제로 트러스트 보안을 활용한 기업보안시스템 강화 방안

이선아* · 김범석 · 이혜인 · 박원형

상명대학교

Enhancement of Enterprise Security System Using Zero Trust Security

Lee Seon-a* · Kim Beom Seok · Lee Hye in · Won hyung Park

Sangmyung University

E-mail : sunnie39@naver.com / dizzvy77@daum.net / hilee0312@naver.com / whpark@smu.ac.kr

요 약

제로 트러스트 보안을 바탕으로 기존 기업보안시스템의 한계를 강화하는 방안을 제시한다. 4차 산업혁명 시대가 도래하면서 보안의 패러다임도 바뀌고 있다. 클라우드 컴퓨팅과 COVID-19로 인해 원격근무가 활발해지면서 변화된 IT 환경에서 발생하는 보안 문제에 대한 이슈가 제고된다. 동시에 공격기법들도 지능화되고 고도화되는 현 상황에서 기업에서는 제로 트러스트 보안을 활용해 현재의 보안 시스템을 더 강화해야 한다. 제로 트러스트 보안은 모든 것을 의심하고 신뢰하지 않는다는 핵심 개념을 토대로 모든 데이터 통신을 감시하고, 접근 요청자에 대한 엄격한 인증과 최소한으로 접근 권한을 허용함으로써 보안성을 높인다. 따라서, 본 논문에서는 기존 보안 시스템을 강화하는 제로 트러스트 보안 솔루션을 소개하고, 기업에서 도입해야 하는 방향성과 타당성을 제시한다.

ABSTRACT

It proposes a plan to strengthen the limitations of existing corporate security systems based on Zero-Trust. With the advent of the era of the Fourth Industrial Revolution, the paradigm of security is also changing. As remote work becomes more active due to cloud computing and COVID-19, security issues arising from the changed IT environment are raised. At the same time, in the current situation where attack techniques are becoming intelligent and advanced, companies should further strengthen their current security systems by utilizing zero trust security. Zero-trust security increases security by monitoring all data communications based on the concept of doubting and trusting everything, and allowing strict authentication and minimal access to access requestors. Therefore, this paper introduces a zero trust security solution that strengthens the existing security system and presents the direction and validity that companies should introduce.

키워드

제로 트러스트, 정보보안, 정보유출, 경계기반 보안모델, 기업보안시스템

Ⅰ. 서 론

COVID-19로 인해 사회적 거리 두기가 강화되면서 원격 근무의 필요성이 증가하였으며 근무 환경의 변화가 발생하였다. 원격 근무가 증가하면서 사이버 공격 범위가 기업 내부에서 외부로 확대되고 있다[1]. 단말기를 이용해 내부 시스템의 불법 침해가 가능하고, 기업 내부에서만 접근 가능했던 내부 자원에 대한 외부의 접근이 증가하면서 비인가 접근과 같은 보안위협이 존재한다[2]. 기존의 보안 시스템은 외부로의 접근만 차단하고, 내부는 신뢰하는 형태이기 때문에 내부 사용자의 공격이나 데이터 유출을 막을 수 없다는 한계점이 있다. 이에 따라 내/외부 네트워크에서 일어나는 모든 통신을 신뢰하지 않는 제로 트러스트(Zero Trust)에 주목하게 되었다. 제로 트러스트 기술을 활용하여

* speaker

접근자에 대한 철저한 인증과 모든 접근에 대해 감시하고 분석하여 사이버 공격으로부터 자원을 보호할 수 있다. 본 논문은 기업의 보안 한계점을 지적하고 보안수준을 높이기 위해 제로 트러스트 보안을 도입한 보안 시스템을 제안하고자 한다.

II. 제로 트러스트 보안

기존 경계기반 보안 모델을 대신해 외/내부 모든 통신을 고려해야 하는 상황에서 주목받는 기술이 '제로 트러스트'이다. 제로 트러스트는 아무도 신뢰하지 않지 않겠다는 전제하에 네트워크, 사용자, 애플리케이션, 서비스 등을 모두 의심해 필요한 사람에게 필요한 애플리케이션에만 접속하도록 하는 원칙이자 보안 모델이다[3]. 접근 요청자에 대해 철저하게 검증하고 최소한의 접근을 허용함으로써 공격이 유입될 수 있는 경로를 좁혀 보안성을 높인다. 비인가된 접근을 통제하고 인증 우회도 막을 수 있다.

