제로트러스트 기반의 안전한 보안 모델 설계

서정우, 홍성원
ICT폴리텍대학
jwseo@ict.ac.kr, 230531@ict.ac.kr

Designing a secure security model based on Zero Trust

Seo Jung Woo, Hong Sung Won
ICT Ploytech Institute of Korea Univ.

요 약

디지털전환과 사이버보안은 상호 균형을 이루면서 발전하고 있으며, 디지털전환이 심화하면서 사이버보안 역시 이에 맞춰 진화를 거듭하고 있다. 모바일, 사물인터넷 및 클라우드 기반으로 네트워크 환경이 변화하면서 기존 경계 기반 보안모델의 한계 상황이 초래되었고, 모든 접근 요구를 정확하게 제어하여 최소권한을 부여할 수 있는 새로운 보안체계로 전환이 요구되고 있다. 제로트러스트는 기존 보안모델의 한계를 보완하기 위한 개념으로 사이버 공격을 효과적으로 대응하기 위한 방법으로 소개되었다. 본 논문에서는 제로트러스트 기반의 안전한 보안 모델 설계를 위한 필요성과 방법론에 대해서 소개하고, 기존 경계 보안의 한계점을 극복하기 위한 대응 방법을 설명한다.

Ⅰ. 서 론

기업의 제어 영역 외부의 모든 사람은 악의적이고 내부의 모든 사람은 정직하고 선의의 사람이라는 네트워크 경계 개념은 오늘날의 비즈니스 환경에서는 더는 신뢰할 수 없는 개념이 되었다. SaaS(Software as a Service) 애플리케이션의 광범위한 채택, 클라우드 기반 아키텍처로의 마이그레이션, 원격 사용자의 증가, BYOD(Bring Your Own Device)의 유입으로 인해 경계 기반 보안은 더 이상 무의해지고 있다[1].

경계 중심 방어는 어플라이언스 및 보안 정책 관리와 빈번한 소프트웨어 업그레이드가 필요하기 때문에 운영 복잡성을 야기하고 과중한 업무에 시달리는 IT 팀에게 부담이 발생한다. 공격 표면이 확장되고 IT 리소스가 점점 복잡해지는 네트워크 아키텍처를 관리하기 위해 노력하는 가운데 사이버 공격자들은 더욱 능숙하고 정교하게 보안 조치를 회피하고 있다.

그림 1 제로트러스트 액세스[2]

제로트러스트 보안 모델은 기업망 내부에 언제나 공격자가 존재할 수 있으며, 기존 통신망에서의 신뢰성이 더는 유효하지 않기 때문에 기업 내 자산에 접근하는 모든 주체에 대해 지속해서 인증하고, 자신에 대한 위험성을 지속해서 평가하여 보안 위험으로 완화 시킬 수 있는 대책을 포함한다. 본 논문에서는 제로트러스트 아키텍처를 기반으로 안전한 업무 환경을 설계하기 위한 방법론 설명을 위해 2장에서는 제로트러스트 전환 요구에 관해 설명하고, 3장에서는 제로트러스트 아키텍처를 소개하고, 3장에서는 결론에 관해 서술한다.

Ⅱ. 제로트러스트 전환 요구

제로트러스트 모델은 경계 중심의 보안 아키텍처를 대체하며, 신원, 디비아스, 사용자 컨텍스트에 따라 보안 및 액세스 결정이 동적으로 적용되는 것을 보장한다. 또한, 제로트러스트 보안 프레임워크는 인증되고 권한이 부여된 사용자와 디바이스만 애플리케이션과 데이터에 액세스할 수 있도록 규정하며, 인터넷의 지능형 위협으로부터 사용자와 애플리케이션들을 보호한다[1,2].

A. 네트워크 액세스가 아닌 애플리케이션 기반 액세스 제공

가상사설망(VPN)과 같은 기존의 원격 접속 기술은 경계가 없어지는 디지털 비즈니스 환경의 요구를 만족하기 어려우며, 사용자 인증 후에는 자유로운 네트워크 액세스를 제공하기 때문에 보안 위협이 존재한다. 공격자는 내부로 침투하면 네트워크 내 모든 시스템이나 애플리케이션에 자유롭게 접속하여 활동할 수 있다. 네트워크 세분화가 보안 강화를 위한 대응 방법일 수 있지만, 비용이 많이 들고 구현하기 어려우며 동일한 서브넷에서 수평적 확산을 막지 못하는 위험이 존재한다.

