위험기반 통합계정관리모델에 관한 연구

강용석*, 최국현**, 신용태***, 김종배****°
*,**,***,****°숭실대학교

A Study on the Integrated Account Management Model

Yong-Suk Kang* · Kook-Hyun Choi** · Yong-Tae Shin***· Jong-Bae Kim****°
*,**,***,****°Soong-sil University
E-mail : *postwin@gmail.com, **khchoi@tsline.co.kr, ***shin@ssu.ac.kr, ****°kjb123@ssu.ac.kr

요 약

최근 해킹 기법의 발전으로 사이버테러를 비롯한 APT공격이 증가하고 있다. 이는 정보기술환경이 모바일, 클라우드, BYOD 기반으로 변화함에 따라 새로운 취약점 또한 증가하고 있기 때문이다. 그러나 기존의 보안 모델은 대응과 치료를 중심으로 적용되고 있어 변화된 침입 위협에 대한 근본적이 방어책을 제시하지 못하고 있는 실정이다. 이에 본 연구에서는 예방 중심의 보안 모델을 제안한다. 본 연구에서 제안하는 모델은, 궁극적으로 보안공격에 대응하기 위해서는 계정, 권한, 인증, 감사추적 및 이상행위 감시라는 것이 매우 중요하다는 관점에서 수립된 모델이다. 본 연구의 결과는 다양한 보안위협요소에 효과적으로 대응할 수 있는 프로세스를 강화함으로써, 끊임없이 진화하는 새로운 유형의 공격에 대비하고, 정보시스템의 신뢰성을 확보할 수 있는 참조모델로 활용될 수 있을 것이다.

ABSTRACT

The recent APT attacks including cyber terror are caused by a high level of malicious codes and hacking techniques. This implies that essentially, advanced security management is required, from the perspective of 5A. The changes of IT environment are represented by Mobile, Cloud and BYOD. In this situation, the security model needs to be changed, too into the Airport model which emphasizes prevention, and connection, security and integration of functions from the existing Castle model. This study suggested an application method of the risk-based Airport model to the cyber security environment.

키워드

APT, 해킹, 보안, 취약점, 통합계정관리

Ⅰ. 서 론

그동안 네트워크 측면에서 접점에 대한 침입차단, 탐지 등과 백신등을 활용한 PC의 악성코드 대응에 대한 사항은 많은 연구를 통해 대책을 수립하고 논의되었지만 IT서비스에 대한 접근을 통제하고 다중의 인증을 통해 권한을 부여하고 이를 적절히 감사하는 한편 실시간 모니터링을 실시하는 측면의 연구는 미비하였다.

본 연구의 목적은 사이버 환경에서 다양한 형태로 제공되고 있는 IT서비스의 안전성 확보를 위하여 항공안전을 보장하기 위해 공항 보안검색 프로세스를 분석, 고찰하여 IT서비스에 대한 접근통제 프로세스를 제시하고자 한다.

Ⅱ. 관련연구

최근 해킹공격은 점점 지능화되어 사고가 발생하기 오랜 시간 전부터 목표에 침투해 모니터링을 하다가 충분한 정보를 수집하고 적절한 시점에 공격을 가한다. 주로 웹과 메일 등을 활용하여

