정 보 보 호 학 회 지
제34권 제3호, 2024. 6

제로트러스트 기반 사이버보안 프레임워크 설계 방향

신 인 준*, 권 상 오**, 김 창 훈***

요 약

코로나 팬데믹 이후 원격근무와 클라우드 업무환경으로의 전환이 가속화되었다. 이러한 급격한 변화로 인해 기존 보안 모델의 문제점이 드러났고, 이를 해결하기 위해 미국을 포함한 여러 국가들이 제로트러스트(Zero-Trust) 기반 보안 모델을 제안하고 있다. 그러나 제로트러스트 기반 보안 모델은 많은 기관의 실질적인 환경으로 직접 적용하기는 매우 어려운 현실이다. 이는 많은 국가들이 제안하는 제로트러스트 기반 보안 모델은 보안 원칙과 구현에 대한 가이드만 제공할 뿐, 적용하는 기관의 상황을 고려한 보안 운영 방안을 제시하지 않고 있어 직접 적용하기에는 한계가 있다. 따라서 본 논문에서는 기관의 제로트러스트 기반 보안 체계 도입을 위한 사이버 보안 프레임워크의 설계 방안을 제안하고자 한다.

Ⅰ. 서 론

코로나 이전의 기업과 기관은 경계기반 보안 모델을 기반으로 내부망과 외부망으로 네트워크를 분리하여 운영하고 있었다. 그러다 코로나 팬데믹이 찾아온 이후 정부에서 사회적 거리두기와 재택근무를 지시하면서 원격근무와 클라우드 업무 환경으로 전환되고 있다. 갑작스러운 환경 변화는 기존 보안 기술의 다양한 문제점을 드러내는 계기가 되었다. 기존의 경계기반 보안 모델은 내부망 보호를 위해 방화벽, VPN(Virtual Private Network), NAC(Network Access Control)을 이용하여 이용자를 통제하였다. 하지만 이 장치들의 문제점은 이용자가 실제 사용하는 클라이언트 애플리케이션을 통제하지 못하여 해커는 이용자 장치의 애플리케이션의 취약점을 이용하거나 VPN의 취약점을 우회하여 경계를 넘어서는 공격이 가능하다. 이러한 문제점을 보완하기 위해 미국을 포함한 여러 국가들은 제로 트러스트(Zero-Trust) 기반 보안 모델을 제시하였다.[1] 제로트러스트는 “모든 요청을 절대 신뢰하지 말고 항상 검증하라”는 원칙의 보안 모델로 내부망과 외부망의 모든 요청을 검증함으로써 기존의 경계기반 보안 모델의 한계점을 극복할 수 있다. 하지만 제로 트러스트 보안 모델을 그대로 기존 환경에 도입하기에는 한계점이 존재한다. 미국과 각 나라 기업에서 제공하는 제로 트러스트 보안 모델은 원칙과 구현에 대한 가이드만 제공하여 적용하는 기관의 상황을 전혀 고려하지 않기 때문이다. 따라서 각 기관과 기업에 맞게 사이버 보안위험을 체계적이고 일관되게 관리할 수 있도록 운영을 위한 지침 사항이 필요하다. 이러한 현실을 반영하기 위해 본 논문에서는 제로트러스트 기반 사이버 보안 프레임워크의 설계 방안에 대해서 기초적인 설계 방향에 대해 제안하고자 한다.

Ⅱ. 제로트러스트 정책 도입

제로 트러스트의 도입은 코로나 팬데믹에 의해서 가속화된 것도 있으나 실질적으로 도입을 촉진되게 한 사건은 미국의 Biden 대통령의 행정명령 14028[2]에 의하여 각 나라의 정부, 민간 기관에 영향을 미치게 된다.

