중소기업을 위한 Hybrid IDS에 관한 연구

모건웅*, 박상운*, 박명범*, 최현규*, 김우찬*, 김대엽**, 조민재
*수원대학교 정보보호학과
**수원대학교 정보보호학과 지도교수
vv9702@suwon.ac.kr, nbiosupr@suwon.ac.kr, audqja0836@suwon.ac.kr,
kkyyss217@suwon.ac.kr, kwoo2756@suwon.ac.kr, daeyoub69@suwon.ac.kr,
minjae.cho@gmail.com

A Study on Hybrid IDS for Small Medium Business Enterprise

Geon-ung Mo*, Sang-Woon Park*, Myung-Bum Park*, Hyun-Kyu choi*,
Woo-Chan Kim*, DaeYoub Kim*, Minjae Cho
*Dept. of information security, University of Suwon

요 약

20세기 이후 대한민국의 중소기업은 큰 성장률을 보인 반면, 정보보안의 중요성에 대한 인식은 크게 개선되지 않아 중소기업에서 이용하는 시스템에 많은 취약점이 존재한다. 이와 같은 취약점을 악용한 해커들의 다양한 자동화 공격 툴로 인해 보안 사고가 꾸준히 증가하는 추세이다. 그러나 중소기업의 특성 상 부족한 예산과 보안 인력의 부재로 실질적인 대응이 어려운 상황이다. 이 프로젝트는 이러한 예산 및 보안 인력의 부재에도 중소기업에서 사용 가능한 보안 솔루션 개발을 목적으로 한다.

1. 서론

1.1 제안 배경

2000년대 초반부터 시작된 정보화 흐름 속에 점점 정보보호의 중요성이 대두되고 있다. 대기업의 경우 여러 보안 솔루션을 도입하여 안전한 정보보호체계를 구축하고 있다. 그러나 중소기업의 경우, 부족한 예산과, 보안담당 인력 부재 등의 문제로 정보보호체계가 취약하게 구성된 경우가 많기 때문에 중소기업은 대기업에 비해 사이버 공격에 취약할 수밖에 없다.

최근 들어 사이버 범죄자들은 이러한 중소기업의 보안 취약성을 악용하여 중소기업을 공격 표적으로 삼기 시작했다. 사용하기 편리한 자동화 공격 툴이 등장하기 시작하면서 사이버 공격자들이 중견중소기업의 정보보호체계를 공략하기 더 쉬워졌다. 통계에 따르면 우리나라 기업 중 99.2%가 중소기업이고 이 중 78%가 지역에 있는 현실에서 많은 중소기업이 전문인력 부족(77.9%), 예산 부족(74.0%) 등을 호소하고 있고 불행히도 국내 사이버 위협의 97%가 중소기업을 대상으로 하는 것으로 파악된다.[1] KISA가 발표한 2020년 리포트에 따르면 정보보호 인식은 증가했으나, 예산 수립 및 전담 등은 소폭 감소했다. 정보보호 예산을 보유하고 있는 사업체는 36.2%이며, IT예산 중 5% 이상 예산 편성 사업체 1.7%로 조사됐다.[2]

중소기업은 동원할 수 있는 자원의 한계로 인하여 자력으로 필요한 정보보호 수준을 유지하는 것이 매우 어렵다. 중소기업의 경우에는 정보기술을 활용한 경영 지원 업무와 이로 인한 침해 대응 담당자가 없거나 한 사람이 여러 업무를 병행함으로 인해 침해 사고 위협과 대응에 취약할 수밖에 없다.[3]

중소벤처기업부에는 2017년 중소기업 기술 보호 수준 실태조사를 실시하였다. 이 조사에서 드러난 주된 기술유출 발생 원인은 보안 전담 인력 부족(56.0%)과 예산 부족(52.9%)이었다[4].

