https://doi.org/10.33778/kcsa.2023.23.3.003

제로 트러스트 아키텍처 도입을 통한 기업 보안 강화 방안 - 마이크로 세그먼테이션 접근법 중심으로 -

주 승 현*, 김 진 민**, 권 대 현**, 신 용 태***

요 약

제로 트러스트는 "Never Trust, Always Verify"라는 원칙으로 알려진 새로운 보안 패러다임이다. 최근에는 원격 및 재택근무 환경의 확산과 클라우드 서비스의 사용 증가로 어디서든 업무 시스템에 접근 가능한 WFA(Work From Anywhere) 환경이 구축되고 있다. 이에 따라 내·외부 경계가 모호해져 기존의 경계 기반 보안 모델(perimeter security)만으로는 다양하고 복잡한 침해사고와 공격에 대응하기 어려워졌다. 이 연구에서는 제로 트러스트의 구현 원칙과 마이크로 세그먼테이션(micro segmentation) 접근법을 소개하며, NIST의 위험 관리 프레임워크를 활용하여 제로 트러스트 도입 절차를 제안하여 기업이 사이버 공격에 대비할 수 있는 보안 전략을 강화하는 방안을 제시한다.

Strengthening Enterprise Security through the Adoption of Zero Trust Architecture - A Focus on Micro-segmentation Approach -

Seung-Hyun Joo*, Jin-Min Kim**, Dae-Hyun Kwon**, Yong-Tae Shin***

ABSTRACT

Zero Trust, characterized by the principle of "Never Trust, Always Verify," represents a novel security paradigm. The proliferation of remote work and the widespread use of cloud services have led to the establishment of Work From Anywhere (WFA) environments, where access to corporate systems is possible from any location. In such environments, the boundaries between internal and external networks have become increasingly ambiguous, rendering traditional perimeter security models inadequate to address the complex and diverse nature of cyber threats and attacks. This research paper introduces the implementation principles of Zero Trust and focuses on the Micro Segmentation approach, highlighting its relevance in mitigating the limitations of perimeter security. By leveraging the risk management framework provided by the National Institute of Standards and Technology (NIST), this paper proposes a comprehensive procedure for the adoption of Zero Trust. The aim is to empower organizations to enhance their security strategies.

Key words : (Zero Trust, Micro Segmentation, WFA, Cyber Security)

접수일(2023년 06월 08일), 수정일(2023년 07월 21일), 게재확정일(2023년 08월 14일)

* 숭실대학교 IT정책경영학과(주저자)
** 숭실대학교 IT정책경영학과(공동저자)
*** 숭실대학교 IT정책경영학과(교신저자)

1. 서 론

전 세계적인 코로나19 팬데믹으로 인해 회사 외부에서 인터넷을 사용하여 원격·재택근무 환경이 급속도로 확대되었다. 또한, 직원들의 원격 접속용 기기가 다양해지고 처리되는 데이터의 양도 증가하면서, 기업들은 편의성과 서비스 유연성을 위해 업무 시스템을 클라우드로 이전하고 있다[1]. 이러한 "Work From Anywhere (WFA)" 환경에서는 내·외부 경계가 모호해지고, 공격 경로가 더욱 복잡해지는 현상이 나타나고 있다[2]. 따라서, 과거의 내·외부 네트워크 구분과 기업 내부에 안전한 경계를 구축하여 모든 것을 안전하다고 여기는 전통적인 사이버 보안 접근 방식인 "경계 기반 보안 모델(perimeter security)"은 업무 환경의 변화와 진화하는 공격에 대응하기에 한계가 있다고 판단되어, 기존 경계 기반 보안 모델의 한계를 극복하기 위해 "제로 트러스트 아키텍처"에 대한 연구가 진행되어 왔다. 기존의 제로 트러스트 연구는 특정 영역의 기술에 제로 트러스트를 적용하는 것에 초점을 맞추고 있었으며, '제로 트러스트를 위한 소프트웨어 정의 경계(SDP) 인증 메커니즘 제안 및 ECC 암호 구현'[3], 제로 트러스트 기반 문서형 악성코드 대응 시스템 설계 및 구현[4], '제로 트러스트 기반 리눅스 시스템 접근 권한 관리 방안'[5] 등과 같은 연구가 일반적이었다. 또한, '제로 트러스트 보안 프레임워크 설계에 관한 연구'[6], '제로 트러스트 원리를 반영한 보안 강화 요소 기술 적용 방안 연구'[7], '제로 트러스트 구축 프로세스에 관한 연구'[8]와 같이 제로 트러스트의 개념적인 연구도 주로 이루어졌다. 그러나 기업의 환경에 적용 가능하고 실질적인 보안 수준을 높이기 위한 실용적인 연구는 부족하였다. 이에 본 연구에서는 제로 트러스트 아키텍처 중 다양한 기업 환경과 사용 사례에 적용 가능한 제로 트러스트 아키텍처 중 마이크로 세그먼테이션(micro segmentation) 접근법을 중심으로 기업 환경에 적절히 적용하여 보안을 강화하는 방안을 제안하고자 한다.