비즈니스를 보호하고 제로트러스트를 활성화하려면 사용자에게 필요한 애플리케이션에만 액세스 권한을 부여하여, 측면 공격을 줄여 네트워크 노출을 제한한다. 제로트러스트 환경에서 보안 시스템의 의존도를 벗어나서 IT 유지 관리 비용을 절감할 수 있고, 애플리케이션에 누가 액세스하고 있으며 데이터가 어디로 흘러가는지 어떻게 액세스하는지에 대한 가시성과 인사이트를 제공할 수 있다.

B. 공용 인터넷 환경에서 네트워크 인프라스트럭처 고립

내부 애플리케이션과 액세스 인프라가 인터넷에 노출되면 DDoS, SQL 인젝션 및 기타 애플리케이션 계층 공격에 취약하다. 사이버 범죄자들은 끊임없이 진화하는 기술을 사용하여 네트워크 구성을 스캔하고 취약한 애플리케이션과 중요 데이터를 검색한다.

따라서, 애플리케이션과 접속 아키텍처를 공용 인터넷으로부터 격리하여

사이버 범죄자가 네트워크를 찾지 못하도록 하고, 실행 중인 애플리케이션과 서비스를 확인할 수 없도록 하여 공격자의 표적이 되지 않도록 해야 한다.

C. 애플리케이션 보호를 위한 웹 방화벽 한계 극복

최신 사이버 공격은 소셜 엔지니어링을 활용하여 특정 사용자를 대상으로 표적 공격을 시도한다. 사용자의 디바이스가 감염되면 좀비 디바이스로 활용되어 경계 방화벽 뒤에서 안전하다고 여겨지는 애플리케이션에 대한 공격을 실행한다. 대부분의 조직은 SQL 인젝션, 악성파일 실행, 크로스 사이트 요청 위조(CSRF) 등과 같이 애플리케이션 계층에서 발생하는 공격을 방어하기 위해 웹 애플리케이션 방화벽을 사용하지만, 내부의 애플리케이션을 보호하기 위해 확장하지는 않는다.

D. 신원 확인, 인증 및 권한 부여

애플리케이션의 액세스는 사용자의 신원을 확인하지 않고, 올바른 비밀번호를 입력하는 모든 사용자에게 접속을 허용하며, 이러한 취약한 자격 증명과 비밀번호 재사용은 공격 범위와 위험을 크게 증가시키는 요인이다. 오늘날의 위협 환경에서는 사용자 이름과 비밀번호와 같은 단일 인증만으로는 충분하지 않으며, 멀티팩터인증(MFA)은 추가적인 수준의 인증 및 보안을 제공하여 검증된 사용자만 애플리케이션에 액세스할 수 있도록 보장한다. MFA를 통해 사용자 인증 및 권한이 부여되면 하나의 자격 증명으로 모든 애플리케이션에 로그인할 수 있으며, 생산성을 향상할 수 있다.

E. 인터넷 연결 트래픽 및 활동 모니터링

제로트러스트 핵심 원칙은 네트워크 환경은 적대적으로 위험에 노출되어 있어 모든 활동을 허용하는 것이 아니라 모니터링하고 확인하여야 한다. 네트워크에서 일어나는 일에 대한 가시성 확보를 위해 충분한 트래픽과 인텔리전스를 요구한다.

네트워크 내·외부의 모든 디바이스(모바일, PC, IoT 등)에서 발생하는 모든 요청을 모니터링하고 확인하여 악의적이거나 허용되지 않는 사이트로 이동하지 않도록 해야 한다. 의심스러운 활동의 징후가 있는지 트래픽을 검사하고, C&C 서버와 통신 또는 데이터 유출과 같은 이상징후가 있는지 검사하여야 한다.

F. 보안 정보 및 이벤트 관리 통합 지원

기업에는 수백, 수천개의 애플리케이션을 가지고 있으며 API를 통해 애플리케이션을 배포하고 액세스를 위한 정책 통제를 설정한다. 추가 조사 및 상관관계 분석을 위해 위협 및 이벤트 데이터를 통합하여 문제를 해결한다.

