 하면, VPN 등을 이용하지 않아도 모든 관계자가 사용할 수 있다. 그리고 협력 기업의 직원은 디바이스에 소프트웨어 에이전트를 설치하거나, 웹 게이트웨이를 통해 데이터 리소스에 액세스할 수 있다.

5. 공개 서비스 또는 고객 서비스 제공 기업

공개 서비스는 많은 기업이 공통으로 제공하는 기능으로 사용자가 로그인 인증정보를 작성하고, 사용자에게 로그인 인증을 발행함으로써 사용하거나, 이를 생략하여 사용할 수도 있다. 액세스를 위해 로그인 인증정보를 요구하지 않는 공개 리소스에 대해서는 제로 트러스트 아키텍처의 원리를 직접 적용하지 않는다. 기업은 고객이나 특수한 사용자와 같은 등록된 사용자를 위한 정책을 설정할 수 있다. 예를 들어, 사용자가 로그인 인증정보를 생성할 때 기업은 패스워드의 길이, 인증 기간 및 기타 세부적인 사항에 대해 정책을 수립할 수 있지만, 기업이 이러한 유형의 사용자를 위해 구현할 수 있는 정책에는 한계가 있다. 또한, 이러한 과정은 정상적인 사용자를 가장한 공격을 탐지하는 데 도움을 줄 수도 있다. 예시로, 등록된 고객이 공개된 웹 브라우저 중 하나를 이용하여 사용자 포털에 액세스하는 것을 알고 있는 경우, 한 브라우저에서 액세스 요청이 갑자기 증가할 경우 자동화 공격으로 의심할 수 있으므로 기업은 식별된 클라이언트의 요청을 제한하는 조치를 할 수 있다. 다만, 기업은 사용자 및 자산에 대해 어떤 정보를 수집하고 기록할 수 있는지에 관련된 법령과 규제사항에 유의해야 한다.

III. 결 론

본 논문에서는 제로 트로스트라는 개념을 소개하고, 이를 기업환경에 적용하기 위한 전략에 대해 살펴 보았다. 제로 트러스트는 모든 접근을 의심하는 핵심원칙 하에서 엄격한 보안이 요구되기 때문에 앞으로의 네트워크 보안 측면에서 큰 역할을 담당할 것으로 사료된다.

References

[1] What is Zero Trust? [Internet]. Available: https://www.vmware.com/kr/topics/glossary/content/zero-trust.html

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

[3] Seo-Young Kim, Kyung-Hwa Jeong, Yuna Hwang, Dae-Hun Nyang, Abnormal Behavior Detection for Zero Trust Security Model Using Deep Learning, Korea Information Processing Society Collection of academic papers, 28(1): 132-135, 2021