2. 제로 트러스트 개요

2.1 제로 트러스트 개념과 역사

제로 트러스트는 2010년, 세계적인 연구기관 포레스터 리서치(forrester research)의 존 킨더버그(john kindervag) 수석 애널리스트가 처음으로 제안했다. 당시 모바일과 클라우드 환경이 점차 확산되면서 신뢰할 수 있는 내부와 공격자가 있는 외부를 나누는 뚜렷한 경계가 존재한다는 믿음을 버려야 한다는 콘셉트로, 기존 경계형 보안 모델과 대조되는 개념으로서 등장했다. 기업의 근무 환경이 점차적으로 분산되고 확대됨에 따라 기본적으로 아무도 신뢰해서는 안 된다는 전제를 가지고, 모든 접근이 잠재적 보안 위협이라는 가정 아래 모니터링하고 검증해야 한다는 주장이다. 현재는 구글의 Beyond Corp을 비롯해서 항공사인 웨스트젯, 글로벌 음료회사인 코카콜라 등 수많은 기업들이 제로 트러스트 보안 모델을 적용하여 기업의 내부 데이터를 보호하고 있다.[9] 이러한 기업 트렌드에 발맞춰서 미국 국립 표준 기술연구소(NIST)는 2020년 8월, 특별 간행물 800-207을 발간하여 제로 트러스트 아키텍처(ZTA, Zero Trust Architecture)의 표준을 제시하였다.[10] 또한, 2020년 미국은 최대 공급망 해킹 사고로 꼽히는 솔라윈즈(solar winds) 사태를 경험하며, 정부가 주도하여 연방 제로 트러스트 보안 전략을 강력하게 추진하고 있다.[11] 2021년 5월, 바이든 대통령은 국가 사이버 보안 강화를 목표로 한 행정 명령(EO14028, executive order on improving the nation's cybersecurity)에 서명하였다. 이 행정 명령에 따라 연방 정부는 보안 모범 사례를 채택하고 제로 트러스트 아키텍처로의 발전을 추구해야 한다. 그 결과, 각 정부 기관은 제로 트러스트를 구체적으로 추진하기 위한 방안을 발표하였다.[12] 미국 사이버 보안 및 인프라 보안국(CISA, The cybersecurity and infrastructure security agency)과 예산 관리국(OMB, The office of management and budget)은 이러한 목표를 달성하기 위해 필요한 기술 로드맵 작성을 감독할 계획을 세우고 있으며, CISA는 제로 트러스트 아키텍처로의 전환 시 참고할 수 있는 '제로 트러스트 성숙도 모델'을 2021년 6월에 발표했다. 또한, OMB는 2022년 1월에는 행정부 기관들이 2024년 9월까지 제로 트러스트를 적용하기 위해 어떻게 움직여야 하는지에 대한 개요를 담은 '제로 트러스트 사이버 보안 원칙을 향한 미국 정부 이동(Moving the U.S. Government Towards

Zero Trust Cybersecurity Principles)'과 같은 여러 문서를 발표했다.[13] 행정 명령에 따라 행정부 부서 및 기관은 2024년까지 제로 트러스트 구현 계획과 예산 추정치를 OMB에 제출해야 한다. 국내에서는 2022년 10월 과학기술정보통신부와 한국인터넷진흥원(KISA)을 중심으로 '제로 트러스트·공급망 보안 포럼'을 발족하고, 제로 트러스트 보안의 구체 방법론과 소요 기술 등 한국형 제로 트러스트 방법론을 담은 제로 트러스트 가이드라인 1.0을 2023년 7월 발표했다. 또한 같은 달 국가정보원에서는 K-제로 트러스트 아키텍처와 가이드라인 개발을 통해 2026년까지 정부 전 기관에 제로 트러스트를 적용하겠다고 밝힌 바 있다.[14][15]

<표 1> 제로 트러스트 관련 미 연방 정부 진행 사항

시기	기관	내용
2020.8	NIST	제로 트러스트 아키텍처 (SP 800-207) 발간
2021.2	NSA	제로 트러스트 보안 모델 수용 지침 발간
2021.5	조 바이든 대통령	국가 사이버보안 개선을 위한 행정 명령(EO14028) 발표
2021.6	CISA (사이버 보안 인프라보안국)	제로트러스트 성숙도 모델 (pre-decisional draft) 발간
2022.1	OMB (관리예산실)	제로트러스트 사이버 보안 원칙을 향한 미 연방정부 전략에 관한 각서 발표
2022.5	NIST	제로트러스트 아키텍처 계획: 연방 관리자를 위한 계획수립 지침 (CSWP 20) 발간
2022.6	법무부	제로트러스트 도입을 포함하는 '2022-2024 회계연도를 위한 미국 법무부 정보기술 전략 계획' 발표

