중소규모 대학의 효율적 보안 강화를 위한 제로 트러스트 관점에서의 접근 방안

이기호*, 유도진**, 이용준***
*극동대학교 인공지능보안학과
**극동대학교 해킹보안학과
***극동대학교 인공지능보안학과
lkheio92@gmail.ac.kr

Approach to Enhancing Security in Small and Medium-Sized Universities through a Zero Trust Perspective

Ki-Ho Lee*, Do-Jin-Yoo**, Yong-Jun Lee***
*Dept. of Artificial Intelligence, Far East University
**Dept. of Hacking Security, Far East University
***Dept. of Artificial Intelligence, Far East University

요 약

디지털 환경의 발전과 함께 중소규모 대학에서는 현재 사이버 위협에 크게 노출되어 있는 상황이다. 대학의 기존 보안 체계에서는 매일같이 늘어가는 위협들을 충분히 방어하기 어려우므로, 본 연구에서는 제로 트러스트 보안 모델의 '아무도 신뢰하지 않는다.'는 원칙을 바탕으로 효율적인 접근 검증 및 보안 강화 방안을 제시하고자 한다. 재학생 5천 명 미만의 중소규모 대학을 대상으로 하고자 하며, 비용 효율적인 오픈소스 솔루션을 통해 제로 트러스트 모델을 적용하는 방안을 제안한다. 이를 통해 중소규모 대학은 제한된 예산과 인력 내에서 네트워크 접근제어(NAC), 침입탐지 시스템(IDS), 다단계 인증(MFA) 등을 솔루션을 활용해 보안 수준을 크게 향상 시킬 수 있다.

1. 서론

디지털 환경의 발전과 함께 교육기관에 대한 사이버 위협은 나날이 증가하고 있다. 많은 대학들이 기존의 전통적 보안 체계를 활용하고 있으나, 내부 네트워크만을 신뢰하는 접근 방식은 더 이상 효과적이지 않다. 이에 대해 제로트러스트 보안 프레임워크는 문제를 해결하기 위해'아무도 신뢰하지 않는다.'는 원칙을 대전제로 모든 접근을 엄격히 통제하고 모니터링할 수 있는 효과적인 보안 수단이다.

본 연구는 재학생 5천 명 미만의 중소규모 대학을 대상으로 제로 트러스트 보안 모델의 적용 방안을 제안하여 제한된 자원 속에서도 효율적으로 사이버 위협에 대응할 수 있는 방안을 모색하고자 한다. 이를 통해 중소규모 대학들이 직면한 보안 문제를 해결하고 안전한 교육 및 연구 환경을 구축하는 데 기여하고자 한다.

2. 중소규모 대학의 보안 현황

2.1 기존 보안 체계의 현황과 문제점

중소규모 대학의 기존 보안 체계는 예산과 인력의 부족으로 인해 전반적으로 취약한 상태라고 볼 수 있다. 부산대학교의 '대학 정보화 현황 조사 및 분석에 관한 연구', 충남대학교의 '정보보호수준 향상방안에 관한 연구', 2023년의 실제 충북지역 중소규모 대학(재학생 3천 명)의 교육부 정보보호 수준 진단 사례를 통해 확인해 보았을 때 중소규모 대학에서 주요한 5개의 문제를 선별한 결과는 아래 [표 1]과 같다.

[표 1] 중소규모 대학의 보안 현황

항목	현황	문제점
보안 인프라	서버 보안 도입 비율 40.95%	네트워크 침입에 취약
정보보호 인력	80.53%의 대학에 정보보호 전담 인력 없음	기존 인력의 정보보호 업무 겸직 수행으로 인한 대응 한계
보안 예산	정보화 예산 대비 정보보안 예산은 평균 3.55% 낮음	예산 부족으로 인해 최신 보안 시스템 도입 어려움
사용자 보안 인식	정보보안 자격 소지자 비율 21.76% 일반 직원 대상 보안 교육 시행률 저조(오프라인)	개인정보 유출에 대한 경각심 및 악성코드 감염 위험에 대한 대응 능력 부족
기술 지원	VPN 도입 비율 52.38%	원격 교육 및 연구 환경의 증가에 따른 취약성 증가

위 표와 같이 중소규모 대학은 예산과 인력의 한계로 사이버 위협에 효과적인 대응을 하기 어려운 상황이다. 이러한 문제의 효과적인 해결을 위해 제로 트러스트 보안의 관점에서 다양한 위협에 대응할 수 있는 유연성과 확장성을 갖출 필요가 있다고 보았다.