2.1. 미국 행정명령 14028

미국 정부의 행정명령 14028은 2021년 5월 12일에 발행된 명령으로 주요 목표는 연방 정부의 사이버보안 태세를 현대화하고, 민간부문과 협력하여 사이버 위협에 효과적으로 대응하는 것을 목표로 둔다. 해당 문서에는 이전 미국의 사이버보안 정책과 환경에 대한 여러 가지 문제점에 대해서 기술하고 있다. 행정명령 이

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음(RS-2020-II201797).
* 대구대학교 IT융합공학과 (대학원생, sij0507@daegu.ac.kr)
** 포위즈시스템 연구소 (수석연구원, sokwon@forwiz.com)
*** 대구대학교 정보보호학과 (교수, 교신저자, kimch@daegu.ac.kr)

전에는 연방 정부의 사이버 보안 정책 및 규정은 기관별로 다르게 적용되었으며, 사이버 위협 사고 정보 공유에 제약이 존재하였다. 또한 클라우드 보안 및 제로트러스트 아키텍처 도입이 일관되지 않았으며 소프트웨어 공급망 보안에 대한 명확한 기준이 부족하였다. 이러한 이유로 바이든 행정부는 다음과 같이 내용을 기술하고 있다.

2.1.1. 사이버 위협정보 공유 강화

사이버 위협정보의 공유를 강화하여 연방기관 간 협력 및 신속한 대응이 가능하게 만들었다. 이를 위해 기존의 사이버 위협정보의 공유를 표준화하고 체계화하기 위한 프로토콜을 수립하였고, 미국의 기관 CISA(Cybersecurity and Infrastucture Seurity Agency)가 중심이 되어 각 연방 기관에서 수집된 사이버 위협 정보를 중앙에서 관리하고 배포하도록 하였으며, 정보통신기술 서비스 제공자와 계약을 맺은 연방기관은 사이버 사건 발생 시 이를 즉시 CISA에 보고하도록 의무화 하도록 하고 있다.

2.1.2. 클라우드 보안 및 제로트러스트 아키텍처

모든 연방 기관이 제로 트러스트 아키텍처를 도입하고 클라우드 서비스 보안을 강화하도록 명령하였는데, 이를 위해 미국 CISA는 클라우드 보안 기술 참조 아키텍처를 개발하여 각 연방 기관이 클라우드로 안전하게 전환할 수 있도록 지원하고 있다. 특히, 모든 연방 기관은 다중 요소 인증(MFA, Multi-Factor Authentication) 및 데이터 암호화를 의무화하여 보안을 더욱 강화하고 있으며, 이는 사이버 공격으로부터 중요한 데이터를 보호하는 데 중요한 역할을 한다.

2.1.3. 소프트웨어 공급망 보안

소프트웨어 공급망 보안을 체계적으로 강화하였다. 연방 정부와 계약하는 소프트웨어들에 소프트웨어 구성목록 (SBOM, Software Bill of Materials)을 도입하여 소프트웨어 구성요소의 투명성을 높이고 보안성을 강화하고 있다. 그리고 NIST(National Institute of Standards and Technology)에서 소프트웨어 공급망 보안을 강화하기 위한 다양한 기준과 지침을 개발하여 온라인을 통하여 배포하고 있다.

2.1.4. 사이버 보안 사고 표준화

각 연방 기관은 사이버 보안 사고 발생 시 따를 수 있는 표준화된 대응 계획(Playbook)을 마련할 수 있도록 선포하였다. 대응 계획에는 사고 식별, 조사, 완화, 복구 등의 단계별 절차가 포함되며, 각 단계에서 수행해야 할 구체적인 활동이 명시되어 있다. 각 단계에서 누가 무엇을 해야 하는지 명확히 정의하여, 역할과 책임을 분담해야 한다. 또한 연방 정부 전반에 걸쳐 엔드포인트 탐지 및 대응 시스템이 구현되어, 사이버 공격에 대한 신속한 대응이 이루어질수 있는 방안을 제시하고 있다.

