지능형지속위협 공격경로차단 위한 정보보호시스템 운영관리 방안

류창수

예원예술대학교

Operation Plan for the Management of an Information Security System to Block the Attack Routes of Advanced Persistent Threats

Chang-Su Ryu

Yewon Arts University

E-mail : twin4me@hotmail.com

요 약

최근 정보보안 환경 변화에 따른 사이버 침해, 사업 기밀유출, 글로벌 보안위협 등의 정보자산에 대한 지속적인 공격으로 위협이 되고 있다. 이는 기존 정보보호시스템에서 대응이 어려운 APT 공격, 우회접근공격 및 암호화 패킷에 대한 공격 등에 대한 탐지와 조치가 가능한 접근에 대해 지속적인 모니터링의 수행이 요구되고 있다. 본 논문에서는 지능형지속위협 공격경로차단을 위한 예방통제(Prevention Control)로 중요한 자산 식별하고 위험을 미리 제거하기 위하여 취약성 분석, 위험분석을 통한 정보통제 정책을 수립하고 서버접근통제, 암호화통신 감시를 통해 탐지통제(Detection Control)를 수립하고 패킷 태깅, 보안플랫폼, 시스템백업과 복구를 통해 교정통제(Corrective Control)를 하여 지능화된 침해대응(Intelligent Violation of Response) 할 수 있도록 정보보호시스템 운영관리 방법을 제안한다.

ABSTRACT

Recent changes in the information security environment have led to persistent attacks on intelligent assets such as cyber security breaches, leakage of confidential information, and global security threats. Since existing information security systems are not adequate for Advanced Persistent Threat; APT attacks, bypassing attacks, and attacks on encryption packets, therefore, continuous monitoring is required to detect and protect against such attacks. Accordingly, this paper suggests an operation plan for managing an information security system to block the attack routes of advanced persistent threats. This is achieved with identifying the valuable assets for prevention control by establishing information control policies through analyzing the vulnerability and risks to remove potential hazard, as well as constructing detection control through controlling access to servers and conducting surveillance on encrypted communication, and enabling intelligent violation of response by having corrective control through packet tagging, platform security, system backups, and recovery.

키워드

Advanced Persistent Threat, Blocking Attack Routes, Information Security System, Prevention Control, Intelligent Violation of Response

Ⅰ. 서 론

최근 정보보안 환경 변화에 따른 사이버 침해, 사업 기밀유출, 글로벌 보안위협 등의 정보자산에 대한 지속적인 공격으로 위협이 되고 있으며, 기존의 정보보호 시스템을 우회하는 공격 기법의 발달로 사용자가 인지하는 못하는 공격 형태로 진화되고 있다[2]. 또한 단일 보안 기술로는 모든

보안위협을 제거할 수 있는 방안을 기대하기는 현실적으로 불가능하다. 현재 발생하고 있는 대부분의 사이버침해가 지능형 지속 위협(Advanced Persistent Threat)공격을 시작하여 공격대상을 찾아 침투하여 주요정보 및 접근권한을 탈취하는 방식으로 사이버침해를 하고 있다[1][3]. 본 논문에서는 지능형지속위협 공격경로차단을 위한 예방통제(Prevention Control)로 중요한 자산 식별하고 위험을 미리 제거하기 위하여 취약성 분석, 위험분석을 통한 정보통제 정책을 수립하고 서버접근통제, 암호화통신 감시를 통해 탐지통제(Detection Control)를 수립하고 패킷 태깅, 보안플랫폼, 시스템백업과 복구를 통해 교정통제(Corrective Control)를 하여 지능화된 침해대응(Intelligent Violation of Response) 할 수 있도록 정보보호시스템 운영관리 방법을 제안한다.

Ⅱ. 관련연구

2.1 지능형지속위협

정교한 수준의 전문 기술 또는 방대한 리소스를 가진 공격자가 명확한 목적을 가지고 특정 대상을 겨냥하여 지능적이고 복합적인 방법을 동원하여 지속적으로 공격하는 위협형태의 목표를 지속적으로 추구하는 것을 말한다. 이러한 APT의 의미는 지능형(Advanced), 지속형(Persistent), 위협(Threat)으로 정의할 수 있다. 일반적인 지능형 지속위협은 정찰, 최초 진입, 권한 상승 및 제어확대, 지속적인 안용의 4가지이며, 지능형지속위협은 그림 1과 같이 4단계이다[1][4-5].

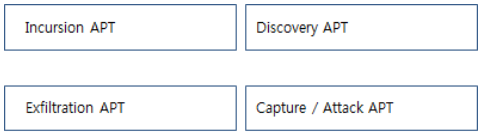

그림 1. 지능형지속위협 단계

2.2 정보보호시스템

허가되지 않은 접근을 통한 정보의 손상이나 변형, 파괴시키는 행위로부터 정보를 보호하고 무결성, 기밀성, 가용성, 인증, 부인방지, 접근통제를 제공하는 시스템을 말한다. 정보보호시스템은 웹 방화벽, 네트워크 접근 통제, 자료유출방지, 정보보호관리체계 강화, 침입차단시스템, 침입방지시스템, DDos 대응, 가상사설망, 서버보안 등을 포함한다[6].

