https://doi.org/10.33778/kcsa.2024.24.1.003

UTM과 ELK Stack을 활용한 소규모 네트워크의 내부망 보안 강화방안

민 송 하*, 이 동 휘**

요 약

현재 사이버 공격과 보안 위협은 지속적으로 진화하고 있으며, 조직은 신속하고 효율적인 보안 대응 방법을 필요로 한다. 본 논문은 Unified Threat Management (UTM) 장비를 활용하여 네트워크 보안을 향상시키고, 이러한 장비를 통해 수집되는 내부망의 로그 데이터를 Elastic Stack (Elasticsearch, Logstash, Kibana, 이하 ELK Stack)을 활용하여 효과적으로 관리하고 분석하는 내부망 보안 강화방안을 제안하고자 한다.

Enhancement of Internal Network Security in Small Networks Using UTM and ELK Stack

Song Ha Min*, DongHwi Lee**

ABSTRACT

Currently, cyberattacks and security threats are constantly evolving, and organizations need quick and efficient s ecurity response methods. This paper proposes ways to strengthen internal network security by utilizing Unified T hreat Management (UTM) equipment to improve network security and effectively manage and analyze the log data of the internal network collected through these equipment using Elastic Stack (Elasticsearch, Logstash, Kibana, her einafter referred to as ELK Stack).

Key words : Internal Network, Security, UTM, ELK Stack

접수일(2024년 02월 20일), 수정일(1차: 2024년 03월 07일), 게재확정일(2024년 03월 20일)

* 동신대학교/정보보안학과(주저자)
** 동신대학교/정보보안학과(교신저자)

1. 서 론

최근 몇 년 동안, 디지털 기술의 급속한 발전과 인터넷의 보편화로 인해 정보 기술과 네트워크의 중요성은 이전보다 훨씬 커졌다. 또한 이와 더불어 네트워크를 악용해 발생하는 사이버 해킹 사고도 꾸준히 늘어나는 추세다.

사이버 해킹의 지능화와 해킹 기술의 다양화 등으로 인해 공격이 더욱 복잡해지고, 확산되고 있으며 많은 보안 침해사고가 발생되고 있다. 이로인해 기업 및 OT시설 등의 인터넷으로 연결된 업무망이 외부의 공격에 직접 노출됨에 따라 내부의 중요 자료가 외부로 유출되는 등 보안관련 피해가 많이 발생하고 있다. 이러한 침해사고를 예방하기 위해 보안 및 내부 데이터 손실 방지와 같은 다양한 방안 및 솔루션이 제시되고 있으며, 원천적으로 중요 정보를 보호하기 위해 업무망(내부망)과 인터넷을 포함한 외부망을 분리할 필요성이 강조되고 있다.

하지만, 많은 솔루션들이 큰 기업의 네트워크를 기준으로 구성되어 있어 소규모 네트워크 입장에서는 경제적 및 기술적으로 많은 부담이 생긴다. 따라서 이러한 문제를 해소하기 위해 본 논문에서는 소규모 네트워크를 대상으로 망분리 솔루션을 제안하였다.

소규모 네트워크의 종류를 크게 [A]스마트공장(OT) 네트워크와 [B]기업네트워크로 나누어 설명하였으며 두 네트워크에 맞는 내부망 보안 솔루션을 제시한 후, 직접 솔루션 환경의 네트워크에 실제 공격자들이 많이 사용하는 공격들로 위협을 가했을 때 로그를 실시간 수집. 분석하여 이를 얼마나 효과적으로 막고 대응할 수 있는지 증명하고자 한다[1][2].

2. 이론적 배경

2-1. 네트워크 보안

네트워크 보안(Network Security)은 컴퓨터 네트워크에서 데이터의 안전성과 기밀성을 보호하는 데 중점을 둔 전문 분야이다. 이는 다양한 위협으로부터 네트워크 시스템과 연결된 장치, 서비스, 데이터를 보호하는 것을 목표로 한다. 주로 민감한 정보나 데이터에 대한 무단 액세스, 변경, 유출, 파괴를 방지하고, 네트워크 서비스의 중단을 막기 위한 방어 수단을 구축하며, 이를 위해 다양한 보안 기술과 전략을 사용한다.