2.2 제로 트러스트 구현 원칙

제로 트러스트는 고정된 네트워크 경계를 방어하는 대신 사용자, 자산, 자원 중심의 방어로 전환하는 진화된 보안 패러다임이다. 제로 트러스트 아키텍처는 기업의 인프라스트럭처와 워크플로우를 설계할 때 제로 트러스트 구현 원칙을 적용한 것이다. 제로 트러스트는 물리적 위치, 네트워크 위치, 자산 소유권(개인 소유, 법인 소유)만을 기준으로 하며, 암묵적인 트러스트는 자산이나 사용자 계정에 부여되지 않는 것으로 가정한다. 인증과 인가는 별개의 기능으로 간주되며, 인증·인가 후에 기업 자원에 대한 세션을 생성한다. 기업 네트워크 트렌드에는 원격 접속, BYOD, 클라우드 등이 포함되며, 이들은 기업 네트워크 외부에 위치한다. 제로 트러스트는 이러한 트렌드에 대응하기 위한 방법이다. 제로 트러스트는 네트워크를 분할하는 것이 아니라 자원(자산, 서비스, 워크플로우, 네트워크 계정 등)을 보호하는 데 중점을 둔다. 네트워크의 위치는 더 이상 자원의 보안 상태를 결정하는 주요 요소로 간주되지 않는다.[10] 이에 따라 본 연구에서는 NIST에서 제시한 제로 트러스트 구현 원칙을 종합하여 사용자 인증 강화, 기기 인증, 권한 관리, 보안 기능의 통합 및 중앙화, 로깅 및 모니터링 등 5가지 원칙을 제시한다.

2.2.1 사용자 인증 강화

WFA(Work From Anywhere), 재택근무 등과 같은 이유로 위치에 관계없이 서비스에 접근하는 환경에서는 계정 탈취 등의 위험을 줄이기 위해 MFA(Multi Factor Authentication) 등을 통해 사용자 인증을 강화해야 한다. MFA는 ID와 패스워드가 탈취되어도 OTP(One Time Password)나 생체 인증과 같은 2차 인증을 요구하여 보안 수준을 높인다. 그러나 다중 인증 방식을 통해 보안성을 강화하더라도 인증 시간이 길어지면서 서비스의 불편함이 증가할 수 있다. 이러한 단점을 완화하기 위해 SSO(Single Sign On) 방식의 통합 로그인을 사용할 수 있다. SSO 방식을 통하면 한 번의 로그인으로 여러 서비스를 이용할 수 있다. 따라서 MFA와 SSO를 결합하여 보안성을 강화하면서도 편리성을 유지할 수 있다. 그러나 SSO와 같은 통합 로그인 방식은 공격자가 한 가지 포인트만 성공적으로 공격하면 전체 시스템을 악용할 수 있기 때문에 신중하게 설정해야 한다.[16]

2.2.2 기기 인증

인가된 기기에서만 서비스에 접근할 수 있도록 해야 하며, 이를 위해 기기 등록 및 기기의 상태를 기반으로 한 동적 신뢰도 평가가 필요하다. 먼저 기기 인증을 위해 디바이스의 식별과 관리가 필요하다. 기업 네트워크에 연결되어 있거나 기업 리소스에 액세스하는 디바이스 중 기업 소유가 아닌 기기를 식별하고 모니

터링할 수 있는 능력을 갖추고, 기기의 접근 위치(내부망 또는 외부망)와 최신 보안 업데이트, 보안 솔루션(백신, DLP 등)의 설치 여부, 디스크 암호화 등 기기의 보안 상태를 확인하고 접근 여부를 결정해야 한다.

2.2.3 권한 관리

기업 리소스에 대한 액세스를 세션 단위로 세분화하고 요청자의 신뢰를 평가한 후 액세스를 허가해야 한다. 또한, 작업 완료에 필요한 최소한의 권한으로만 접근을 허용해야 한다. 이는 한 리소스에 인증 및 인가가 이루어져도 다른 리소스에 자동으로 접근 권한이 부여되지 않음을 의미한다. 리소스 접근 시에는 속성 기반 접근 제어(ABAC, Attribute Based Access Control)를 통해 접근 여부를 결정한다. ABAC에서는 세 가지 유형의 속성을 사용한다. 첫째, 'Subject'는 권한 관리 대상인 개인의 이름, 직업, 역할 등을 나타낸다. 둘째, 'Resource'는 시스템 기능, 웹 서비스 등과 관련된 자원을 나타낸다. 셋째, 'Environmental'은 현재 위험 수준, 네트워크 위험 수준 등과 같은 운영, 기술, 장소적 환경을 나타낸다.[17] 이러한 속성은 비즈니스 프로세스의 요구사항과 수용 가능한 위험 수준을 기반으로 작성되며, 리소스 액세스 정책은 데이터의 중요도와 민감도에 따라 유동적으로 변경될 수 있다. 최소 권한 원칙을 적용하여 가시성과 접근성을 제한해야 한다.

2.2.4 통합 및 중앙화

기업은 리소스 접근에 대해 일관되고 중앙 집중적인 정책 관리가 필요하다. 정책 관리 지점이 분산되어 있다면 일관된 정책 수립이 어려우며, 새로운 접근 주체나 리소스 추가 시에 정책 적용이 매우 어려울 수 있다. 또한, 어떤 접근 주체가 어떤 리소스에 접근할 때도 해당 정책을 결정하고 실행하는 지점은 이미 수립된 일관되고 중앙 집중적인 정책에 따라야 한다. 분산된 접속 방식이나 리소스 종류에 따라 정책을 결정하고 실행하는 지점이 있더라도 중앙 집중적인 정책 관리를 통해 일관된 접근 여부 결정이 이뤄져야 한다.

