논문 15-40-05-09 The Journal of Korean Institute of Communications and Information Sciences '15-05 Vol.40 No.05
http://dx.doi.org/10.7840/kics.2015.40.5.841

안전한 XaaS 구현을 위한 APT 공격 분석과 대응방안에 관한 연구

이 선 호◆, 김 대 엽°

Study on APT Penetration Analysis and Plan of Reaction for Secure XaaS

Sun Ho Lee◆, DaeYoub Kim°

요 약

XaaS(Everything as a Service)는 사용자가 필요한 소프트웨어 컴포넌트를 네트워크를 통하여 제공하고,, 사용자는 자신이 이용한 컴포넌트에 따라 과금을 지불하는 서비스이다. 일반적으로 XaaS는 클라우드 컴퓨팅의 일종으로 간주된다. 그러나 XaaS는 일반적으로 중앙의 서비스 사업자에 의하여 제공되기 때문에 다양한 해킹 공격의 목표가 되기 쉽다. 특히, XaaS가 APT (Advanced Persistent Threat) 공격의 목표가 된다면, XaaS 서비스 사업자뿐만 아니라 사용자들까지 심각한 위험에 노출될 수 있다. 현재 다양한 APT 공격 대응 방안이 제안되고 있으나, 보안 통제 측면에서 모든 요소를 고려하고 있지 못하다. 본 논문에서는 안전한 XaaS 운영을 위한 기술적, 정책적 요소를 고려한 보안 감사 방안을 제안한다.

Key Words : XaaS, APT, Compliance, Control Policy, Cloud Network

ABSTRACT

XaaS (Everything as a Service) provides re-usable, fine-grained software components like software, platform, infra across a network. Then users usually pay a fee to get access to the software components. It is a subset of cloud computing. Since XaaS is provided by centralized service providers, it can be a target of various security attacks. Specially, if XaaS becomes the target of APT (Advanced Persistent Threat) attack, many users utilizing XaaS as well as XaaS system can be exposed to serious danger. So various solutions against APT attack are proposed. However, they do not consider all aspects of security control, synthetically. In this paper, we propose overall security checkup considering technical aspect and policy aspect to securely operate XaaS.

Ⅰ. 서 론

XaaS(Everything as a Service)는 클라우드 서버를 이용한, 온라인 서비스를 통하여 사용자들이 필요한 소프트웨어, 플랫폼, 인프라 등을 제공하고, 사용자의 이용 따라 돈을 지불하는 방식으로, 새로운 IT 요소 제공 방식으로 주목 받고 있다. 특히, 스마트 단말기의 급속한 보급에 따라, 언제 어디서나 서비스를 제공

※ 본 연구는 정보통신기술진흥센터의 산학협력 특성화 지원사업(IITP-2015-R03461510010001002) 지원으로 수행되었습니다.
※ 본 연구는 한국연구재단 기초연구사업과제(NRF-2013R1A1A2008389) 지원으로 수행되었습니다.
◆ First Author : Suwon University Department of Information Security, tjsgh9000@naver.com, 학생회원
° Corresponding Author : Sunwon University Department of Information Security, daeyoub69@suwon.ac.kr, 정회원
논문번호 : KICS2015-03-067, