제로 트러스트 구축 프로세스에 관한 연구

이대성

부산가톨릭대학교

A Study on Zero Trust Building Process

Daesung Lee

Catholic University of Pusan

E-mail : dslee@cup.ac.kr

요 약

현재 대부분 기업은 웹 서비스, 클라우드 시스템, 데이터센터용으로 방화벽이나 WAF(Web Application Firewall) 등의 보안 솔루션을 갖추고 있다. 최근 원격접속의 필요가 높아지면서 원격접속 제어의 보안 취약점을 극복해야 하는 과제가 중요시되고 있다. 본 논문에서는 제로 트러스트 관점의 네트워크 보안 모델에 대한 개념과 이를 활용한 전략 및 보안체계에 대해 살펴보고자 한다.

ABSTRACT

Currently, most companies have security solutions such as firewalls or WAF (Web Application Firewall) for web services, cloud systems, and data centers. Recently, as the need for remote access increases, the task of overcoming the security vulnerabilities of remote access control is becoming more important. In this paper, the concept of the network security model from the perspective of zero trust and the strategy and security system using it will be reviewed.

키워드

Zero Trust Architecture, Network Security, Building Process, 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]. 지금까지의 보안체계는 경계형 보안을 기본으로 다계층 보안체계로 구성되어 있었다. 또한, 일하는 장소와 장비의 다양화, 클라우드 시스템의 활용, 보안 위협의 분산화 등이 보안 대책의 과제로 제시되고 있다. 때문에, 대부분의 기업은 많은 시간을 제로 트러스트와 경계 기반의 보안 개념을 병행하면서, 제로 트러스트 기반으로 전환하기 위해 프로세스의 변화, 기술 솔루션의 도입 등으로 상당한 비용 투자가 이루어질 것으로 보고 있다. 본 논문에서는 제로 트러스트 기반 보안체계 구축을 위한 여러 프로세스를 소개한다.

Ⅱ. 제로 트러스트 기반 보안체계 구축 프로세스

1. 주체의 식별

식별하려는 주체에는 사람과 사물이 모두 포함되며, 개발자나 시스템 관리자 등 특수 권한을 가진 사용자에게 속성이나 역할을 부여할 때는 그들이 비즈니스 요구사항을 만족하게 할 수 있도록 충분한 유연성을 허용해야 한다. 또한, 로그 및 감사를 통해 액세스 패턴을 식별할 수 있어야 한다. 하지만, 최근에는 단말 로그, 네트워크의 로그, 인증 로그, IaaS (Infrastructure as a Service)나 SaaS(Software as a Service) 로그 등 확인해야만 하는 로그가 광범위해지고 있고 또한 사내 네트워크나 외부의 단말, 클라우드 시스템 등 로그를 확인해야만 하는 범위도 넓어지고 있다[2, 3]. 관련 솔루션중 하나로 SIEM(Security Information & Event Management) 가 있다. SIEM 은 크게 4가지 기능으로 데이터 통합, 탐지, 조사, 대응으로

나타낼 수 있다. 이러한 기능을 이용하여 각종 로그를 집적하여 로그를 해독하는데 특화돼 있으므로 제로 트러스트를 기반으로 한 보안 운용 및 감시를 보다 효율적으로 실시할 수 있게 해준다[4].

2. 기업 소유 자산의 식별

제로 트러스트 아키텍처의 핵심 요구사항 중 하나는 디바이스 식별 및 관리 능력이다. 따라서 기업 네트워크에 연결되어 있거나 기업 리소스에 액세스하는 디바이스 중, 기업 소유가 아닌 디바이스를 식별하고 모니터링하는 능력을 갖춰야 한다. 기업 자신은 노트북, 핸드폰과 같은 하드웨어 컴포넌트와 사용자 계정, 애플리케이션, 디지털 인증서와 같은 디지털 아티팩트 두 가지로 나뉘어 관리된다. 제로 트러스트 아키텍처는 이러한 자산들을 물리적 위치나 네트워크를 포함하여 설정 및 조사와 업데이트가 항시 가능해야 한다. 또한, 기업 소유 인프라에서 새롭게 발견된 자산을 식별 및 구분, 액세스하는 능력을 갖추어야 한다. 추가로 기업 소유가 아닌 자산과 기업 소유의 쉐도우 IT를 구분할 수 있어야 한다. 쉐도우 IT는 네트워크 액세스가 필요하므로 특수한 문제를 일으키며, 액세스 결정이나 모니터링 및 포렌식에도 활용되기 때문이다. 효율적으로 감시 및 식별을 하기 위해서는 사용자나 객체의 행동을 감시하는 것이 중요하다. 광범위한 로그로부터 모든 행동을 세밀하게 확인하는 것은 현실적이지 못하기 때문에 조직 및 기업에서 중요한 리소스가 무엇인지 조사하여 어떠한 사용자와 객체로부터 어떠한 행동이나 접근을 탐지 및 방어해야 하는지에 대한 보안정책을 정의하는 것이 바람직하다[2, 5].