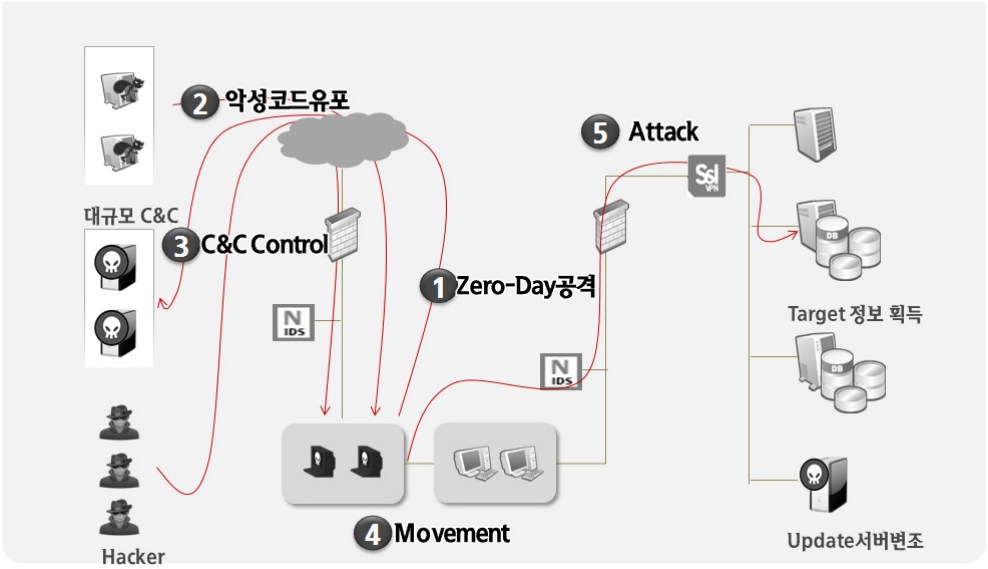

그림 1. APT 공격기법과 프로세스

불특정 다수를 악성코드에 감염시킨 후에 이들을 모니터링하여 목표를 정하고 공격을 시도하는 것이다. APT는 다단계의 공격 프로세스를 거쳐서 이루어진다. 먼저 공격자가 악성코드를 포함한 메일을 목표가 된 기업, 기관 등의 사용자에게 보낸다. 또는 취약점이 존재하는 웹 서버를 감염시켜 방문자들을 감염시키고, 모니터링을 통해 공격자가 원하는 공격 대상을 선별하는 방식이다.

보통 사용자는 drive-by-download에 의해 악성코드가 다운로드 되고, 실행되면서 감염된다. 사용자가 감염이 된 후에는 보안 솔루션을 우회하기 위해 몇 주간을 휴면 상태로 지내기도 하고, 백신의 프로세스를 정지시키거나, 삭제가 되도 재설치하게 하는 등의 방법을 통해 장기적으로 공격을 할 수 있는 기반을 마련한다.

이렇게 공격 기점을 마련하면 공격자는 C&C 서버를 이용해 감염 대상을 제어하고, 네트워크 공유 파일 등을 통해 감염 대상을 확대시킨다. 이렇게 확보된 감염 대상에게서 중요 정보가 담긴 데이터들을 FTP, HTTP 등의 신뢰할 수 있는 서비스를 이용해 C&C 서버로 다운로드 받을 수 있다.

이처럼 사용자들은 점점 지능화되고 지속적인 위협에 노출되어 있지만, 공격자들의 치밀하고 다양한 침투방법, 보안 솔루션을 우회하는 공격 등을 가하고 있어 보안 담당자들이 사전에 위협을 파악하고 대처하기가어려운 실정이다. 이는 안티바이러스 제품의 시그니처 탐지 기반 구조가 가지는 취약점을 이용한다. 백신에서 탐지가 되지 않고, 정상적인 프로그램처럼 동작하면서 공격에 필요한 정보들을 수집하기 때문에 보안 담당자가 사전에 이를 파악하는 것은 무척이나 어렵게 된다.

궁극적으로 APT공격을 시도하는 해커가 원하는 정보는 목표시스템에 접근하기 위한 계정과 패스워드에 집중된다. 또는 이러한 정보취득이 여의치 않다면 악성코드에 감염된 좀비PC등을 활용한 일시적 Traffic 폭증을 활용한 DDoS 공격이나 좀비PC의 정보를 모두 삭제하는 등의 공격도 서슴치 않는다.

해커가 취득한 계정과 패스워드로 핵심 정보시스템에 접근하고자 하는 시도를 무력화하기 위한 방법의 마련이 반드시 필요하며 이러한 방안을 본 연구를 통해 수립하고자 한다.