2.2.5 로깅 및 모니터링

기업은 모든 자산의 무결성과 보안 상태를 감시하고 조치해야 한다. 자산을 기본적으로 신뢰하지 않으며, 리소스에 대한 요청을 평가할 때 자산의 보안 상태를 평가해야 한다. 제로 트러스트를 구현하려는 기업은 사용자 이상 징후 탐지와 대응을 위해 내부와 외부의 모든 트래픽에 대한 중앙화와 가시성을 제공해야 한다. 침해가 발견된 자산, 알려진 취약점이 있는 자산, 조직에서 관리하지 않는 자산은 가장 안전한 상태로 간주되는 디바이스와 다르게 처리되어야 한다. 또한, 일부 리소스에는 액세스가 허용되지만 다른 리소스에는 액세스가 제한되는 디바이스(예: 개인 소유)도 다르게 처리되어야 한다. 이러한 경우에도 기업 리소스의 현재 상태에 대한 실용적인 데이터를 제공하기 위해 강력한 모니터링 및 보고 시스템이 필요하다.

3. 마이크로 세그먼테이션

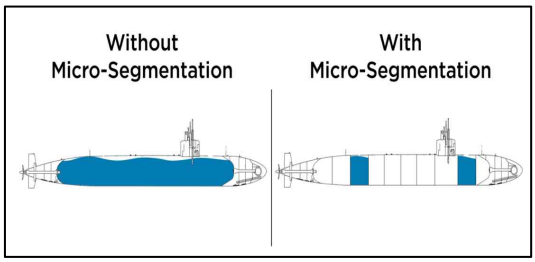
3.1 마이크로 세그먼테이션의 개념

제로 트러스트 아키텍처 보안 모델을 구성하기 위한 접근 방법은 여러 가지가 있다. NIST SP 800-207에서는 세 가지 접근 방법으로 분류하였다: 강화된 아이덴티티 거버넌스를 사용한 접근법(인증 체계 강화), 마이크로 세그먼테이션을 사용한 접근법, 그리고 네트워크 인프라 및 소프트웨어 정의 경계(SDP, Software Defined Perimeter)를 사용한 접근법이다.<표 2> 이 중 마이크로 세그먼테이션을 활용한 접근법은 다양한 유스 케이스에 적용할 수 있다. 이 접근법은 네트워크 세그먼트를 개별 워크 로드 수준까지 작은 영역으로 분할하여 세분화된 보안 정책을 각 개별 애플리케이션 워크 로드에 적용할 수 있게 한다. 이를 통해 외부망에서 내부망(north-south)으로의 침투 시에도 해당 사용자의 권한을 최소한으로 제한하여 마이크로 세그먼테이션을 통해 end to end로 구현하면 측면 이동(lateral movement)을 방지하여 시스템 간의 접근(east-west)을 차단할 수 있다.[18] 또한, 정의된 보안 모니터링 정책에 따라 네트워크 전반에서 침해 확산을 방지할 수 있고 침해 사고로 손상된 서버, 시스템, 클라우드 인스턴스 등을 빠르게 격리할 수 있다. 마지막으로 IT 환경에서 서비스나 데이터를 쉽게 분리할 수 있어 변화

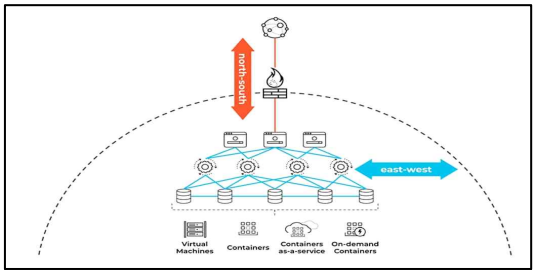
하는 IT 환경에 유연하게 대응할 수 있다.[19]

<표 2> NIST SP 800-207 제로 트러스트 아키텍처 접근 방법 비교

접근 방법	세부 내용
인증 체계 강화	• 행위자의 식별자를 핵심 요소로 설정하여 정책 작성 • 개방형 네트워크, 방문객 접근 허용 기업망, 기업 소유가 아닌 기기가 자주 연결되는 기업망 등에 적합 • 클라우드 기반 응용/서비스 사용 환경에도 유리 • 리소스 포털 배치 모델에 효과적
마이크로 세그먼테이션	• 보안 게이트웨이로 보호되는 단독 네트워크 구역(segment)에 개별 리소스 (혹은 리소스 그룹) 배치 • 다양한 유스케이스 및 배치 모델에 적용 가능 • 게이트웨이 기기 및 방화벽으로 일부 구현 가능하나 관리 비용 증가
소프트웨어 정의 경계	• 소프트웨어 정의 경계 기법을 활용하여 정책 엔진의 결정에 따라 컨트롤러가 네트워크를 재구성 • 디바이스 에이전트-게이트웨이 배치 모델 활용 • 클라우드 가상 네트워크 혹은 IP 기반이 아닌 네트워크 등에서도 변형된 형태로 사용 가능



(그림 1) 마이크로 세그먼테이션 개념도



(그림 2) 측면 이동(lateral movement)

3.2 마이크로 세그먼테이션 구현 방식

마이크로 세그먼테이션은 네트워크 기반, SDN 기반, 호스트 기반의 세 가지 방식으로 구현된다. 네트워크 기반은 네트워크 세그먼트를 세분화하고 분리하여 보안을 강화하지만 정책 관리와 비용 문제가 있다. SDN 기반은 소프트웨어로 구현되어 중앙화와 자동화를 가능하게 하지만 보안 기능에 제한이 있다. 호스트 기반은 워크 로드에 에이전트를 설치하여 유연하고 가시성이 우수하나 에이전트 관리에 우려가 있다.