보안 전문가들은 네트워크 보안을 강화하기 위해 다음과 같은 방법을 사용한다. 암호화 기술, 방화벽, 침입 탐지 시스템 (IDS) 및 침입 방지 시스템 (IPS), 접근 제어 및 식별, 보안 업데이트 및 패치 관리 등 이러한 네트워크 보안 조치는 데이터의 무단 접근을 막고, 중요한 정보의 안전성을 보장하여 기업과 사용자들이 안전하게 네트워크를 활용할 수 있도록 돕는다.

2-2. Unified Threat Management (UTM)

UTM은 이러한 도전에 대응하기 위한 핵심 보안 도구 중 하나로, 다양한 보안 기능을 통합하여 제공합니다. 이러한 기능에는 방화벽, 침입 탐지 및 방지 (IDS/IPS), 암호화, 웹 필터링, 바이러스 및 악성 코드 탐지 등이 포함된다. UTM은 네트워크 트래픽을 검사하고 악성 활동을 식별하는 데 중요한 역할을 한다.

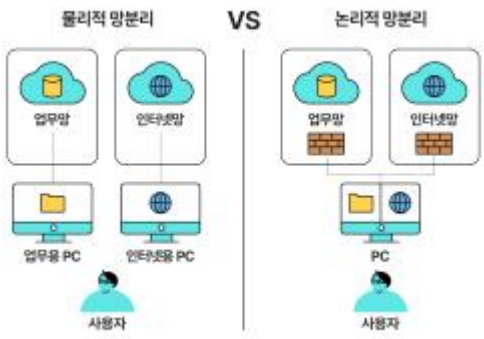
2-3. Elastic Stack (ELK Stack)

ELK Stack은 로그 데이터 수집, 분석 및 시각화에 사용되는 오픈 소스 도구로 Elasticsearch, Logstash, Kibana의 약어이다. Elasticsearch는 대규모 데이터 검색 및 분석을 위한 검색 엔진으로, Logstash는 다양한 소스에서 로그 데이터를 수집하고 변환하는 데이터 파이프라인 도구로, Kibana는 데이터를 시각화하고 대시보드를 생성하는 데 사용된다. ELK Stack은 대용량 로그 데이터를 실시간으로 분석하고 보안 이벤트를 모니터링하는데 이상적인 도구이다[3][4].

2-4. 망분리

망분리는 네트워크나 시스템을 완전히 나누어, 각각이 독립된 영역으로 운영되는 보안 접근 방식이다. 이를 통해 민감한 정보나 시스템을 외부 공격이나 내부 위협으로부터 보호한다. 이 분리는 물리적이거나 논리적으로 이루어질 수 있는데, 물리적 망분리는 물리적 장치를 사용하여 완전히 분리하는 것이고, 논리

적 망분리는 소프트웨어 기술을 활용하여 가상적으로 분리된 환경을 만드는 것이다. 이런 방식을 통해 하나의 부분에서 문제가 생겨도 다른 부분에는 영향을 미치지 않으므로 시스템의 안정성과 보안성을 높일 수 있다[5].



[그림 1] 물리적 망분리와 논리적 망분리 차이

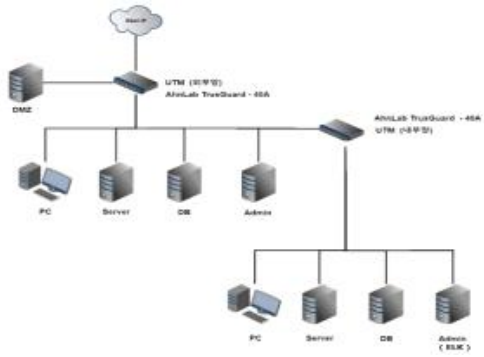
2-5. OT 네트워크 (OT = Operational Technology)