한편, 지난 5년간 발생한 주요한 보안 사고를 분석한 결과 최근의 공격동향인 APT를 포함한 다양한 해킹, 정보유출사고를 완벽하게 방어하는 것은 쉽지 않지만 가장 중요한 NW, 서버, DB에 대한 계정에 대한 관리 강화 및 권한의 구체적 정의, 접속에 대한 사용자별, 디바이스별 인증을 통해 보안 사고를 미연에 방지할 수 있음을 알 수 있다.

표 1. 주요 보안사고의 시사점

사고명	유형	사고원인	대책
농협 전산망 마비	서비스 중단	시스템 계정 노출, 외부접속 허용	계정관리강화, 권한관리 강화
네이트 고객 정보유출	정보 유출	악성코드 감염, DBA계정 노출	계정관리강화, Multi-Factor 인증
현대캐피탈 고객정보 유출	정보 유출	퇴사자계정존치	계정관리강화, 권한관리 강화

KT대리점 고객정보 유출	정보유출	대리점관리소홀, 이상행위검증미흡	사용자/디바이스인증, 이상행위검증
북한의 S사 네트워크 침투	NW 노출	권한관리 미흡, 네트워크 미분리	사용자별 권한관리, 해외접속 업무분리

III. 위험평가기반 접근통제 모델

3.1 위험평가기반 접근통제의 핵심요소 정의

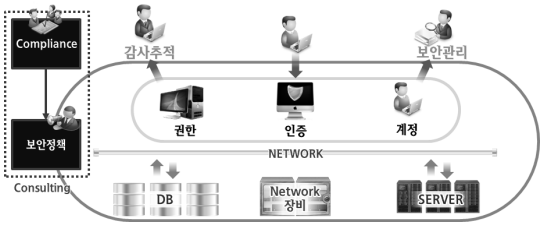

그림 2. 접근통제체계의 핵심요소 구조도

3.2 위험평가 기반의 접근통제 프로세스

IT서비스에 대한 접근에 대한 이상행위는 로그인, 개인정보조회, 거래에 대한 요청에 있어 모든 User, Device, Location에 대한 정보를 수집하고 과거의 이력과 비교하여 위험평가를 실시한 결과에 따라 위험등급이 산정되며 해당 등급에 대해서 사전에 정의된 보안정책 및 사용자의 Profile을 활용한 비즈니스 Rule에 따라 접속에 대한 승인, 추가인증요청, 접속거부의 결과로 반영되고 또한, 이렇게 정의된 결과 값은 접속유형관리를 통하여 위험관리모델에 Feedback이 이뤄져야 지속적인 보안관리가 이뤄질 수 있다.

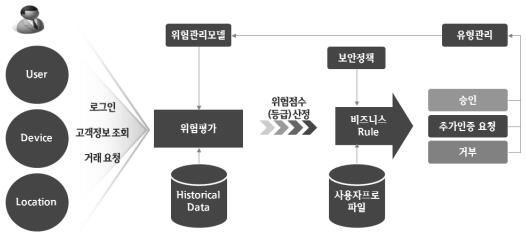

그림 3. 위험평가기반의 접근통제 프로세스

또한 이러한 프로세스의 반영은 DB, 서버, 네트워크장비 등에 접속하는 모든 사용자에 대해 개인정보보호법 및 정보통신기반보호법 등의 Compliance 요구사항을 준수하고 기업과 기관의 보안정책에 따라 계정의 Life-Cycle 및 권한을 관리하고 이상행위에 대한 감사추적을 실시하는 것을 유도할 수 있다.

