경계 기반 망 분리와 제로 트러스트 N2SF의 비교 연구: 스턱스넷 사례를 중심으로

한희수[1], 박기웅[2*]
[1]세종대학교 정보보호학과 학부생
[2]세종대학교 정보보호학과 교수
[1]crowndaisy76@gmail.com, [2]woongbak@sejong.ac.kr

A Comparative Study on Perimeter-Based Network Separation and Zero Trust-Based N2SF: Focusing on the Stuxnet Case

Huisu Han[1], Ki-Woong Park[2]
[1]Dept. of Information Security, Sejong University
[2]Dept. of Information Security, Sejong University

요 약

본 논문은 '스턱스넷(Stuxnet)' 사례를 통해 경계 기반 보안 모델이 갖는 횡적 이동 공격의 취약점을 분석한다. 또한, 제로 트러스트(Zero Trust) 원칙에 기반한 국가 망 보안체계(N2SF)가 데이터 등급별 접근 통제를 통해 어떻게 공격을 원천적으로 차단하고 업무 효율성을 확보할 수 있는지 그 방안을 제시한다.

1. 서론

클라우드와 생성형 AI 활용이 필수적인 현대 IT 환경에서, 외부망 접근을 차단하는 기존의 경계 기반 보안 모델은 업무 효율성을 저해하고 횡적 이동 공격에 취약한 한계를 노출하고 있다. 이에 대한 대안으로 국가정보원은 제로 트러스트 기반의 국가 망 보안체계(National Security Framework, 이하 N2SF)를 제시하였다.

본 논문은 '스턱스넷(Stuxnet)' 사례를 통해 기존 경계 기반 보안의 한계를 심층적으로 분석하고, N2SF가 어떻게 보안성과 업무 효율성이라는 두 가지 목표를 균형 있게 달성하는 효과적인 대안이 될 수 있는지 고찰한다.

2. 경계 기반 보안의 한계

전통적인 네트워크 보안 패러다임은 신뢰할 수 있는 내부망과 신뢰할 수 없는 외부망을 분리하는 경계 기반 보안 모델에 근간을 둔다. 이 모델의 대표적인 구현 방식인 망 분리는 네트워크 경계를 설정하여 외부로부터의 침입을 방어하는 데 모든 보안 역량을 집중한다.

그러나 이 방식은 '내부망은 안전하다'라는 암묵적 신뢰를 전제로 하기에 근본적인 한계를 내포한다. 대표적 사례인 '스턱스넷'은 외부 인터넷과 물리적으로 차단된 폐쇄망 환경을 USB 메모리를 매개로 공격하여 경계를 성공적으로 우회했다 [1]. 이후 악성코드는 '신뢰 영역'으로 간주된 내부망에서 별다른 제지 없이 횡적 이동을 통해 확산되었으며, 이는 망 분리 모델이 내부 위협 확산에 본질적으로 취약함을 시사한다.

더욱이 원격 및 하이브리드 근무가 보편화된 현대 업무 환경에서는 네트워크의 엄격한 분리가 오히려 유연한 접속을 저해하여 업무 생산성을 떨어뜨리는 문제점을 야기하고 있다 [2].

3. 제로 트러스트 패러다임과 N2SF 프레임워크

스턱스넷과 같은 사례를 통해 경계 기반 보안의 한계가 명확해지면서, '절대 신뢰하지 않고, 항상 검증한다(Never Trust, Always Verify)'라는 제로 트러스트 패러다임이 핵심적인 대안으로 부상했다.

* 교신저자

본 논문의 개선을 위해 귀중한 조언과 피드백을 아끼지 않으신 박기웅 교수님께 깊은 감사를 드립니다.

이러한 원칙을 국가·공공기관 환경에 맞게 구현한 프레임워크가 바로 N2SF이다. N2SF의 핵심은 보안의 기준점을 네트워크의 물리적·논리적 '위치'에서 '데이터' 자체의 중요도로 전환했다는 점이다. 이에 따라 기관의 모든 데이터를 기밀(Classified)·민감(Sensitive)·공개(Open) 등급으로 분류하고, 자산의 저장 위치와 무관하게 일관된 보안 정책을 적용한다. 이는 획일적인 차단 위주의 망 분리와 달리, 데이터 가치에 기반한 차등적 통제를 통해 유연성과 보안성을 동시에 확보하는 것을 목표로 한다 [3].