OT 네트워크란 산업 및 생산 시스템에서 사용되는 기술을 가리킨다. OT 네트워크는 주로 산업 시설이나 제조업, 에너지 생산 등과 같은 환경에서 사용되며, 이러한 시스템들을 제어하고 모니터링하기 위한 네트워크이다. 예를 들어, 공장 내의 생산 라인, 발전소의 제어 시스템, 수송 시스템 등이 OT 네트워크에 속한다. 이러한 네트워크는 산업적인 프로세스를 자동화하고 관리하기 위해 사용되며, 효율성을 높이고 생산성을 향상시키는 데 중요한 역할을 한다. OT 네트워크는 정보 기술(IT) 네트워크와는 다소 다른 특징을 가지고 있다. IT 네트워크는 주로 데이터 처리, 정보 교환, 업무 컴퓨팅 등을 목적으로 하지만, OT 네트워크는 물리적인 시스템과 연관되어 있어서 실시간 제어와 모니터링이 중요하다. [2]

3. 네트워크 망분리 솔루션(UTM)

3-1. UTM을 이용한 [A]기업 네트워크 망분리

네트워크 보안을 강화하고 공격자로부터 최대한 내부 시스템을 보호하기 위해서는 망분리 환경이 필요하다. 보통 망분리 환경으로는 논리적 망분리와 물리적 망분리를 흔히 사용하지만 본 논문에서는 소규모 네트워크 환경으로 진행하기에 UTM을 이용해 [그림 2]처럼 내·외부망을 분리하였다.



[그림 2] 기업네트워크 망분리 구성도

기업의 네트워크는 내.외부망을 간단하게 PC, Server, DB, Admin구간으로 구성하였으며 외부망에 UTM장비를 연결해 내부망을 구축하였다. 이와 더불어 외부에서 내부 시스템으로의 직접 액세스를 방지하고, 내부와 외부 네트워크에 각각 맞는 보안 정책을 구성하고 적용할 수 있었으며, 또한 내·외부의 데이터 트래픽을 효과적으로 관리 및 분석, 외부의 공격, DDoS 공격등으로부터 내부시스템의 공격을 최소화할 수 있도록 [그림 3]과 같이 정책을 설정하였다.

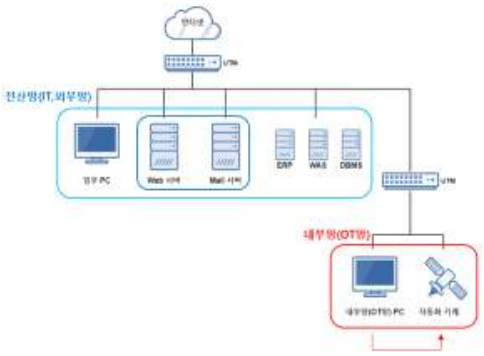
출발지	도착지	서비스	처리방법
all	DMZ	HTTP HTTPS	허용
Admin	DB DMZ PC Server	SSH	허용
DMZ Server	DB	Server-DB접속포트	허용
PC	Default	DNS HTTP HTTPS	허용
all	all	all	차단

[그림 3] 보안장비 정책설정

3-2. UTM을 이용한 [B]스마트공장 네트워크 망분리

과거의 공장 네트워크(OT)환경은 외부와 단절된 폐쇠망으로 운영하여 비교적 안전한 환경을 운영할 수

있었지만, 기술의 발전과 더불어 원격근무 환경이 생겨남에 따라 외부에서 접속이 가능하도록 IT환경이 필요했다. 따라서 외부와 연결된 시점부터 내부 시스템에 접근하려는 악의적인 공격들이 꾸준히 발생하였으며, 이로인해 공장의 내부에 있는 내부 PC의 중요 정보 유출이나 기계 조작과 같은 침해사고가 발생되었다. 그래서 이러한 위협을 최소화하기 위해 공장 네트워크 또한 기업망처럼 UTM을 사용해 내부망, 외부망을 분리시켰다.