Ⅲ. 정보보호시스템 운영관리방안

3.1 필요성

기존 정보보호기술을 우회하는 공격 기법의 발달로 사용자가 인식 못하는 공격 형태로 진화하고 있고, 암호화된 트래픽과 서버의 정상 접근에 대한 정보 누출 그리고 사용자의 정상적인 트래픽을 이용한 정보 누출, 다중 공격과 같은 기존의 사이버침해 공격대응 방식에서의 한계점을 가지고 있다. 따라서 침해예측 시도에 즉각적인 대응을 지원하는 관리시스템이 필요하다.

3.2 예방통제(Prevention Control)

정보에 대한 영향평가로 중요자산정보에 대한 식별과 위험분석을 통한 취약성 파악과 분석을 통한 정보통제정책을 정의하며 이를 정책에 반영한다.

3.3 탐지통제(Detection Control)

관리자 계정을 관리하고 모니터링 하는 것으로 APT에 대응하려면 최대한 빨리 위협을 감지할 수 있어야 한다. 듀얼 인증관리를 통한 사용자 업무 데이터 관리, 주요보안 사항 로그관리, 주기적 점검사항 로그관리를 통한 비정상적 암호화 패킷 모니터링을 하며 유해사이트 및 P2P 접근관리, 권한 상승, 권한 무단 사용 시도 감시 및 기록을 통한 통제정책을 관리하고 모니터링 한다.

3.4 침해대응(Intelligent Violation of Response)

초기 침입이 발생 했을 때 최적의 전략을 결정하고 관리자 승인을 획득하여 실행하는 것으로 액세스되고 사용되고 이동하며 저장되는 데이터를 파악하여 관련 데이터를 수집하고 침입 탐지 로그와 데이터 식별을 위한 네트워크 기반의 로그 분석과 동시에 네트워크 구조와 접근 통제 리스트를 분석하여 통제정책과 시스템 구성 정보 기반의 회피 기법을 비교 분석을 한다.

3.5 교정통제(Corrective Control)

침입이 발생 했을 때 듀얼인증을 통한 관리자에게 통보하고 로그를 저장하며 네트워크 트래픽을 집중 감시하며 침입자 네트워크를 차단하고 포렌식을 위한 이미지를 보관 및 결과를 통제정책에 반영하고 시스템이미지를 복구하고 보안 에이전트 플랫폼을 동작시킨다.

3.6 정보보호시스템 운영관리

물리적 중요 시설물에 대한 출입통제 및 보호가 이루어지며 관련 중요자료는 백업을 한다. 시스템 관리자는 서버의 업데이트 구성변경 등 설치에 필요한 권한에 한정되어 있으며 보안관련 로그 파일정보는 확인할 수 없으며, 모든 액세스 권한은 읽기 전용으로 보안 관리자 역할을 하며, 감사 담당자는 로그 파일을 볼 수만 있으면 시스템 변경은 수행할 수 없다. 그림 2는 지능형지속위협 공격경로차단 위한 정보보호시스템에 대한 것으로 시스템 관리에서 보안을 분리하며 지능형 지속위험을 제거하기 위한 사고 유형을 분류하고

공격환경과 대응 능력을 부여한 적절한 통합 정보보호시스템을 운영 관리한다.

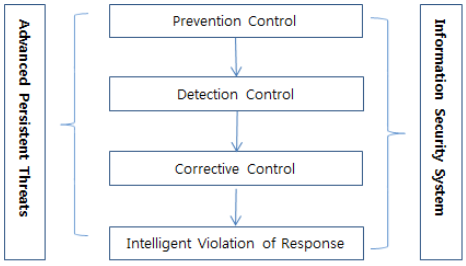

그림 2. 정보보호시스템 도식

Ⅳ. 결 론

APT에 대응하는 데 반드시 필요한 핵심은 방어책이다. 거의 모든 공격의 성공 여부는 권한 있는 아이덴티티에 대한 액세스 권한을 확보하는 중간 단계에 의해 결정된다. 그러므로 지능형지속위협 공격경로차단을 위한 예방통제와 탐지통제를 통해 교정통제된 침해대응 할 수 있도록 정보보호시스템 운영관리 하여야 한다. 향후에는 IoT 기반의 지능형지속위협 공격경로차단 기법에 대한 수집 및 공격에 대한 시스템을 연구할 것이다.

참고문헌

[1] 이문구, 배춘석, “지능형 지속 위협에 대한 차세대 융합 보안 프레임워크”, 전자공학회, 제50권, 제9호, pp. 2336-2343, 2013.

[2] 한국인터넷진흥원, 침해사고대응팀(CERT) 구축/운영 안내서, 2010.

[3] 미래창조과학부, 세계최고의 스마트 안심국가 실현을 위한 사물인터넷(IoT) 정보보호 로드맵, 2014.

[4] 구미숙, 이영진, 악성코드의 유입경로 및 지능형 지속 공격에 대한 대응 방안, 중소기업융합학회, 제5권, 제4호, pp. 37-42, 2015.

[5] CA Technologies, http://www.ca.com

[6] 한국정보화진흥원, 2015 국가정보화 백서, 2015.