이와 같은 여러 조사 결과에서 알 수 있듯이, 중소기업들은 인력과 예산 부족 문제로 늘어가는 사이버 공격에 무방비로 노출되고 있다. 기존 보안 장비들은 초기 도입 비용이 높고, 보안 전문 인력의 지속적인 관리가 필요하기 때문에 중소기업에서 이와 같은 시스템을 운영하는데 한계가 있다. 그러므로 중소기업의 예산 여건과 인력 수급 여건에 맞고, 중소기업에 맞는 요구 사항을 적절하게 수용하는 보안 솔루션이 필요하다.

1.2. 중소기업을 위한 보안 솔루션의 요구사항

중소기업의 보안 솔루션 운영 요구사항을 분석한 결과는 다음과 같다.

(1) 보안 시스템 도입 시 적정한 비용이 소요
(2) 상용 솔루션에 상응하는 성능을 제공
(3) 소수의 전문 인력만으로 운용이 가능
(4) 제로데이 취약점 등장 시에도 유연하게 대처 가능
(5) 무중단 운용을 위한 기능 제공

1.3. 중소기업을 위한 보안 솔루션 제안

우리는 이와 같은 요구사항을 모두 충족한 정보보안 솔루션을 제안한다. 증가하고 있는 중소기업 대상 사

이버 공격 피해를 감소시키는 것을 목적으로 하며 제안할 솔루션의 특징은 다음과 같다.

(1) 다중(AI + 시그니처) 패킷 필터링 구현으로 최신 공격 트랜드에 유연하게 대응
(2) 검증된 성능 보장과 비용 감소를 위해 오픈소스 시그니처 공격 탐지 모듈 탑재
(3) 비 전문인력도 쉽게 다룰 수 있는 직관적인 UI 제공
(4) 네트워크 보안지식이 부족한 사람도 쉽게 이해할 수 있도록 탐지 로그를 다양한 방법으로 표현하는 시각화 제공
(5) 공격 탐지 이벤트 로그에 대해 이해하기 쉽도록 설명하며, 대처 방안 또한 제공
(6) 상황 발생 시 타 기관에게 기술 지원을 받을 수 있도록 리포트 제공
(7) 무중단 운용을 위해 자동백업 기능을 탑재

2. 배경 기술

이 섹션에서는 솔루션을 구성하는 필수적인 배경 기술에 대해 설명한다.

2.1. IDS (Intrusion Detection System)

전통적인 방화벽이 탐지할 수 없는 모든 종류의 악의적인 네트워크 트래픽 및 컴퓨터 사용을 감지한다. 취약한 서비스에 대한 네트워크 공격과 애플리케이션에서의 데이터 처리 공격(Data Driven Attack), 권한 확대(Privilege Escalation) 및 침입자 로그인/ 침입자에 의한 주요 파일 접근 / 악성 소프트웨어(컴퓨타 바이러스, 트로이 목마, 웜)와 같은 호스트 기반 공격을 탐지한다.

2.2. Signature Based Network IDS

시그니처 기반 네트워크 공격 탐지 시스템은 시그니처 룰셋(출발지, 목적지, 프로토콜, 바이너리 데이터, 텍스트 데이터 등의 내용이 담김)과 패킷 내용을 대조하여 공격을 탐지한다.

2.3. ML Based AI Network IDS

KDD와 같은 네트워크 패킷 데이터셋으로 침입 탐지 모델을 모델링하여 알려지지 않은 공격들(제로데이 취약점)을 탐지한다.

2.4. Hybrid IDS

Signature Based Network IDS와 ML Based AI Network IDS의 침입 탐지 방식을 혼합한 IDS의 구조를 의미한다.

2.5. CIC flow[4]

네트워크 기반 이상 탐지기에 초점을 맞춰 침입 탐지 시스템을 분석, 테스트 및 평가를 위해 데이터 셋을 생성했다[6]. 최종 데이터 셋에는 Broute-force, Heartbleed, Botnet, Dos, DDos, Web attacks, Infiltration of network from inside 등 공격 시나리오가 포함되어 있다.