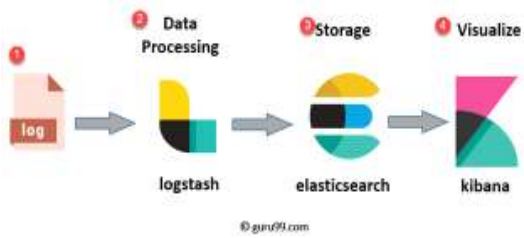


[그림 4] 스마트 공장 네트워크 망분리 구성도

4. 내부망 보안 솔루션(UTM+ELK)

4-1. 내부망에 ELK Stack 시스템 구축

UTM이 로그 데이터를 수집하지만, 데이터 양이 커지면 로그 분석과 관리가 어려워 질 수 있다. 이를 보완하기 위해 대용량 데이터를 처리하고 저장하는데 뛰어난 확장성을 제공하며, 더 많은 로그 데이터를 처리하고 분석할 수 있는 ELK를 구축하였다. 또한, UTM은 실시간 분석 및 경보 시스템을 제공하기 어려운 반면 ELK는 뛰어난 로그 수집 및 검색 기능과 시각적 기능이 뛰어나다.



[그림 5] ELK Stack의 과정

따라서, [그림 5]의 과정처럼 [A]의 경우 내부망의 Admin 구간에, [B]의 경우 기계에 명령을 내리는 내부OT망의 PC구간에 Winlogbeat를 설치하여 외부로부터 들어오는 모든 윈도우 이벤트 로그를 실시간으로 수집할 수 있다. 그리고 이러한 로그들을 Logstash를 통해 데이터를 정제한 뒤, Elasticsearch에 전달하여 각 로그를 분석하여 악성 이벤트 로그를 판별 후, Kibana로 분석 결과를 시각화하여 어떠한 악성 로그가 날라왔는지, 어떤 로그가 많이 날라오는지 등 로그를 실시간으로 관리함으로써 바로 대응할 수 있어 내부 [A]와 [B]네트워크의 내부망 구간의 보안을 강화시킬 수 있었다.

[그림 6] ELK를 통한 로그 시각화

이후, [그림 6]처럼 [A]네트워크의 Admin 구간과 [B]네트워크의 내부망 PC구간에 들어온 로그를 자세히 분석하고 시각화하기에 만약, 이상 로그가 유입될 시 즉시 대응이 가능하다. 또한, UTM의 로그와 ELK에서 수집한 로그를 비교 분석하여 공격자를 파악하는 데 도움을 얻을 수 있다.

4-2. 상관분석 관제

UTM로그를 ELK 분석로그를 시각화하여 분석할 수 있게 ESM(Enterprise Security Management)에 적용하여 전산환경의 장애 발생 시 중앙에사 원격으로 통제하여 처리 및 조치를 취할 수 있도록 전산환경의 성능이나 보안의 취약성을 종합 관리하여 시스템의 안전성을 높여주는 시스템이다. 이 시스템은 여러 보안 장비들의 로그가 한 곳에 모아 관리하리 할

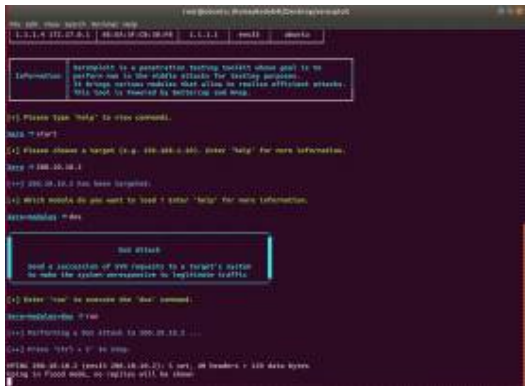
수 있다는 장점이 있고, 이를 본 연구에서 제안한 UTM + ELK를 이용한 버안아키텍처에 적용시켜 보안을 더 강화 시켰다. UTM과 ELk를 통한 내부망 보안 강화 솔루션에서 로그를 수집하고 분석하였는데, 이때 분석된 로그들을 ESM으로 보내어 실시간 관제를 하는 것이다. 이를 통해 보안 위협이 일어나면 실시간으로 모니터링하여 빠른 대응을 할 수 있어 매우 효과적이다. 따라서 본 연구와 병합하여 사용하면 보다 효과적으로 위협로그를 탐지할수 있다.