2.1.5. 소프트웨어 개발 보안 라이프사이클 표준

NIST에서 소프트웨어 개발 보안 라이프사이클 표준 및 소스 코드 테스트 최소 요구사항을 수립하여 이를 통해 소프트웨어의 보안성을 평가하고, 개발 관행을 개선할 수 있는 지침을 제시하고 있다.

해당 정책 발표 이후 NIST, CISA, DoD, NSA 등 여러 관계 기관에서 해당 행정명령을 실질적으로 이행하기 위한 각종 문서를 발간하고 있으며, NIST를 중심으로 관련 기업들의 기술을 모아 실 업무 적용을 위한 실험을 실시하고 있는 것으로 알려져 있다. NIST는 소프트웨어 공급망 보안 강화 지침을 수립하고, 소비자용 사이버 보안 라벨링 프로그램의 초기단계를 완료하였으며 제로트러스트 아키텍처로 전환하기 위한 가이드라인을 제공하고 있다.

2.2. NIST CSF

NIST CSF(Cybersecurity Framework)는 2013년 2월 12일, 오바마 대통령의 행정명령 13636에 따라 시작되었다. 이 프레임워크는 중요한 인프라의 사이버 보안을 강화하기 위해 다양한 이해 관계자와 협력하여 개발되었다. 국가의 중요한 인프라는 사이버 보안 위협에 취약하며, 이는 국가 안보와 경제에 심각한 영향을 미칠 수 있다. 행정명령 13636[3]은 이러한 문제를 해결하고자 국가 중요 인프라의 보안과 회복력을 강화하는 것을 목표로 하였다. 이 프레임워크는 다양한 산

업 분야에서 사이버 보안 위험을 관리하고 대응하는 데 중요한 지침이 되어 왔다.

2.2.1. CSF v1.0

NIST CSF v1.0[4]의 주요 목표는 조직의 사이버 보안 관리를 위한 표준을 정하고, 사이버 보안 위험 관리를 개선하며, 사이버 보안 위험과 비즈니스 목표 간의 균형을 유지하고, 조직의 사이버 보안 성숙도를 향상시키는 데 있다. 이 프레임워크는 다섯 가지 핵심 기능으로 구성된다.

- 식별(Identify): 자산, 비즈니스 환경, 거버넌스, 위험 평가, 위험 관리 전략
- 보호(Protect): 정보 보호 정책, 접근 통제, 데이터 보안, 교육
- 탐지(Detect): 이상 탐지, 보안 모니터링, 사건 분석
- 대응(Respond): 사건 대응 계획, 의사 소통, 분석, 완화, 개선
- 복구(Recover): 복구 계획, 개선 활동, 커뮤니케이션 복구

NIST CSF 1.0의 주요 특징으로는 조직의 규모와 복잡성에 맞게 조정할 수 있는 유연성과 확장성, 위험 평가 및 우선순위 설정을 지원하는 위험 기반 접근, 현재 상태 평가와 목표 설정 및 개선 계획 수립을 돕는 성숙도 평가, 국제 표준과 지침을 통합한 표준화 그리고 이해관계자와의 효과적인 의사소통을 지원하는 도구가 있다.

2.2.2. CSF v1.1

NIST CSF v1.1[5]은 2018년 4월 16일에 발표되었다. 급변하는 사이버 보안 환경과 최신 기술 발전, 그리고 새로운 위협에 효과적으로 대응하기 위해 CSF의 개선이 요구되었다. 기존의 NIST CSF v1.0은 공급망 보안 이슈와 같이 최신 기술의 등장과 함께 수반되는 새로운 위협에 대응하기 위해 업데이트가 필요했다. NIST CSF v1.1의 주요 변화는 다음과 같다. 첫 번째로 기능의 확장으로 기존 다섯가지 프레임워크의 기능을 확장하여 최신 위협과 기술 발전을 반영하였다. 두 번째로 새로운 카테고리 추가로 인증, 인증 관리, 암호화 등 새로운 보안 카테고리와 서브 카테고리가 추가하였다. 세 번째로 자원 관리 강화를 통해 조직이 사이버 보안 자원을 효과적으로 관리하고 보안 태세를 평가할 수 있도록 하는 도구와 지침을 추가 하였다. 네 번째로 협력 및 정보 공유 강화를 통해 정부, 민간 부문, 국제 파트너 간의 협력을 강화하여 사이버 보안 정보를 공유하고 대응할 수 있는 메커니즘을 마련하였다. 마지막으로 프레임워크 구현 지원으로 조직이 프레임워크를 효과적으로 구현할 수 있도록 지원하는 추가 자료와 도구를 제공하고 있다.