<표 3> 마이크로 세그먼테이션의 구현 방식 비교

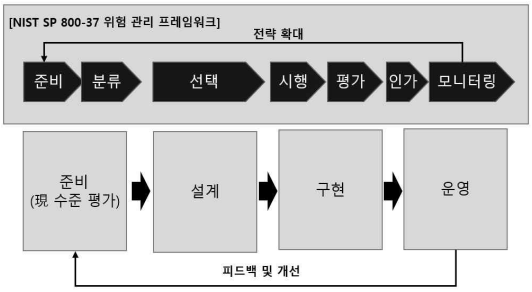
구분	특징
네트워크 기반 (network-based)	• 네트워크 장비(스위치, 라우터, 방화벽 등)의 액세스 제어 목록(Access Control List), 서브넷팅, VLAN 등을 통해 분리, 제공함으로써 구현 • 규모가 큰 네트워크의 경우, 정책 관리의 복잡성이 높아지고, 관련 장비에 대한 투자가 필요하며, 이로 인해 높은 비용이 요구됨. 또한, 이슈 및 장애 발생 확률이 비교적 높음
SDN 기반 (Software Defined Networking -based)	• 네트워크 기반에서 사용되던 장비들이 소프트웨어로 구현되는 방식 • 소프트웨어로 구현되면서 상대적으로 낮은 비용으로 마이크로 세그먼테이션의 중앙화·자동화 가능 • 단, 네트워크 기술로 보안 기능 적용에는 한계가 존재
호스트 기반 (host-based)	• PC·서버와 같은 워크로드에 에이전트를 설치하는 방식으로 에이전트에 내장된 방화벽 기능을 활용 • 회선 성능 저하가 없고, 유연한 동적 적용이 가능하며, 개별 어플리케이션 및 서비스에 대한 정보 획득으로 가시성 확보에 우수 • 워크로드 내에 에이전트 배포 및 관리에 대한 우려 존재

4. 제로 트러스트 도입 (마이크로 세그먼테이션 접근법 기반)

4.1 제로 트러스트 도입 프로세스

제로 트러스트의 구현 원칙과 마이크로 세그먼테이션을 반영하여 기업의 환경에 맞춰서 구현이 필요하다. 제로 트러스트 도입 단계를 위험 관리 프레임워크인 NIST SP 800-37의 단계와 매핑하여 준비 → 설계 → 구현 → 운영으로 구분하고 지속적으로 피드백 및

개선이 이뤄질 수 있도록 해야 한다.



(그림 3) 제로 트러스트 도입을 위한 절차

<표 4> 제로 트러스트 도입 단계별 세부 내용

구분	세부 내용
준비	• 제로트러스트 도입 전 기업망 핵심요소(기기, 네트워크, 시스템, 데이터 등)를 파악하고 이를 중심으로 현재 보안 대상·수준을 평가
설계	• 비즈니스 프로세스의 접근 주체와 리소스 상태를 파악하고, 중요한 자산과 리소스를 결정하여 데이터 등급 분류를 통해 보안 정책 수립
구현	• 주요 자원의 위치, 프로토콜, 서비스 등을 고려하여 각 기업 의 업무 환경에 적합한 솔루션 검토 및 구현
운영	• 제로 트러스트 솔루션 도입 후 정책 설정 및 시행하고 자산 및 리소스 액세스 패턴을 파악한 후 점진적으로 정책을 개선
피드백·개선	• 제로 트러스트 아키텍처를 개선하기 위해 지속적 평가와 재식별 수행을 통한 수준 고도화

4.1.1 준비 단계

준비 단계에서는 기업이 제로 트러스트 아키텍처 도입을 위해 현재 상황과 수준을 정확히 파악하고 평가하는 것이 중요하다. 이를 위해 비식별된 Shadow IT 영역을 최소화하고 모든 주체, 자산, 데이터 및 워크플로우를 식별하고 각 IT 영역 별 특성에 따라 마이크로 세그먼테이션 접근법 적용을 위한 성숙도 평가를 해야 한다.<표 5>,[20] 첫째로, 주체는 리소스에 접근하려는 사용자와 서비스 계정 등 리소스와 상호 작용하는 모든 주체를 의미한다. 주체의 직무, 역할, 상태 등의 정보는 최소한의 접근 권한 부여 시 중요한 정보가 될 수 있다. 둘째로, 자산을 식별하고 평가하는 것은 제로 트러스트 아키텍처 도입의 핵심 요소이다. 기업 자산에는 하드웨어(노트북, 핸드폰, IoT 디바이스) 및 소프트웨어(애플리케이션, 인증서) 등이 포함된다. 기업은 자산의 상태 정보를 실시간으로 모니터링하고 관리하여 최신 상태를 유지해야 한다. 이를 통해 기기의 리소스 접근 정책을 결정할 수 있어야 한다. 셋째로, 데이터 및 워크플로우이다. 기업은 접근 주체의 리소스 접근을 허용하거나 거부하는 정책과 제로 트러스트 아키텍처를 어떻게 도입할지 결정하기 위해 데이터 및 워크플로우를 평가해야 한다. 예를 들어, 비즈니스 위험도가 낮은 업무 시스템부터 위험도가 높은 대외 서비스로 점진적으로 제로 트러스트로 전환하는 것도 하나의 방법이다.