2.6. SNORT[5]

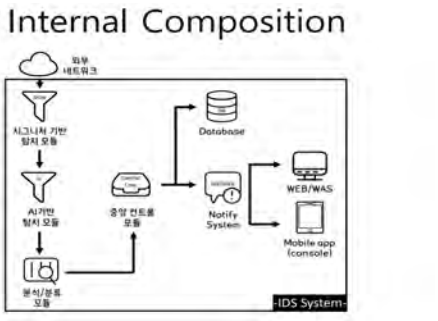
SNORT는 네트워크 실시간 트래픽 분석 및 패킷 로깅 기능을 갖춘 오픈 소스 IDS이다. Snort는 프로토콜 분석 및 콘텐츠 검색/매칭을 수행하고, 사전 정의된 시그니처를 활용하여 침입탐지를 수행할 수 있다 .[3]

2.7. ELK[6]

“ELK”는 오픈소스 프로젝트인 Elasticsearch, Logstash 및 Kibana의 머리글자이다. Elasticsearch는 검색 및 분석 엔진이다. Logstash는 여러 소스에서 동시에 데이터를 수집하여 변환한 후 Elasticsearch 같은 “stash”로 전송하는 서버 사이드 데이터 처리 파이프라인이다. Kibana는 사용자가 Elasticsearch에서 차트와 그래프를 이용해 데이터를 시각화할 수 있게 해준다 [4].

3. 중소기업을 위한 Hybrid IDS

우리는 중소기업을 위한 보안 요구사항을 충족하는 Hybrid IDS 기반의 보안 솔루션을 제시한다. 이 솔루션은 실시간 네트워크 패킷을 입력으로, 1차적으로 시그니처 기반 네트워크 침입탐지, 2차적으로 머신러닝 기반 AI 이상탐지를 실시한다. 두 모듈은 직렬로 배치하여, 중복 탐지로 인한 오버헤드가 발생하지 않도록 한다. 탐지 활동 시 실시간으로 산출되는 이벤트 로그는 ELK스택을 통해 수집되고 가공된다. 중앙화된 로그는 관리자를 위한 웹/앱 애플리케이션을 통해 열람할 수 있다. 알림 시스템은 중앙 저장소를 감시하며, 특이 사항이 있을 경우 관리자에게 알릴 수 있도록 한다. 신속하고 정확한 대처를 위해 대처방안과 대처를 위한 연계 기관을 함께 안내한다. 솔루션을 구성하는데 사용되는 모든 모듈은 비용 절감 효과와 안정성을 위해 오픈소스 모듈을 사용하였다.



(그림1) 개략적인 솔루션 구조도

3.1. 기능

본 프로젝트에서 제안하는 솔루션은 다음과 같은 기능을 갖는다:

(1) 다중 네트워크 공격 패킷 탐지

1차적으로 Signature RuleSet에 따라 공격을 탐지하고, 이를 통과한 패킷들을 AI 공격 탐지 모델로 재검사하여 공격 탐지하도록 하였다. 이를 통해 이미 침입시도로 확정된 패킷을 중복 검사하여 발생하는 오버헤드를 줄인다.

(2) 시그니처 자동 업데이트

공격을 탐지하기 위한 시그니처 정보를 자동으로 업데이트하여 최신 공격 시도를 신속하게 탐지할 수 있도록 한다.

(3) 자동 이벤트 분석 및 분류

공격 시도 이벤트 로그를 분석하고 공격 별로 분류하여, 관리자가 보안 현황을 쉽게 알 수 있도록 가공한다.

(4) 3.1.4. 공격 대처 솔루션 제공

NIST, KISA 등에서 제공하는 공격 정보를 이벤트 로그와 Mapping하여 관리자에게 설명을 제공한다. 이에 대한 대처 방안과 도움을 줄 수 있는 연계 기관을 함께 안내한다.

(5) 탐지 현황 리포트 제공

보호하고 있는 네트워크의 현황을 리포트 형태로 가공하여, 타 기관으로부터 기술 지원을 받을 때 참고 자료로 제출할 수 있도록 한다.

(6) 시스템 자동 백업

시스템에 문제가 생길 시 바로 복구할 수 있도록 자동 백업을 실시한다.