2.2.3. CSF v2.0

NIST CSF v2.0[6]은 2024년 2월 26일에 발표되었다. Biden 정부로 넘어오면서 행정명령 이후 제로트러스트 철학이 추가된 프레임워크로 개발되었다. 해당 CSF의 개선점은 첫 번째로 프레임워크 기능의 확장으로 기존의 기능을 강화하고 거버넌스(GOVERN)라는 새로운 대 분류 수준의 기능을 추가하였다. 둘째, 세분화된 프로파일과 티어로 조직의 사이버 보안 상태를 보다 세부적으로 평가하고 관리할 수 있도록 지원하고 있다. 세 번째로 온라인 리소스 통합을 통해 Implementation Examples, Informative References, Quick-Start Guides 등을 포함한 다양한 온라인 리소스를 제공하여 프레임워크 구현을 지원한다. 네 번째로 위험 관리 통신 및 통합 강화를 통해 조직 내외부의 이해 관계자와 사이버 보안 위험에 대해보다 효과적으로 소통하고 통합할 수 있는 방법을 제시하고 있다. 다섯 번째, 기술 변화 반영으로 클라우드, 모바일, AI 시스템 등 최신 기술과 환경 변화를 반영한 보안 프레임워크를 제공한다. 마지막으로, 지속적인 개선 및 업데이트를 통해 사용자의 피드백을 통합하여 프레임워크를 지속적으로 업데이트하고 개선할수 있는 환경을 제공하고 있다.

2.3. 미국 주요 기업 변화

2.3.1. Microsoft

Microsoft에서는 MCRA (Microsoft Cybersecurity Reference Architecture)[7]라는 새로운 프레임워크를 제시하고 있다. MCRA는 제로 트러스트 원칙에 기반

하여 조직의 보안 태세를 강화하기 위해 ID 및 액세스 관리, 위협 보호, 정보 보호, 보안 관리를 통합한 포괄적인 사이버 보안 프레임워크로 정의할 수 있다. 이 프레임워크는 제로 트러스트의 세 가지 주요 원칙을 명확하게 준수하고 있음을 보여준다. 첫 번째 원칙인 명확히 검증하라(Verify Explicitly)는 다단계 인증(MFA)과 조건부 액세스 정책을 사용하여 사용자와 장치의 신원을 지속적이고 동적으로 검증하는 것을 의미한다. 이를 통해 접근 결정이 최신 상황과 위험 분석에 기반하도록 한다. 두 번째 원칙인 최소 권한 접근(Least Privilege Access)은 엄격한 접근 통제를 구현하여 사용자와 애플리케이션에 필요한 최소한의 권한만 부여하는 것을 의미한다. 역할 기반 접근 제어(RBAC)를 통해 이러한 원칙을 준수한다. 세 번째 원칙인 침해 가정(Assume Breach)은 이미 손상이 발생했다고 가정하고, 이에 따라 적극적인 보안 조치를 취하는 것을 의미한다. 여기에는 지속적인 모니터링, 위협 탐지, 사고 대응 계획이 포함되어 있어 신속하게 보안 사고를 식별하고 완화할 수 있다. 이러한 제로 트러스트 원칙을 준수함으로써 MCRA는 지속적인 검증, 최소 권한 접근, 그리고 적극적인 위협 관리가 가능하게 하여 현대의 사이버 위협에 효과적으로 대응할 수 있는 견고한 보안 환경을 조성한다. MCRA는 또한 다양한 산업과 조직에 적용될 수 있는 유연성과 확장성을 제공하여, 사이버 보안 전략을 보다 효율적이고 체계적으로 관리할 수 있도록 돕는다.