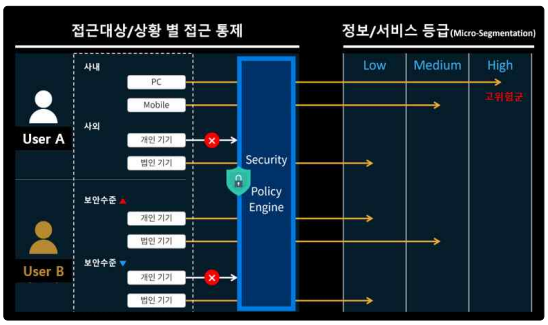
<표 5> IT 영역 별 성숙도 평가 시 고려사항

구분	고려 사항
주체	• 업무 상 필요한 권한이 적절히 부여되었는지 등 정기적 감사 여부 • 세부 인증 기술, 싱글사인온(SSO), 다중 인증(MFA) 방법 및 안전성 • 지속적인 신원 인증 방법 및 안전성 • 컨텍스트 기반 인증, 사용자 모니터링 및 행동 분석, 가시성 확보 방법 • 최소 권한 부여 정책 도입 여부 • 접근제어 기술/수준 (ABAC 적용 여부) • 개발자 및 시스템 관리자와 같은 특수 권한 사용자의 접근 권한에 대한 정밀한 제어 기술
자산	• 모든 기업 소유 자산 및 담당자, 속성 식별 및 분류 여부 • 기기 로그인(비밀번호, PIN, 생체 인식 등) 방법 및 안전성 • 기기에서 제공하는 사용자 인증 방법의 안전성 • BYOD 단말 보안 및 접근제어 정책 • 자동화된 단말 등록 및 자산·취약점 관리 수준 • 기기 상태 및 정책 준수에 대한 실시간 지속 모니터링, 가시성 확보, 검증 방법 • 등록되지 않은 기기의 접근 권한 차등 부여 혹은 접근 차단 정책, 감시 방법
데이터 및 워크플로우	• 패킷 검사 및 동적 필터링, 암호화 패킷 분석 등 위협 대응 기술 • 네트워크 암호화 기술 • 온프레미스·클라우드 시스템 계정 관리 및 접근 통제 기술 • 응용 및 워크로드 접근에 대한 중앙 집중적 인증·인가 및 실시간 위험 분석

	• 응용 개발·배포 시 DevSecOps 등 적용 • 자동화된 데이터 분류 및 위험 기반 동적 접근제어 정책 • 데이터 저장 시 암호화 기술 • 데이터 분류 시 중요(민감) 정보 태깅 • 데이터 분류 기준에 따라 암호화 적용

4.1.2 설계 단계

먼저, 어떤 비즈니스 프로세스에 제로 트러스트를 도입하는 것이 가장 적합한지 판단한 후, 선택된 비즈니스 프로세스에 대해 중요성과 관련된 접근 주체 및 리소스의 현재 상태를 파악하고 정책을 수립해야 한다. 리소스 접근과 관련된 정책 설계는 기업 관리자가 후보 비즈니스 프로세스에서 사용하는 리소스에 대해 기준을 결정하거나 중요도에 따른 가중치를 부여해야 한다. 이를 위해 관리자는 조정 단계에서 기준과 가중치를 조정할 수도 있다. 또한, 신뢰도 평가 알고리즘을 고려하여 해당 프로세스에서 사용되는 기준과 중요도에 따른 가중치 또는 점수를 결정해야 한다. 이를 위해서는 데이터 등급 분류 작업도 수행되어야 한다. 특히, 마이크로 세그먼테이션을 기반으로 한 세부 보안 정책을 적용하기 위해서는 데이터 등급 분류가 중요하다. 모든 네트워크 자산과 리소스를 동일한 수준으로 보호할 수는 없으므로, 비즈니스 프로세스에서 가장 중요한 자산과 리소스를 먼저 결정하고 활동의 우선순위를 지정하는 것이다.



(그림 4) 마이크로 세그먼테이션 기반 접근 정책 예시

4.1.3 구현 단계

선택된 비즈니스 프로세스에 제로 트러스트 아키텍처를 설계하려는 기업 담당자는 어떤 제로 트러스트 솔루션을 적용하여 구현할지 결정해야 한다. 이를 위해 마이크로 세그먼테이션의 세 가지 구현 방식인 네트워크, SDN, 호스트 기반 중 기업 환경에 적합한 방식을 고려하여 적절한 솔루션을 선택해야 한다. 이 과정에서 기기에 에이전트 프로그램을 설치할지 여부, 적용되는 운영 체제의 범위(MacOS, Windows 등), 클라우드와 온 프레미스 환경의 지원 여부, 다양한 응용 서비스 프로토콜(HTTP, HTTPS, SSH 등)의 지원, 성능, 업무 편의성, 업무 특성 등을 고려해야 한다. 비즈니스에 적용할 때는 기존 비즈니스 프로세스에 직접 적용하는 대신 파일럿 프로그램을 작성하여 사전 테스트를 진행하고 안정성을 검증하는 것이 적절하다.