3.2. 구조

본 프로젝트에서 제안하는 솔루션은 다음과 같이 구성된다:

(1) 시그니처 기반 침입 탐지 엔진(Snort)

실시간 네트워크 패킷은 우선적으로 이 모듈을 거친다. 이 모듈은 침입과 관계없는 패킷은 버리고(스트리밍 서비스의 UDP 데이터그램 등), 그 외 모든 패킷을 탐지가 가능한 형태로 전처리한 후, 침입 시그니처와 비교하여 침입여부를 결정한다.

(2) 머신러닝 기반 AI 이상탐지 엔진

이 모듈은 시그니처 기반 탐지 엔진에서 침입으로 탐지된 패킷을 제외한 패킷을 입력으로 받아들여 침입탐지를 수행한다.

(3) 패킷 덤프 모듈(PacketBeat)

이 모듈은 시그니처 기반 침입 탐지 엔진을 거친 모든 패킷을 덤프화하여 파일시스템에 저장한다.

(4) 필요 특징 추출 모듈(Logstash)

이 모듈은 패킷 덤프 모듈에서 저장한 패킷 덤프에서 머신러닝 기반 이상 탐지 엔진에서 사용할 특징을 추출하여 중앙 저장소 혹은 이상 탐지 엔진에 전달한다.

(5) 이상탐지 모델 업데이트 모듈

이 모듈은 중앙저장소에 저장된 침입 탐지된 패킷의 추출된 특징을 활용하여 이상 탐지 모델을 업데이트하고 머신러닝 기반 AI 이상탐지 엔진에 적용한다.

(6) 시그니처 업데이트 모듈

이 모듈은 시그니처 기반 탐지엔진의 침입 탐지 시그니처를 최신 상태로 유지한다.

(7) IDS 내부 저장소

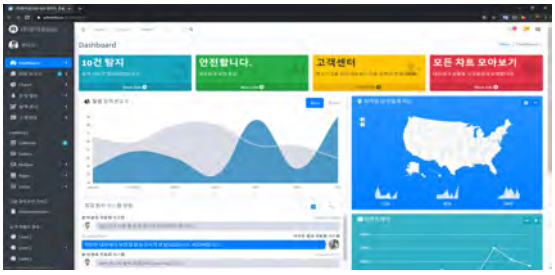
이 모듈은 시그니처 기반 탐지엔진을 통과한 패킷의 추출된 특징을 보관하고, 탐지 이벤트 로그를 보관한다.

(8) 중앙 저장소

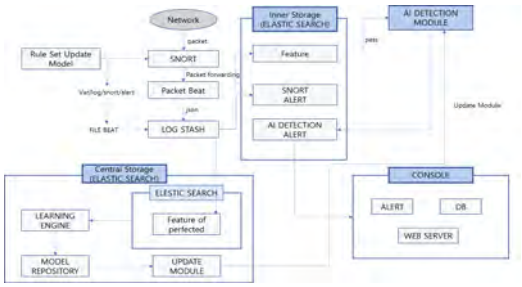
이 모듈은 IDS 내부 저장소에 산재되어 있는 탐지 이벤트 로그를 집약하여 저장하고, 침입 탐지된 패킷의 추출된 특징들을 보관한다.

(9) 관리자 콘솔

관리자는 이 콘솔을 통해 네트워크의 상태와 발생한 이벤트 로그, 알림, 대처방안, 연계 기관 등을 확인할 수 있다. 시각화 요소를 많이 배치하여 정보보호 전문 인력이 아니더라도, 쉽게 접근할 수 있도록 설계하였다.



(그림 2) 관리자 콘솔 프로토타입



(그림 3) 상세 솔루션 구성도

3.3. 솔루션 배치

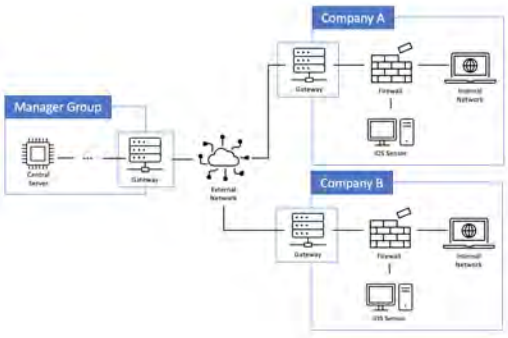
솔루션은 보호 대상 기업에 배치될 IDS 센서와 이들을 관리할 중앙 서버로 나뉜다.