<그림 1>은 제로 트러스트가 동작하는 구성도로, 자원에 접근하려는 접근 요청자를 제어하고 검증하는 프로세스를 가지고 있다. Control Plane을 통해 접근 허가 여부를 확인하고, 접근이 허가되면 Data Plane을 통해 기업과 기관의 자원에 접근하는 방식으로 제로 트러스트 보안을 수행한다. Policy Engine에서 접근 정책에 따라 최종적으로 접근허용 여부를 결정하고 Policy Administrator를 통해 직접 데이터를 송수신하고, Policy Enforcement Point는 원활한 데이터 전송 환경이나 조건이 충족되어있는지 확인한다. 여기서 모든 데이터 통신에 대해서 이벤트 발생 로그를 남기고 검증하기 때문에 보안 기능으로서 중요하다.

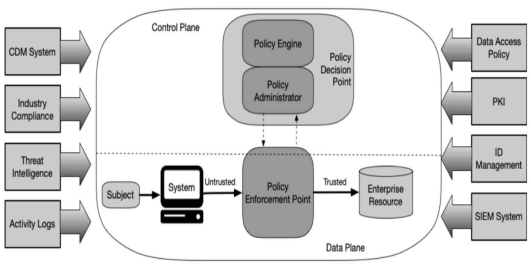

그림 1. 제로 트러스트 구성도 [4]

III. 기존 기업보안시스템

기존 기업 보안 시스템은 외부에서 내부로의 접근을 차단하고 방어하는 경계기반 보안 모델 기반으로 운영된다. 기본적으로 방화벽으로 비인가된 접근자가 내부로 접근하는 것을 방지한다. 웹 서비스에 특화된 웹 방화벽도 사용한다. 방화벽 외에도 IDS, IPS 등 침입차단 및 방지를 위한 보안 장비를 구성해 네트워크를 통해 발생할 수 있는 보안 사고를 예방한다. 그밖에도 다양한 보안강화를 위한 솔루션들이 이미 존재하지만, 보안 취약점을 통한 침해사고들은 계속 발생하고 공격 역시 고도화 지능화되고 있다. 경계기반 보안 모델은 내부접근이 일단 허용되면 내부 보안은 고려하지 않는다는 문제점이 있다.

클라우드 컴퓨팅 사용과 원격 근무가 증가하는 가운데, 경계기반 보안 시스템은 유의미한 보안 대책이 아니다. 외부에서 사원이 개인 PC를 통해 회사 내부 시스템에 접근할 필요가 있는 경우가 많아지고 이를 이용한 공격은 치명적이다. 동시에, 보안 담당자는 회사 네트워크로 접속하는 모든 기기를 관리하는 것은 현실적으로 어렵다. 외부와 내부를 막론하고 모든 접근에 대한 의심과 철저한 인증을 기반으로 하는 새로운 보안 체계가 필요하다.

IV. 기업보안시스템 강화 방안

제로 트러스트와 기존 보안 모델의 차이점은 차단을 중점으로 두는가, 아니면 인증을 중점으로 두는가에 있다[5]. 접근 허가된 사용자에게도 추가적인 인증을 통해 제로 트러스트를 실현해야 한다.

원격 근무에서 가장 취약한 부분은 개인 PC 침해 즉, 단말기에 있다. 기업 내부 PC보다 상대적으로 보안에 취약한 개인 단말기는 공격자들의 공격대상이 되기 쉽다. 공격자들이 단말기를 통해 내부까지 접근하게 되면 해당 기업의 예민한 정보 유출 또는 랜섬웨어 감염의 우려가 있다. NAC (Network Control Access)와 EDR (Endpoint Detection & Response)을 통해 비인가된 접근을 통제하고 단말기를 감시하여 1차 보안을 선제적으로 한다. 그 이후에는 MFA (Multi-Factor Authentication)와 SSO (Single Sign-On), DID (Decentralized Identify) 등 철저한 신원 인증을 위한 기술들을 통해 제로 트러스트를 구현해야 한다.

NAC는 네트워크 접근제어 기술로 네트워크에 접속하는 장치에 대한 접속 가능 여부를 확인하여 인가된 장치만이 접속할 수 있도록 제한하는 기술이다[6]. 사용자의 단말기를 인증하고, 접근을 제어하며 무결성을 확인한다. EDR은 단말기에서 위협탐지 및 대응을 하는 솔루션으로 실시간 차단보다 모니터링에 초점을 맞추고 있다[7]. 클라우드로 인해 개발된 보안 솔루션이지만, 다양한 형태로 존재하는 단말기에서 발생할 수 있는 이상 탐지하는 데에 목적이 있다. 원격 근무로 외부에 존재하는 단말기들의 모든 트래픽을 감시하고 실시간 검증을 통해 기업 정보를 보호해야 한다.