<표 6> 요구사항 별 제로 트러스트 솔루션 예시

요구사항	세부내용	관련 솔루션
통합 계정인증 (SSO)	서비스 별 분산된 계정을 통합하여 SSO 환경 구축	Azure AD (IDaaS, SAML SSO)
통합 권한관리 (IAM)	ABAC 기반의 조건부 액세스를 통해 중앙 접근제어	Azure AD (조건부 액세스)
기기 검증	기기의 상태체크 및 정책준수 체크 및 모니터링	Intune + SCCM
보안위험 점수	주체 및 기기의 보안위험 점수를 반영한 접근제어	Identity Protection + MDATP
서비스 통제 (HTTP)	On-Premise 웹서비스 및 Public SaaS 서비스에 대한 세부 권한 통제	MCAS
서비스 통제 (non-HTTP)	SSH, FTP 등 non-HTTP 서비스 제어	PAM, GlobalProtect

4.1.4 운영 단계

제로 트러스트 솔루션을 도입하여 특정 비즈니스 프로세스에 대한 제로 트러스트 아키텍처 보안 모델이 구현하였다면, 기업 관리자는 해당 솔루션을 기반으로 정책을 설정하고 시행해야 한다. 그러나 정책 시행 과정에서는 여러 문제가 발생할 수 있다. 예를 들어, 정상 사용자의 접근이 거부되거나 실제보다 과도한 권한이 부여될 수 있다. 새로운 제로 트러스트 비즈니스 워크플로우에 대해 정책이 효과적으로 운영 가능한지 확인될 때까지 리포팅만 수행하는 모드(reporting-only mode)로 운영할 수도 있다. 이를 통해 기업은 자산·리

소스에 대한 액세스 요청·행위·통신 패턴의 베이스라인을 인식할 수 있다.[21] 리포팅 모드는 기본적인 정책을 제외한 대부분의 접근 요청을 허가하면서 접속 로그를 분석하여 최초 정책과 비교하는 방식이다. 그러나 보안이나 기업 정책상 리포팅만으로 운영이 어려운 경우, 기업 운영자는 로그를 주의 깊게 모니터링하여 비정상적인 접근 제어를 확인하고, 문제가 있다고 판단되면 접근 제어 정책을 지속적으로 튜닝하여 운영을 개선해야 한다.

4.1.5 피드백 및 개선 단계

시범 운영이 성공적으로 완료되면 기업 관리자는 판단에 따라 정상적인 운영 상태로 전환한다. 이때 사용자, 자산, 네트워크를 지속적으로 모니터링하고 관련 정보와 로그를 기록해야 한다. 기업 관리자는 필요에 따라 접근 제어 정책을 조정할 수 있지만, 영향 평가와 사전 테스트를 통해 심각한 영향을 최소화해야 한다. 운영 과정에서는 접근 주체, 리소스, 프로세스에 대한 이해관계자가 운영 개선을 위한 피드백을 제공할 수 있으며, 기업 관리자는 이러한 피드백을 지속적으로 유도하고 반영해야 한다. 피드백과 개선 단계에서 기업 관리자는 제로 트러스트 아키텍처를 개선하고 성숙도를 높이기 위해 접근 주체, 자산, 비즈니스 프로세스, 워크플로우를 재식별하고 지속적인 평가를 수행해야 한다. 이때 현재 운영 중인 제로 트러스트 아키텍처와 관련하여 비즈니스 프로세스, 워크플로우, 접근 주체의 변화, 회사 내부 정책, 컴플라이언스, 법적 요건 등을 고려해야 한다.

5. 결 론

본 연구는 전 세계적인 코로나19 팬데믹으로 인해 원격 및 재택근무 환경이 확대되고 기업들이 클라우드 기반의 업무 시스템을 채택하는 추세에서, 기존의 경계 기반 보안 모델인 'Perimeter Security'의 한계를 극복하기 위한 제로 트러스트 아키텍처와 마이크로 세그먼테이션 접근법의 중요성을 탐구하였다. 제로 트러스트 아키텍처는 고정된 네트워크 경계 대신 사용자, 자산, 자원 중심의 방어로 전환하는 새로운 사이버 보안 패러다임으로, 사용자 및 기기 인증, 권한 관리, 보안 기능의 통합과 중앙화, 로깅 및 모니터링 등의 구현 원칙을 제시하였다. 마이크로 세그먼테이션은 제로 트러스트 아키텍처의 구현 방법 중 하나로, 네트워크 세그먼트를 개별 워크로드 수준까지 작은 영역으로 분할하여 세분화된 보안 정책을 적용함으로써 외부망에서 내부망으로의 침투와 측면 이동을 방지하고 침해사고로부터 자원을 격리하는 등의 보안 강화 효과를 제공한다. 마이크로 세그먼테이션을 기반으로 한 제로 트러스트 아키텍처의 도입 절차는 NIST의 위험 관리 프레임워크를 활용하여 준비, 설계, 구현, 운영 단계로 구분하였으며, 이를 통해 기업은 현재 상황과 수준을 파악하고 리소스 식별 및 평가, 중요도에 따른 정책 수립, 적절한 제로 트러스트 솔루션 선택 등을 진행할 수 있다. 이를 통해 기업은 제로 트러스트 아키텍처와 마이크로 세그먼테이션을 활용하여 업무 환경의 보안을 강화하고 변화하는 사이버 공격에 대비할 수 있으며, 제로 트러스트 도입 절차를 따라가며 지속적인 피드백과 개선을 통해 보안 전략을 강화해야 한다.