2.3.2. Cisco

Cisco는 보안 프레임워크로 SASE(Secure Access Service Edge)[8]를 제시하고 있다. SASE는 클라우드 기반 네트워크 보안 아키텍처로, 네트워크 보안 및 WAN 기능을 통합하여 사용자와 디바이스가 전 세계 어디서나 안전하고 최적화된 액세스를 가능하게 한다. SASE의 주요 구성 요소에는 SD-WAN(Software-Defined Wide Area Network), 클라우드 기반 보안 서비스와 제로트러스트 기술을 통합하였으며 전 세계에 분산된 클라우드 데이터 센터를 통한 클라우드 네트워크가 포함된다. 이러한 요소들은 중앙에서 통합적으로 관리되며, 동적 확장과 사용자 경험 최적화를 통해 원격근무 환경에서도 일관된 네트워크 성능과 보안을 제공한다. 또한, 초기 투자 비용과 운영 비용을 절감할 수 있는 비용 효율성을 갖추고 있어, 현대의 분산된 비즈니스 환경에서 안전하고 효율적인 네트워크 운영을 가능하게 한다.

2.3.3. OpenGroup

OpenGroup은 IT 표준 및 인증 프로그램을 개발하고 보급하는 글로벌 표준화 기관이다. OpenGroup에서는 여러 민간 기관을 포함한 다양한 기관에서 사용할 수 있도록 Zero-Trust 가이드라인을 제안한다. OpenGroup에서 제안하는 Zero-Trust는 현재 2.0[9]까지 발행되었다. Zero Trust 2.0은 다음과 같은 주요 특징을 갖는다. 첫 번째로, 실시간 동적 접근 제어를 통해 사용자와 기기의 행위를 분석하고 상황에 따라 접근 권한을 동적으로 부여하거나 차단한다. 두 번째로, 세분화된 접근 권한 관리가 가능하여 리소스별로 매우 정밀한 접근 정책을 설정할 수 있다. 세 번째로, 지속적인 모니터링과 분석을 통해 네트워크와 시스템 활동을 실시간으로 감시하고 이상 징후를 신속하게 탐지하여 대응할 수 있다. 네 번째로, 다양한 보안 솔루션이 통합된 통합 보안 플랫폼을 제공하여 보안 정책의 일관성과 관리 효율성을 높인다. 마지막으로, 적응형 보안을 통해 실시간으로 변화하는 위협 환경에 대응하고 동적으로 보안 정책을 적용한다. 이러한 특성 덕분에 Zero Trust 2.0은 현대의 사이버 보안 환경에서 효과적인 솔루션으로 인정받고 있다.

2.3.4. NIST와 민간 업체의 ZT 정책 차이점

공통적으로 모든 제로트러스트 정책은 신뢰하지 않음, 최소 권한 원칙, 지속적인 검증에 대한 철학은 모두 가지고 있다. 하지만 NIST와 OpenGroup은 기술 중립적으로 표준 기반의 접근 방식을 통해 다양한 산업에서 적용가능한 참조 아키텍처와 지침을 제공한다. 어떤 기관에서 사용될지 모르니 범용적인 지침을 제공하는 것이다. 반면 Microsoft와 Cisco의 경우 자사의 기술에 통합할 수 있도록 설계하였으며 사용자 인증, MFA, 조건부 엑세스 정책 등 사용자 중심의 접근방식을 채택한다. 이처럼 민간기업에서는 비즈니스 및 엔터프라이즈, 보안 아키텍처와의 통합을 중점으로 둔다.