3.3.1 IDS 센서

IDS 센서는 보호 대상 기업 네트워크 내부에 있는 방화벽과 연결된다. 방화벽을 통하는 모든 패킷을 트렁킹하여 침입 탐지 기능을 수행한다.

3.3.2 중앙 서버

중앙 서버는 이 솔루션을 총괄할 역할을 가진 관리 집단의 네트워크에 배치된다. 각 기업에 배치된 IDS 센서로부터 침입탐지 알림, 침입 탐지된 패킷의 추출 특징을 집약한다.



(그림 4) 솔루션 배치도

4. 활용 분야 및 향후 연구 방향

4.1. 활용 분야

보안 솔루션을 위한 중소기업의 투자비용이 감소하여 도입이 쉬워질 것이다. 또한 계속해서 진화하는 공격 트렌드에 시그니처 탐지모듈뿐 아니라 AI 탐지 모델 탑재로 제로데이 존재 시에도 유연하게 대처할 수 있으며 개발된 프로그램 사용이 증가하며 수익이 창출되고 중소기업 보안대상의 증가 효과 역시 얻을 수 있다.

4.2. 향후 연구 방향

해당 솔루션은 중소기업형 보안에 중점을 두고 있다. 그에 맞는 간소한 기능들만을 포함하고 있고 탐지 시스템에 그친다. 후에 IPS와 같이 탐지와 더불어 방화벽 역할을 할 수 있는 탐지 모델 개발을 생각하고 있다. AI 모델의 영역을 넓혀 탐지뿐 아니라 대응 방안의 유연함을 보이는 것이 목적이다.

5. 결론

(중소기업을 향한 사이버 공격은 증가하고 있다. 이로 인해 많은 보안사고가 발생하고 있는데, 가장 큰 원인은 인력문제와 예산문제이다.(목차1.1) 이 가장 큰 원인들을 해결하기 위해, 먼저 중소기업을 위한 보안솔루션의 요구사항을 정리하였다. 요구사항은 적절한 비용, 상용 솔루션 수준의 성능, 소수 인원 운용 가능, 제로데이 취약점 대처, 무중단 운용을 위한 기능이었다.(목차1.2)

우리는 이 요구 사항을 충족하는 보안 솔루션의 구조와 기능, 배치 방법을 제시하였다. 저비용으로 사용 수준에 충족하는 솔루션을 개발하기 위해, 검증된 오픈소스 모듈인 SNORT, ELK, CIC Flow를 활용하였다. 탐지 성능을 향상시키기 위해 하이브리드 형태의 네트워크 패킷 탐지 모듈을 적용하였다. 인력 부족 문제점을 해결하기 위해 AI 기반 패킷 탐지 기능을 적용하고, 공격에 대한 정보를 안내하도록 하였다. 또한 관련 기관에 협조를 요청하기에 유용한 기능을 추가하였다. 제로데이 취약점은 AI 기반 탐지 엔진을 통해 대응하도록 하였다. 무중단 운용 기능을 제공하기 위해 시스템을 신속히 복구할 수 있도록 백업기능을 추가하였다.)

'본 논문은 과학기술정보통신부 정보통신창의인재양성사업의 지원을 통해 수행한 ICT멘토링 프로젝트의 결과물입니다.
'

참고문헌

[1][2][3] [국내] 장상수. (2020). "국내외 중소기업 정보보호 지원 정책 분석 및 개선 검토", 한국인터넷진흥원, 나주, pp.20-22
[4] van de Bijl, Etienne Pieter. Towards Graph-Based Intrusion Detection in Cybersecurity. Diss. Vrije Universiteit Amsterdam, (2020)
[5] Roesh, "Lightweight Intrusion Detection System", Proceedings of LISA: 13th Systems Administration Conference, (1999)
[6] V. Sharma, Beginning Elastic Stack, Springer, (2016)