4. 스턱스넷 사례 비교 분석

만약 스턱스넷 공격이 N2SF 환경에서 발생했다면, 공격의 양상은 근본적으로 달라졌을 것이다. 초기 침투 단계, 즉 악성코드가 담긴 USB가 내부 PC를 감염시키는 상황까지는 동일하게 발생할 수 있다. 그러나 결정적인 차이는 악성코드가 횡적 이동을 시도하는 단계에서 나타난다.

N2SF 환경에서 공격의 최종 목표인 산업 제어 시스템(Industrial Control System, ICS)은 최고 등급인 기밀(C) 자산으로 분류될 것이다. N2SF 보안의 근간을 이루는 강제적 접근통제(Mandatory Access Control, MAC) 정책에 따라, C등급 자산에는 사전에 명시적으로 인가된 사용자 및 프로세스만이 접근할 수 있도록 엄격한 규칙이 적용된다 [3]. 따라서 일반 사무용 PC에서 실행된 스턱스넷 악성코드가 C등급의 제어 시스템으로 접근을 시도하는 순간, MAC 정책은 이 비인가된 요청을 원천적으로 차단하게 된다 [4]. 즉, 공격은 최초 감염 지점에서 고립되며, 피해 확산의 핵심 경로인 횡적 이동이 봉쇄되는 것이다.

5. N2SF 도입의 의의 및 기대효과

N2SF는 이처럼 MAC의 강력한 통제 원칙을 통해 스턱스넷과 같은 내부 확산형 공격에 대한 근본적인 방어 체계를 제공한다. 동시에 N2SF는 속성 기반 접근통제(Attribute Based Access Control, ABAC)의 유연성을 결합하여 현대적 업무 환경의 요구사항을 충족시킨다 [3]. ABAC는 사용자의 직책, 접속 위치, 단말기의 보안 상태 등 다양한 속성(Attribute)을 실시간으로 평가하여 접근 권한을 동적으로 부여하는 모델이다 [5]. 이는 더 이상 네트워크 위치만으로 신뢰도를 판단할 수 없는 원격 및 하이브리드 근무 환경에서 정교하고 유연한 보안 정책 적용을 가능하게 한다.

궁극적으로 MAC과 ABAC의 특징이 결합한 N2SF를 적용하면, 데이터의 중요도에 따라 강력한 기밀성을 보장함과 동시에 변화하는 위협과 업무 환경에 유연하게 대응하는 동적 접근 통제를 구현할 수 있다. 이를 통해 기존 망 분리 체제의 경직성을 극복하고 보안성과 업무 효율성이라는 두 가지 목표를 균형 있게 달성하는 효과를 기대할 수 있다.

6. 결론

본 논문은 스턱스넷 사례를 통해 기존 경계 기반 망 분리 모델이 내부 위협 확산에 취약함을 분석했다. 이에 대한 대안으로 N2SF가 데이터 중심 보안과 MAC/ABAC의 결합을 통해 높은 수준의 보안성과 업무 효율성의 균형을 이루는 해결책임을 제시했다. 이러한 분석은 향후 N2SF를 금융, 의료 등 주요 민간 분야로 적용을 확대하기 위한 후속 연구의 필요성을 시사한다.

참고문헌

[1] E. Byres, "The air gap: SCADA's enduring security myth", Communications of the ACM, Vol. 56, No. 8, pp. 29-31, 2013.

[2] T. Abdiukov, "Beyond the Perimeter: Redefining Insider Threat Modeling through Adaptive Behavioral Analytics in Hybrid Work Environments", Iconic Research And Engineering Journals, Vol. 6, No. 2, pp. 393-404, 2022.

[3] 국가정보원, "국가 망 보안체계 보안 가이드라인", 2025.

[4] Y. Jiang, C. Lin, H. Yin, Z. Tan, "Security analysis of mandatory access control model", IEEE International Conference on Systems, Man and Cybernetics, The Hague, Netherlands, 2004, pp. 5013-5018.

[5] V. C. Hu, D. Ferraiolo, D. R. Kuhn, et al., "NIST Special Publication 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations", National Institute of Standards and Technology (NIST), 2014.