Ⅲ. 우리나라 변화

3.1. 망분리 환경

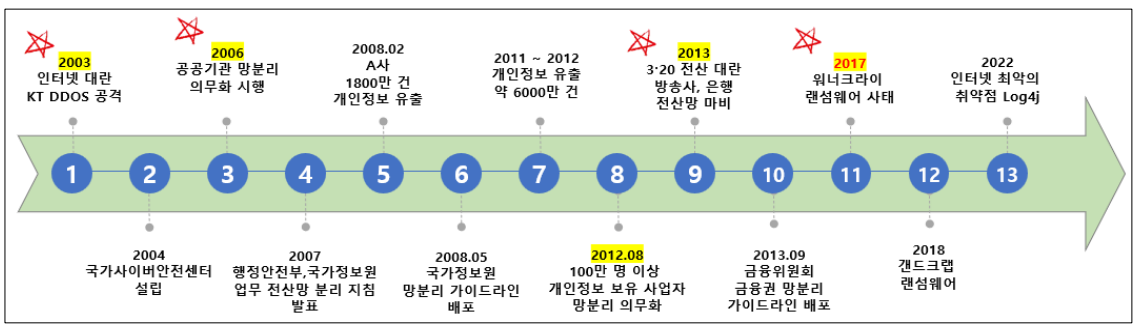
우리나라의 경우 인터넷 대란 이후 보다 현실적인 보안체계를 구축해왔다. 우리나라가 선택한 최적의 기술은 네트워크 및 업무의 물리적인 분리를 통한 보안성 강화였다. 현재 망분리 환경은 우리나라의 많은 기업과 기관이 기본으로 구축하고 있는 보안환경이 되었다. 망분리 환경을 도입하게 된 결정적인 사건들이 발생하였도, 최초로 IT 보안에 대한 경각심을 가지게 된 사건은 2003년 1월 25일 발생한 인터넷 대란으로 KT DNS 서버가 DDoS 공격을 당하면서 전국 인터넷망이 마비되는 사건이 일어났다. 해당 사건으로 경각심을 가진 우리나라는 2004년에 국가사이버안전센터를 설립하였으며 2006년에는 공공기관 망분리 의무화가 시행되었다. 그리고 2008년부터 2012년까지 민간기관에서 개인정보 유출이 심해지자 2012년 8월 100만명이상의 개인정보 보유 사업자는 망분리가 의무화 되었다. 그리고 2013년 3월 20일 북한 정찰총국 소행으로 방송사와 금융권의 전산망이 마비되는 사건이 발생한다. 해당 사건 이후 금융권 망분리 가이드라인이 배포되면서 금융권 까지 본격적으로 망분리 환경을 구축하게 된다. 최근 당야한 해킹공격피해 사례가 급증 하고 있지만, 외국 기관 대비 우리나라 공공 및 금융기관등 망분리 환경을 구축한 기관에서의 해킹 피해 사례는 매우 적은 실정이다. 이는 내부 악성코드를 통해 외부로의 자료유출을 시도하더라도 망연계 장치를 통한 TCP/IP 세션을 만들 수 없기 때문에 보안 담당자의 정책설정에 실수를 하지 않는다면 현실적으로 안전한 시스템으로 인정받고 있다.