3. 핵심 프로세스 식별 및 위험 평가

세 번째는 비즈니스 프로세스와 데이터 플로우의 관계를 식별하고, 성능, 사용자 경험, 워크플로우 취약점 증가 가능성 사이에서 균형을 고려해서 순위를 부여하는 과정이다[2].

4. 제로 트러스트 아키텍처 후보에 대한 정책 수립

후보 서비스나 워크플로우는 프로세스의 중요성, 영향을 받는 주체, 워크플로우에 사용되는 리소스의 현재 상태 이 세 가지에 따라 결정된다. 따라서 자산이나 워크플로우를 식별한 후, 워크플로우가 사용하거나 영향을 주는 ID 관리 시스템, 데이터베이스, 마이크로서비스와 같은 모든 업스트림 리소스와 로깅, 보안 모니터링과 같은 다운스트림 리소스, 그리고 주체 및 서비스 계정과 같은 엔티티들을 식별해야 한다. 또한, 기업의 모든 주체가 사용하는 애플리케이션 및 서비스보다는 일부만이 사용하는 애플리케이션 및 서비스를 후보로 하는데 있어 유용하기 때문에 기업관리자는 후보 비즈니스 프로세스의 리소스 기준과 중요도에 따른 가중치를 결정해야 한다[2, 6].

5. 솔루션 후보 식별

비즈니스 프로세스 후보 목록이 작성 완료되면 설계자는 그에 맞춰 아래 기준에 따라 솔루션 후보 목록을 작성한다[2].

- 솔루션이 기업 소유가 아닌 자산을 사용하는 비즈니스 프로세스에는 적용이 제한되므로 클라이언트에 컴포넌트 설치하는지 확인
- 후보 비즈니스 프로세스의 리소스 위치는 제로 트러스트 아키텍처, 후보 솔루션에 영향을 주기 때문에 솔루션이 비즈니스 프로세스 리소스가 모두 온 프레미스(on-premise)에서도 동작하는지 확인
- 솔루션이 분석에 필요한 로그 상호작용에 대한 방법을 제공하는지 확인
- 프로토콜 및 전송을 광범위하게 지원하는 솔루션인지, 좁은 범위의 솔루션인지 확인
- 솔루션이 주체의 행위 변경 요청 시, 특정 워크플로우 수행을 위해 기업 주체는 수행 방법 변경요망

6. 초기 시행 및 모니터링

후보 워크플로우와 제로 트러스트 아키텍처 컴포넌트를 선택이 완료되면 초기 시행단계가 시작된다. 기업관리자는 처음에 관리자 계정이 필요한 리소스에 접근제한이 되거나, 할당된 접근 권한이 과도할 수 있으므로 주로 모니터링 모드로 운영하거나 새로운 제로 트러스트 정책이 효과적이고 운영 가능한지 확인 작업을 계속 수행하는 Reporting-only 모드로 운영할 수도 있다. 이러한 모드 운영을 통해 기업은 자산과 리소스에 대한 액세스 요청과 행위 통신 패턴의 베이스라인을 인식할 수 있다. 또한, 기본적인 정책을 실행하고 로그를 기록한다[2].

7. 제로 트러스트 아키텍처 확대

워크플로우 정책이 개선이 완료되면, 기업은 정상적인 운영 단계를 시작한다. 네트워크 및 자산을 지속해서 모니터링하고, 트래픽을 로그에 기록한다. 이때, 대응 및 정책 변경이 제때 이루어져야 하며, 주체 및 리소스와 프로세스의 이해 관계자는 운영 개선을 위한 피드백 활동을 계속 이어나가야 한다. 이 마지막 단계에서 기업관리자는 제로 트러스트의 다음 전개를 계획할 수 있다. 이 경우, 처음과 마찬가지로 워크플로우 후보 및 솔루션 후보를 식별하고, 정책 또한 새로 작성해야 한다. 또한, 신규 디바이스 접속, 제로 트러스트 논리 컴포넌트의 중요 업데이트, 조직 구조의 이동 등과 같은 시스템의 변화는 워크플로우와 정책 또한 변화시킬 수 있으므로, 이 경우에는 전체 프로세스를 다시 점검 및 검토해야 한다.

III. 결 론

본 논문에서는 제로 트로스트라는 새로운 네트워크 방어 개념을 소개하고, 다양한 기업환경에 적용하기 위한 보안구축 프로세스에 대해 살펴보았다. 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

[4] Jiyong Chun, Zero trust basis of network security strategy, IDG Summary AKAMAI MEGAZONE, 2021

[5] Zero Trust Introduction Acceleration-Microsoft's report [Internet]. Available: https://blog.naver.com/cspark14/222453433114

[6] Minju Hwang, Microsoft Zero Trust Network Strategy and Implementation Plan, Cyber Security Solutions Group