5. 내부망 보안 솔루션에 대한 검증

본 논문에서 제시한 [A]기업네트워크와 [B]공장 네트워크에 대한 내부망 보안 솔루션(UTM을 이용한 망분리+ELK를 통한 로그 분석 및 모니터링)의 효과를 직접 검증하고자 직접 구축한 [A],[B]네트워크에 악의적인 공격들을 실행하였다. 공격 종류로는 (1). DDOS 공격 ,(2)TCP SYN Flooding 공격, (3).ICMP Flooding Permalink 공격,(4). ARP-SpoofingPermalink 공격을 진행하였으며, 해당 공격을 ELK가 설치되어 있는 [A]의 내부망 Admin구간, [B]의 내부망 PC구간에 보내었다. 이로인해 많은 패킷과 로그가 날라와 피해구간의 ELK에서 해당 이벤트로그를 수집하였고 악의적인 의도로 접근한 공격이라는 것을 시각화하여 보여주었다. 이러한 자료를 보고 어떤 공격인지 분석하고, 다시 피해 입지 않도록 UTM 장비에서 공격에 대응하는 추가적인 정책을 설정하여 2차 피해를 막을 수 있다.

5-1. SYN+ACK 반사 공격

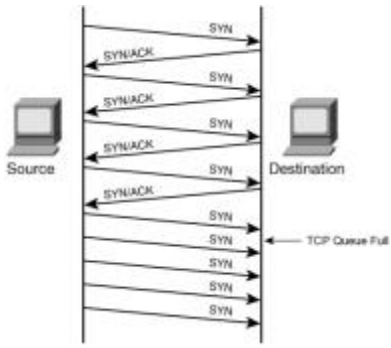
SYN+ACK Flood는 DRDoS의 형태를 지닌 공격방식으로서, 공격자가 피해자의 IP를 도용한 후 반사체로 악용될 서버에 SYN 패킷을 보내고 해당 응답인 SYN/ACK 패킷을 피해자에게 전송하게 하는 공격이다. 피해자는 SYN/ACK패킷을 대량으로 전송 받게 되면 해당 패킷을 처리하기 위해 리소스를 소모하게 되고, 그 과정에서 서버의 부하가 발생되어 정상 사용자들이 접속할 수 없게 된다. 따라서 이러한 공격이 기업과 공장 네트워크에 접근하게 된다면 기업의 서버가 멈추거나 공장의 기계들의 작동이 멈추게 되는 큰 피해가 발생한다. 이를 대응하기 위해 아래 그림과 같이 네트워크에 공격을 해보았고 ELK로 어떻게 탐지되는지 확인하였다.



[그림 7] SYN+ACK 반사 공격

5-2. TCP SYN Flooding 공격

TCP 패킷의 SYN 비트를 이용한 공격 방법으로 많은 연결 요청을 전송해서 대상 시스템이 Flooding (범람)하게 만들어 서비스를 중단시키는 공격방법으로 마찬가지로 기업과 공장 네트워크에 가해지면 매우 위험한 공격이다. 위와 마찬가지로 공격을 진행한 후, ELK로 악의적인 로그들을 확인하였다.