3.2. 보안 설계 방향

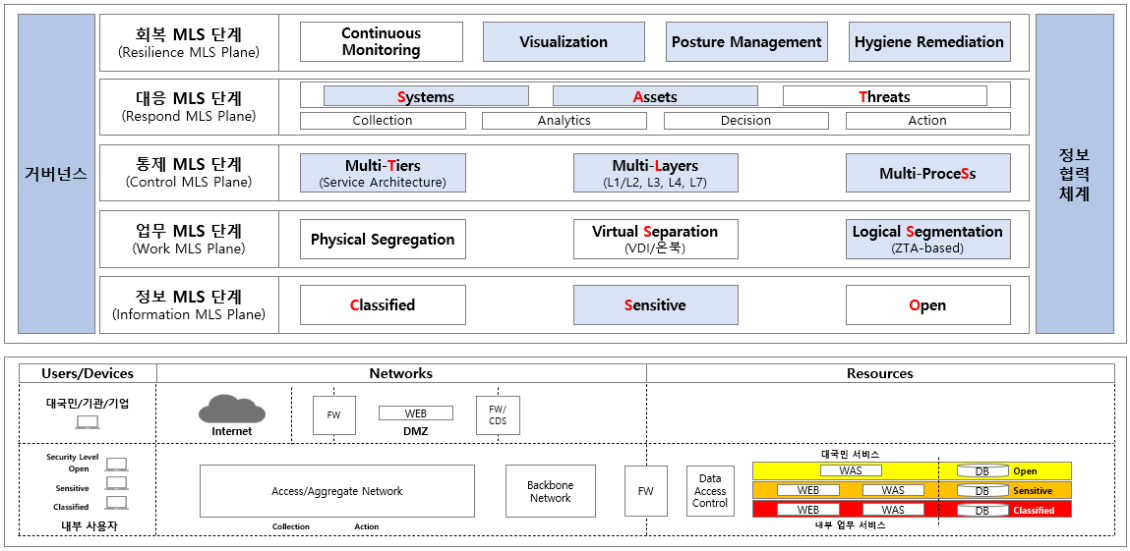
코로나 팬데믹 이후로 원격근무와 클라우드 업무 환경으로 전환되면서 리모트 엑세스 기술이 필수적으로 발생한다. 현재 망분리 기술은 이러한 외부 접속을 고려한 기술이 아니기 때문에 이에 대한 보강 기술이 요구된다. 이에 대표적인 사례가 미국이다. 미국은 망분리 제도 개선의 핵심 기술인 제로트러스트를 구현하고 있는 국가이다. 미국 연방정부 차원으로 NIST, CISA, DoD, NSA 등 여러 조직이 데이터나 통제에 대한 거버넌스는 물론 관련 체계를 어떻게 갖출지에 대한 새로운 프레임워크를 만들어 가고 있다. 미국은 제로트러스트 타임라인은 다층보안 개념이 적용돼 있다는 특징이 있다. 현지 기업들은 이러한 프레임워크와 문서를 기반으로 자체적으로 통제 항목을 갖추고 있다. 우리나라 보안 예방 관련 문서로는 국가정보보안기본지침[10], 원격근무 가이드, 클라우드 가이드, 공급망 보안 가이드[11] 등이 있다. 하지만 민간은 물론 기관에서 보안 프레임워크를 도입하려 해도 설계, 발주, 도입, 구축, 운영, 대응, 복원까지 전 생애주기를 아우르는 라이프사이클 개발이 쉽지 않다. 이러한 문제를 해결하기 위해, 다중계층보안(MLS, Multi-Level Security) 프레임워크를 제안한다. MLS는 보안정책을 통해 다양한 보안 수준을 가지는 정보를 보호하는 시스템이다.

3.3. MLS 프레임워크

MLS는 기본적으로 보안정책을 통해 다양한 보안 수준을 가진 정보를 보호하는 시스템이다. 각 보안 계층이 서로 다른 기밀성 및 무결성 가질 수 있어 기존 망분리 환경에 해당 프레임워크를 도입하면 수월하게



[그림 1] 망분리 타임라인



[그림 2] MLS Framework 초안

안전한 보안 환경을 구축할 수 있다. 해당 MLS 환경에 대해서는 특정 업무에 대한 사이버 보안 맵, 특정 업무의 사이버 보안을 위한 포지셔닝 서비스, 통제 네비게이터가 개발이 필요해 보인다. 종합적으로 사이버 위협으로부터 데이터를 보호하기 위한 엔드투엔드(End-to-End) 보안서비스의 종합적인 접근 방식이 필요하다. 해당 정책을 고려하고 기존 망분리 환경을 개선한 MLS 프레임워크 초안을 그림 2와 같이 제시 한다. 이는 정보보안 수준에 맞는 역할 및 상황 기반 업무의 데이터 흐름 통제·대응을 보여준다. MLS 프레임워크 거버넌스는 정보, 업무, 통제, 대응, 복원 단계로 이뤄진다. 가장 기초인 정보 MLS 단계에서는 기밀정보(Classified), 민감정보(Sensitive), 공개정보(Open)로 구분된다.