<그림 2>는 Cisco Duo의 MFA 인증 절차를 보여준다. ID/PW를 통해 1차 인증 후 지문인식, 앱, U2F 토큰 등 다양한 인증방식을 통해 2차 인증으로 사용자의 신뢰도를 확보할 수 있다.

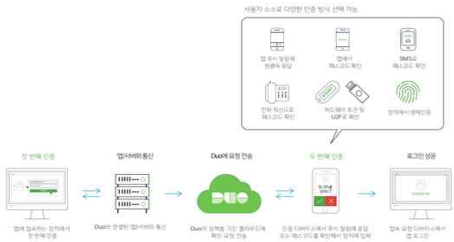

그림 2. 사용자 트러스트(멀티팩터 인증:MFA) [8]

MFA는 사용자가 1차 보안을 거친 후, 신원 인증을 할 때 쓰이는 솔루션이다. 사원의 아이디와 패스워드가 도난당하더라도, 두 번째 인증을 요구하여 보안성을 높인다. 이중 인증방식을 통해 보안성을 확보하더라도 길어진 인증시간으로 서비스의 불편함을 느낄 수 있다. 이러한 단점은 SSO 방식의 통합로그인 것으로 상쇄된다. SSO는 한 번의 로그인으로 해당 세션동안 여러 개의 서비스를 이용한다. MFA와 SSO를 통해 개인정보 보안을 한층 더 강화하면서 편리성도 유지할 수 있다. 그러나 SSO 솔루션의 통합로그인 방식은 공격자가 하나를 뚫으면 전체를 이용할 수 있으므로 신중하게 설정해야 한다. DID는 블록체인(Block-Chain)을 기반으로 사용자의 신원을 증명하는 솔루션이다. 정보를 분산해서 신원을 위한 최소한의 정보만을 선택해 증명할 수 있어 기업으로부터의 정보누출을 최소화할 수 있다. DID 기술은 마이 데이터(My Data)라는 개념이 부상하면서 주목받고 있다. 이는 사용자가 정보를 주체적으로 관리할 수 있다는 점에서 의미가 있다.

앞서 소개한 솔루션들은 기존 경계기반 모델과 비교하면 인가된 사용자도 재인증 과정을 거침으로써 보안을 한층 강화할 수 있을 것으로 기대된다. 제로 트러스트를 통해 제로데이 공격도 감소할 것으로 예측된다.

V. 결 론

본 논문은 기업에서 원격 근무 활성화로 인해 발생할 수 있는 문제점에 대한 보안강화 방안의 필요성과 제로 트러스트 보안을 도입한 방안을 제안한다. 제로 트러스트는 비인가 접근을 엄격히 통제하여 정보를 보호할 수 있다. 모든 접근과 통신에 대해 감시하고 최소한의 접근 권한만을 허용하기 때문에 공격자가 경로를 우회하여 접근하는 시도도 막을 수 있어 내/외부 시스템의 보안을 강화한다. 기존 보안방식의 한계점을 극복하는 제로 트러스트에 대한 꾸준한 논의와 분석을 통해 안전하고 확실한 기업보안 시스템으로 구축해야 한다. 제로 트러스트 보안을 활용한 보안 체계를 구체적으로 설계해야 하며, 기업에서 정상적인 업무 방해 없이 강화된 보안을 다양하게 활용될 수 있도록 추가적인 연구도 필요하다.

References

[1] Yongjin Jeon, “Effect of financial security and trust on non-face-to-face financial transactions”, Digital Convergence Journal, Vol. 19, No. 7, pp. 147-154, 2021.07

[2] Financial Security Agency, “Prospects for Digital Finance and Cybersecurity Issues in 2021”, 2020.02

[3] Ji Yong Chen, “No one believes in it, so it's a more complete zero trust-based network security strategy, IDG Summary | akamai megazone, 2021

[4] Scott Rose, Oliver Borchert, Stu Mitchell et. , “Zero Trust Architecture”, NIST Special Publication 800-207, Gaithersburg US, 2020

[5] Hak Jun Lee, The paradigm of corporate security, Zero Trust, which is drawing attention again [Internet]. Available : https://www.samsungsds.com/kr/insights/zero_trust.html

[6] GENIANS, Understanding of NAC [Internet]. Available:https://docs.genians.com/release/ko/intro.html

[7] AhnLab, Security Terms You Should Know in 2020 [Internet]. Available: https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=29228

[8] Cisco, “Cisco Duo Security Zero Trust Solution for User and Device Security”, CISCO systems Korea Ltd, Seoul, 2020