[그림 8] TCP SYN Flooding 공격

5-3. ICMP FloodingPermalink 공격

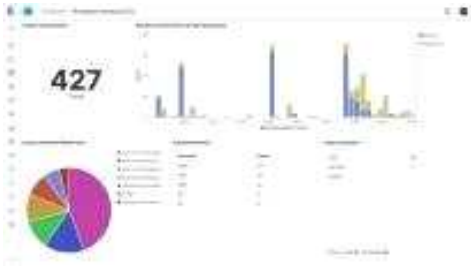
공격자가 다량의 ICMP 패킷을 서버로 전송하여 서버가 보유한 네트워크 대역폭을 가득 채워 다른 정상적인 클라이언트의 접속을 원활하지 못하도록 유발시키는 공격으로위와 마찬가지로 공격을 진행한 후, ELK로 악의적인 로그들을 확인하였다.

[그림 9] ICMP FloodingPermalink 공격

5-4. ARP SpoofingPermalink

클라이언트의 MAC 주소를 중간에 공격자가 자신의 MAC 주소로 변조하여 마치 서버와 클라이언트가 통신하는 것처럼 속이는 공격으로 위와 마찬가지로 공격을 진행한 후, ELK로 악의적인 로그들을 확인하였다.

[그림 10] ARP SpoofingPermalink 공격



[그림 11]. 공격에 대해 ELK에서 탐지

5. 결 론

제안된 논문은 디지털 기술과 인터넷의 보편화로 인한 정보 기술과 네트워크의 중요성이 증가함에 따라 사이버 공격 사례가 증가하고 이에 따라 많은 기업과 OT(운영 기술) 시설이 외부 공격에 취약해지며 중요 정보가 유출되는 등의 보안 문제를 바탕으로 만들어 졌으며

본 논문은 이러한 문제를 완화하고 소규모 네트워크에서의 보안을 강화하기 위해 망분리 아키텍처를 제안하였다. 연구는 먼저 스마트공장(OT) 네트워크와 기업네트워크 환경을 직접 구성하였고, 각 중요 네트워크 구간에 ELK시스템을 도입해 효율적인 내부망 관리 환경을 구축하였다. 이후, 제안한 솔루션의 효과를 입증하기 위해 공격 시나리오를 진행하여 해당 공격자들이 사용하는 일반적인 공격에 대한 로그를 실시간으로 수집하고 분석하는 실험을 진행하였다. 이 논문의 목적은 소규모 네트워크에서도 효과적인 보안 아키텍처를 제시하여 중요한 정보를 보호하는 데 기여하고, 제안된 솔루션의 효과적인 동작과 보안 강화에 대한 입증을 통해 산업 현장에서 보안 문제를 완화하고, 정보 유출과 공격으로부터 보호하는 활용 할 수 있다.

참고문헌

[1] 임병하, 정보보안을 위한 망분리 구축에 대한 연구, 전자무역연구, 12(4), pp.1-21, 2014.

[2] 신지호, “OT 보안을 위한 산업제어시스템 EWS의 디지털포렌식 프레임워크 설계”, 순천향대학교 대학원 박사학위논문, 2022.

[3] 홍성대, “Sysmon과 ELK Stack를 이용한 윈도우시스템 사이버 위협 탐지 및 가시성 증대에 관한 연구”, 동국대학교 대학원 석사학위논문, 2020.

[4] 김용준, 손태식, “Sysmon과 ELK를 이용한 산업제어시스템 사이버 위협 탐지”, 정보보호학회논문지, 29(2), 331-346, 2019.

[5] 이동휘, 김홍기, “망분리 네트워크 상황에서 사이버보안 취약점 실시간 보안관제 평가모델”, 융합보안학회논문지, 21권 1호, pp.45-53, 2021.

〔저자소개〕

민 송 하(Song Ha Min)
2023년 동신대학교 정보보안학과 재학

email : thdgk1052@naver.com

이 동 휘 (DongHwi Lee)
2007년 경기대학교 정보보호학 박사
2011년~2012년 University of Colorado Denver, Dept. of Computer Science
2015~현재 동신대학교 정보보안학과 교수
email : dhclub@dsu.ac.kr