기본적인 방향은 기밀정보, 민감정보, 공개정보이며 업무환경도 비밀업무환경, 민감한 업무 환경, 오픈 환경등 여러 가지를 고려한다. 우리나라는 미국과 달리 이미 망분리가 돼 있는 환경이기에, 망분리 환경에 맞는 정책결정지점(PDP)과 정책시행지점(PEP) 구조가 설계되야 한다.

Ⅳ. 결 론

본 논문에서는 제로트러스트 기반 사이버보안 프레임워크 설계 방향을 제안하였다. 우리나라의 경우, 과거의 주요 사이버 보안 사건들로 인해 망분리 환경이 기본적인 보안 체계로 자리 잡았다. 그러나, 코로나 팬데믹 이후 원격근무와 클라우드 기반 업무 환경으로의 전환은 기존 망분리 환경의 업무단위, 서비스단위, 통제항목 단위의 보안 체계에는 한계가 있었다. 본 논문에서는 우리나라의 기본 망분리 환경의 장점을 살리면서 사이버보안기능을 향상시키기 위한 신 보안 프레임워크 설계(MLS)에 대한 초안을 제시하였다. 향후 연구방향으로는 거버넌스 및 정보협력체계에 대한 세부 항목이 추가된 MLS 프레임워크를 설계하고자 한다.

참 고 문 헌

[1] NIST, “Zero Trust Architecture”, SP 800-207, Aug 2020

[2] Whitehouse, “Executive Order on Improving the Nation’s Cybersecurity”, EO14028, May 2021

[3] CISA, “Improving Critical Infrastructure Cybersecurity”, EO 13636, February

[4] NIST, “Cybersecurity Framework Version 1.0”, Feb 2014

[5] NIST, “Cybersecurity Framework Version 1.1”, April 2018

[6] NIST, “Cybersecurity Framework Version 2.0”, Feb 2024

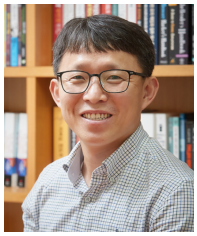
[7] Microsoft, “Microsoft Cybersecurity Reference Architectures”, Dec 2023

[8] Cisco, “Cisco Security Reference Architecture”, Mar 2021
[9] Opengroup, “Zero Trust Core Principles”, April 2021
[10] 국가사이버안보센터, “국가정보보안지침”, Nov 2021
[11] 한국인터넷진흥원, “SW 공급망 보안 가이드라인 1.0” May 2024

<저 자 소 개>

신 인 준 (In June Shin)
2023년 2월 : 대구대학교 컴퓨터공학부 학사
2023년 2월~현재 : 대구대학교 IT융합공학과 석사과정
<관심분야> 통신공학, 정보보호, 네트워크 보안

권 상 오 (Sang Oh Kwon)
1996년 2월 : 금오공과대학교 전자계산기공학과 졸업
1996년 3월 : ㈜씨에스티 수석연구원
2012년 2월 : ㈜아비스 이사
2020년 9월~현재 : ㈜포위즈시스템 수석연구원
<관심분야> 네트워크보안, 클라우드, SDN/SDP/NFV, QoS/QoE



김 창 훈 (Chang Hone Kim)
종신회원
2001년 2월 : 대구대학교 컴퓨터공학부 학사
2003년 2월 : 대구대학교 컴퓨터정보공학과 석사
2006년 8월 : 대구대학교 컴퓨터정보공학 박사
2007년 9월~현재 : 대구대학교 컴퓨터정보공학부 교수
<관심분야> 통신공학, 정보보호, 네트워크보안, 클라우드, SDN/SDP, 제로트러스트