3. 중소규모 대학을 위한 제로 트러스트 적용 방안

3.1 다단계 인증(MFA)솔루션 적용

제로 트러스트의 '아무도 신뢰하지 않는다.' 는 원칙을 중소규모 대학에 적용하기 위해서는 비용을 최소화하면서도 보안을 강화할 수 있는 무료 솔루션과 오픈 소스 등 기존 시스템을 활용하는 것이 중요하다.

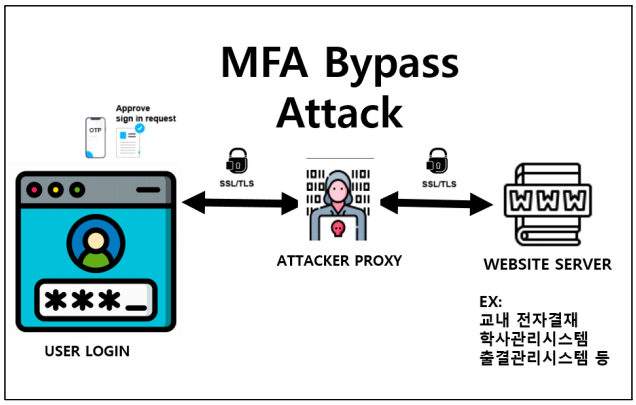
그 중에서도 규모가 작은 대학은 무료 MFA 솔루션으로 Google Authenticator, Microsoft Authenticator, Authy 등을 활용할 수 있다. 이들은 2FA(2-Factor Authentication) 방식을 제공하며 사용자에게 등록된 기기에서 일회용 인증 코드를 생성하고, 서버와 사용자 기기 간의 시간 기반 일회용 비밀번호 프로토콜을 통해 작동한다.

MFA 솔루션의 핵심은 사용자의 첫 인증 이후 추가 인증을 요구하는 정책, 그리고 사용자와 인증 서버의 시간에 기반한 동기화 방식을 통해 OTP가 일정 시간마다 갱신된다는 것에 있다.

이러한 MFA 솔루션을 통해 학생은 학사관리 시스템, 교직원은 전자결재나 업무용 학사 시스템 등에 접근할 때마다 다단계 인증을 거치게 되므로 내부 사용자에 대한 보안 검증을 강화할 수 있다.

이는 제로 트러스트 원칙인 끊임없는 검증을 구현하는 중요 수단으로 작용할 것이며, 대학은 특별한 비용 없이도 강력한 계정 보호 수단을 확보할 수 있다. 또한, 사용자 계정 탈취 방지, 정보 유출 최소화, 내부 시스템 보호 등 다양한 보안 효과를 가져올 수 있을 것이다.

MFA 솔루션은 일반적인 수준의 보안을 충족시켜줄 수 있고, 없는 것 보다는 사이버 침해 시도에 있어 훌륭한 대책이 될 수 있다. 다만, 아래 그림[1]과 같이 사용자가 로그인 절차를 거치는 동안 공격자가 중간에 개입하여 다단계 인증(MFA) 프로세스를 우회하는 경우 사용자의 계정이 탈취될 위험이 존재한다.



[그림 1] MFA 우회 공격(MFA Bypass Attack)

MFA 솔루션 사용자는 일반적으로 MFA를 요구하는 웹사이트인 출결 관리 시스템, 학사관리시스템 등 대학 내의 교육 및 연구, 업무 등에 관련한 웹사이트에 로그인을 시도한다. 로그인을 시도할 때, 사용자는 공격자가 제공한 피싱 사이트를 통해 ID와 비밀번호를 입력하고 이후 추가 인증 요청을 받는다. 이 때, 사용자가 접속한 페이지는 공격자의 프록시 서버로 중계되어 사용자와 웹서버 간의 통신이 프록시를 통해 이뤄지게 된다. 공격자는 프록시를 이용해 사용자가 입력한 로그인 정보를 웹서버로 전달하면서 동시에 사용자의 인증 세션을 도용할 준비를 한다.

웹서버는 사용자에게 다단계 인증 요청을 전송하고, 사용자는 휴대폰이나 OTP(One-Time Password) 앱을 통해 인증 요청을 승인한다. 사용자가 MFA를 승인하게 되면 인증이 공격자의 프록시 서버를 통해 웹서버로 전달되어 정상 접근이 허용된다. 이러한 방식은 사용자에게 정상적인 인증 과정으로 보이지만, 실질적으로는 공격자가 사용자와 웹서버 간의 인증을 도용하여 불법 접근을 수행하는 것이다.

일반적으로 MFA 우회 공격은 사용자가 푸시 알림을 허용하도록 유도하는 방법을 사용하므로, 단순 푸시 기반 MFA만으로는 위험할 수 있다. 가장 좋은 방법은 물리적 인증키를 추가하는 것일 수 있으나, 우선 시 되어야 할 것은 나날이 발전하는 피싱 수법에 대한 경각심을 가질 수 있도록 보안 교육

을 진행하는 것이다.