Ⅲ. 제로트러스트 아키텍처

A. 인증 및 정책

전통적으로 경계 내부에서 시작되는 모든 네트워크 연결은 신뢰할 수 있는 것으로 판단하지만, 로컬 네트워크의 모든 연결을 허용하기 전에 적절한 인증을 수행한다. 강력한 제로트러스트 아키텍처를 구축하기 위해서는 보호할 모든 자원과 트래픽의 보안 수준을 정의해야 한다.

B. 정책 기반 액세스

제로트러스트에서는 네트워크 위치에 기반한 묵시적 신뢰는 더는 인증 조건이 아니며, ID 기반 인증을 사용하여 신뢰를 구축하고 정보 자원에 대한 액세스를 제공한다. 정책은 사용자, 데이터, 자산, 애플리케이션 및 서비스에 할당되며 최소한 권한 원칙을 적용하여 접근을 제한한다.

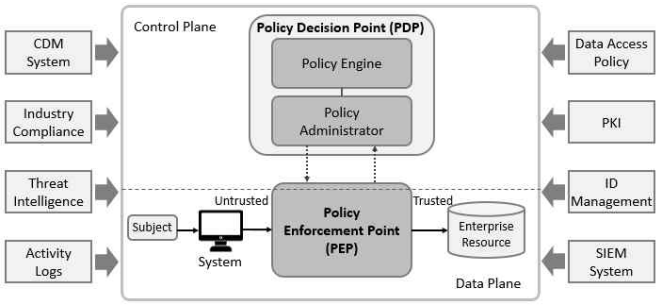

그림 2 제로트러스트의 논리적 구성[2]

C. 최소 권한 원칙

제로트러스트 환경에서는 액세스 및 보안 관리에서 최소 권한 원칙을 적용하여야 하며, 특정 작업을 완료할 수 있을 만큼의 액세스 권한을 부여해야 한다.

D. 디바이스 관리 및 서비스 모니터링

제로트러스트 전략의 필수적인 부분은 디바이스와 서비스의 상호 작동 방식, 요청되는 내용, 액세스 활동, 액세스 데이터를 지속해서 모니터링하고 기록한다. 신뢰할 수 있는 디바이스만 네트워크 사용을 허용하려면 각 디바이스에 고유 ID를 설정하는 것이 필요하며 ID는 네트워크에 대한 가시성을 제공하고 정책에 따라 권한 및 액세스를 인증한다.

E. 네트워크 세분화

제로트러스트 아키텍처를 구현할 때 사용할 수 있는 접근 방법의 하나이며 경계영역 내부에서 측면으로 이동하는 것을 방지한다. 마이크로 세그먼트는 각 워크로드 레벨로 논리적인 보안 세그먼트를 구성하여 계층화된 보안을 제공한다.

F. 소프트웨어 정의 경계(SDP, Software Defined Perimeter)

액세스 요청에 대한 세분화된 최소 권한 액세스 제어를 제공하며, 가상사설망에 대한 대안으로 안전한 원격 액세스를 제공한다. 소프트웨어를 기반으로 제로트러스트 정책과 사용자 ID, 최소 권한 기준으로 액세스를 부여하여 공격 표면을 줄일 수 있다.

Ⅳ. 결론

제로트러스트 모델의 적용은 보안을 유지하면서 비즈니스를 성공적으로 발전시켜 혁신과 민첩성을 확보할 수 있다. 제로트러스트 모델을 적용함으로써 애플리케이션(SaaS, 온프레미스, IaaS)에 대한 진화된 위협 방지, 애플리케이션 가속화, 다중요소인증 등의 이점을 제공한다. 그리고, 제러트러스트 모델은 API를 통한 오케스트레이션과 SIEM 및 워크플로 자동화 플랫폼과 통합하여 사용자와 애플리케이션에 대한 가시성을 제공하는 동시에 사용자와 애플리케이션에 대한 인사이트를 제공할 수 있다.

참 고 문 헌

[1] Akamai, "Zero Trust Security Transformation," June 2023.

[2] KISA, "Zero Trust Guideline," June 2023.

[3] Cyber Centre for Cyber Serutiy, “A zero trust approach to security architecture,” ITSM.10.008, March 2023.