3.3 지능형 접근통제를 위한 인증기능요소

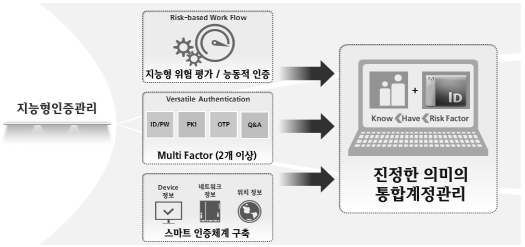

그림 4. 지능형 인증서비스를 위한 필수 기능요소

IV. 결 론

본 연구는 IT시스템의 발달에 따라 변화한 정보보호 요구사항에 대해 IT서비스의 안전성을 보장하기 위한 목적에 따라 위험관리기반의 Airport 모델을 수립하였으며, 궁극적으로 보안공격에 대응하기 위해서는 계정, 권한, 인증, 감사추적 및 이상행위 감시라는 것이 매우 중요하다는 관점에서 수립하였다.

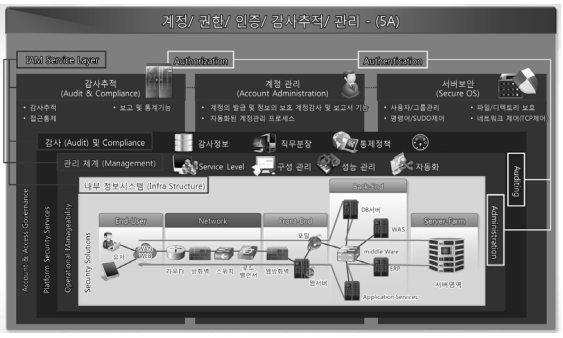

그림 5. 5A기반 Airport모델 Blueprint

향후 연구과제는 정보자산에 대한 접근에 있어 이상행위를 검출하기 위해 로그인, 개인정보조회, 거래에 대한 요청에 있어 모든 User, Device, Location에 대한 정보를 수집하고 과거의 이력과 비교하여 위험평가를 실시한 결과에 따라 위험등급을 산정하며 해당 등급에 대해서 사전에 정의된 보안정책 및 사용자의 Profile을 활용한 비즈니스 Rule에 따른 접속에 대한 승인, 추가인증요청, 접속거부의 결과로 반영하기 위한 프로세스에 대한 설계 연구와 계정, 인증, 권한에 대한 빅데이터 관점의 감사추적 및 이상행위에 대한 사전예방적 연구가 필요하다.

이렇게 정의된 연구결과는 접속유형관리를 통하여 위험관리모델과 접목되어 지속적인 보안관리 및 정보자산에 대한 보안성강화의 기반기술로

활용될 것이다.

참고문헌

[1] 김경진, “신뢰할수있는개인정보보호접근제어 모델연구”, 성신여자대학교박사학위논문, 2013

[2] 최향창, “ID관리환경에서 접근통제기반 프라이버시 보호 모델”, 전남대학교박사학위논문, 2005

[3] 김동률, “모바일환경에서안전한일회용패스워드 인증”, 한국디지털정책학회, v.11, no.12, 2013

[4] 양종모, “농협전산망 장애 사건의 형사법적 고찰”, 법학연구, v.19, no.2, 2011

[5] 심우민, “네이트해킹사고와포털의개인정보보호”, 이슈와논점(국회입법조사처), no.282, 2011

[6] 이대영, “개인정보유출사고사례조사를통한 기업대응전략에대한연구:현대캐피탈해킹사건을중심으로”, 서울과학종합대학원석사학위논문, 2013

[7] 권건호, “개인정보 유출은 남 회사 일?”, 주간동아, 850호, p30~31, 2012.8

[8] 천영식, “北, 南 IT 기업 해킹 국가전산망 장악 기도”, 문화일보, 2013.10.16.

[9] 이주형, “미래 공항보안 검색 방향에 관한 고찰”, 항공진흥, v58, 2012.8

[10] 최상균, 이철웅, “시뮬레이션을 이용한 공항 보안검색 시스템 개선으로 이용객 서비스 수준제고 방안 연구”, 한국컴퓨터정보학회, v.18, no.3, 2013.3

[11] 임설화, 김종수, 양준근, 임채호, “ APT현황과 신종 악성코드 대응방안”, 정보보호학회지, v24, no.2, 2014.4