3.2 오픈 소스 기반 시스템 적용(NAC, IDS, IPS)

네트워크 접근제어인 NAC(Network Access Control) 솔루션은 사용자의 역할과 권한을 기반으로 접근을 제한할 수 있다. 오픈 소스 솔루션 중 대표적으로 PacketFence을 활용하면 교내 네트워크에 연결된 기기들의 접근을 신속하게 관리할 수 있으며, NAC를 통해 모든 사용자와 기기에 대해 인증받은 사용자와 기기만 접근을 허용함으로써 내부 보안을 강화할 수 있다.

침입 탐지 시스템인 IDS와 침입 방지 시스템인 IPS는 외부 위협과 내부의 비정상적인 활동을 실시간으로 탐지해 대응할 수 있게 도와주는 시스템이다. 대표적으로 Snort나 Suricata 같은 오픈 소스 기반의 IDS/IPS가 있으며, 이를 통해 학내 네트워크에서 발생하는 트래픽을 분석하고 의심스러운 활동을 탐지할 수 있다.

NAC 오픈소스인 PacketFence, IDS 오픈소스인 Snort, Suricata, IPS 오픈소스인 OSSEC, Wazuh의 경우에는 다양한 네트워크 장비와 호환되어 구축이 용이하고, 설치와 사용이 간단하여 기본적인 개발 지식만 있다면 교내 IT 부서에서도 충분한 운영이 가능하다. 다만, 초기 설정과 지속적인 업데이트가 필요하므로, 직원의 기초적인 네트워크 및 시스템 관리 역량이 요구될 수 있다.

4. 결론

4.1 기대효과

중소규모 대학에서 위 솔루션과 같은 제로 트러스트 관점에서의 보안 모델을 적용할 경우, 오픈 소스와 무료 솔루션을 활용하여 제한적인 예산 내에서도 안정적인 보안 시스템을 구축하고 유지할 수 있다는 장점이 있다.

또한, 제로 트러스트 원칙을 통해 사용자와 디바이스에 대한 지속적인 검증이 이뤄지도록 할 수 있게 되므로, 교내의 연구와 교육, 업무가 안전하게 진행될 수 있다.

4.2 향후 연구 및 개선 방향

각 대학의 환경에 맞는 제로 트러스트 보안 정책을 수립하고, 정책에 따라 운영하는 프로세스를 개선할 수 있도록 연구가 진행되어야 할 것이다. 특히 다양한 오픈소스 솔루션이 결합하여 학내 요구 사항에 맞는 보안 환경을 구축하고 정기적으로 점검할 수 있는 방향이 마련된다면, 안정적인 업무 및 교육 환경 구축에 이바지 할 수 있을 것으로 보인다.

또한, 제로 트러스트의 관점에서 보안 모델의 실효성을 높이기 위해 사용자인 교직원과 학생을 대상으로 보안 인식 교육을 강화하여 보안 위협에 대한 기본적인 지식과 대응 역량을 높여야 할 것이다.

더불어 기존에 구축된 학내 IT 인프라와 제로 트러스트 솔루션의 호환성을 고려해야 하므로, 대학에서는 불가피한 인력에 대한 지출을 망설이지 말아야 한다.

참고문헌

[1] 부산대학교, “2021년 대학정보화 현황 조사 및 분석에 관한 연구”, 2021년

[2] 충남대학교, “정보보호수준 향상방안에 관한 연구”, 2021년

[3] KISA, “2023 사이버 보안 위협 전망 보고서”, 2023년

[4] 임채원, 공예나, “재택근무 위험평가를 통한 보안 대책 연구”, 한국산업보안연구, 제11권 제1호, pp. 271-299, 3월, 2021년

[5] 윤혜정, 이용우, 임효정, 전삼현, “재택근무 환경 개선을 위한 제로 트러스트 추진 동향 및 실효성 제고 방안 연구”, 한국IT정책경영학회, 제14권 제2호, pp.2915-2916, 4월, 2022년

[6] 이기호, 이용준, 강장묵, “대학 정보보호 강화 방안 연구: 교육부 정보보안 수준진단을 기준으로”, 한국산학기술학회, 제25권 제3호, pp.461-466, 3월, 2024년

[7] 최진명, 김두연, “교육기관의 정보시스템 보안관리 방안 연구”, 컴퓨터교육학회, 제20권 제6호, pp.95-104, 11월, 2017년

[8] 정철기, 안성진, “교육환경에 적합한 정보보호관리체계 개선방안 연구”, 한국컴퓨터교육학회, 제16권 제2호, pp.157-160, 8월, 2012년