참고문헌

[1] 이민원, 권헌영, "제로 트러스트 명문화를 통한 신보안체계 강화 방안 연구-전자금융거래법상 법적 개선을 중심으로", 융합보안논문지, 제23권, 제1호, pp. 9-17, 2023.

[2] 데이터넷, "보안 경계 사라지는 재택근무", https://www.datanet.co.kr/news/articleView.html?idxno=152597, 2022.

[3] 이윤경, 김정녀, "제로 트러스트를 위한 소프트웨어 정의 경계(SDP) 인증 메커니즘 제안 및 ECC 암호 구현", 정보보호학회논문지, 제32권, 제6호, pp. 1,069-1.080, 2022.

[4] 장예슬, "제로 트러스트(Zero-Trust) 기반 문서형 악성코드 대응 시스템 설계 및 구현", 중앙대학교, 2022.

[5] 최여정, "제로 트러스트 기반 리눅스 시스템 접근 권한 관리 방안", 한남대학교, 2022.

[6] 임형석, "제로 트러스트 보안 프레임워크 설계에 관한 연구", 중앙대학교, 2022.

[7] 이다인, 이후기, "제로 트러스트 원리를 반영한 보안 강화 요소 기술 적용 방안 연구", 융합보안논문지, 제22권, 제3호, pp. 3-11, 2022.
[8] 이대성, "제로 트러스트 구축 프로세스에 관한 연구", 한국정보통신학회 종합학술대회 논문집, 제25권, 제2호, pp. 464-466, 2021.
[9] IT DAILY, "제로 트러스트(Zero Trust) 보안 체계 구현을 위한 차세대 인공지능 보안관제", http://www.itdaily.kr/news/articleView.html?idxno=210351, 2022.
[10] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, "Zero Trust Architecture, NIST Special Publication 800-207", NIST (National Institute of Standards and Technology), 2020.
[11] 최윤영, "미국의 소프트웨어 공급망 보안 정책 동향: SBOM 사례를 중심으로", 정보보호학회지 제32권, 제5호, pp. 7-14, 2022.
[12] JOSEPH R. BIDEN JR., "Executive Order on Improving the Nation's Cybersecurity", The White House, 2021.
[13] Shalanda D. Young, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles", The WhiteHouse, 2022.
[14] IT DAILY, "과기정통부, 제로 트러스트 가이드라인 1.0 발표", http://www.itdaily.kr/news/articleView.html?idxno=215209, 2023.
[15] 전자신문, "2026년부터 정부 조기관에 K-제로 트러스트 적용된다" https://www.etnews.com/20230719000149, 2023.
[16] 이선아, 김범석, 이혜인, "제로 트러스트 보안을 활용한 기업보안시스템 강화 방안", 한국정보통신학회 제25권 제2호 pp. 214-216, 2021.
[17] Muhammad Umar Aftab, Zhiguang Qin, "Role-Based ABAC Model for Implementing Least Privileges", ICSCA '19: Proceedings of the 2019 8th International Conference on Software and Computer Applications, pp. 467-471, 2019.
[18] 데일리시큐, "[보안칼럼] Zero Trust 구현하기", https://www.dailysecu.com/news/articleView.html?idxno=129154, 2021.
[19] Palo Alto Networks Cloud Security Team, "What Is Microsegmentation?", Palo Alto Networks, 2023.
[20] 제로트러스트포럼, "제로트러스트 가이드라인 1.0", 과학기술정보통신부, pp. 77-80, 2023.
[21] 이대성, "팬데믹 시대의 사이버 보안 기술 및 표준화 동향", 융합연구리뷰, Vol.8, pp. 3-28, 2022.

〔저자소개〕

주 승 현 (Seung-Hyun Joo)
2018년 건국대학교 정보보안학과 석사
2022년 숭실대학교 IT정책경영학과 박사과정
email : mrjoo33@gmail.com

김 진 민 (Jin-Min Kim)
2000년 숭실대학교 컴퓨터학부 학사
2002년 포항공과대학교 컴퓨터공학과 석사
2022년 숭실대학교 IT정책경영학과 박사과정
email : mins831@naver.com

권 대 현 (Dae-Hyun Kwon)
1997년 한양대학교 전자공학과 학사
2000년 한양대학교 전자공학과 석사
2022년 숭실대학교 IT정책경영학과 박사과정
email : daehyunka@ls-electric.com

신 용 태 (Yong-Tae Shin)
1985년 한양대학교 산업공학과 학사
1990년 Univ. of lowa, 컴퓨터학과 석사
1994년 Univ. of lowa, 컴퓨터학과 박사
1995년 숭실대학교 컴퓨터학부 교수
email : shin@ssu.ac.kr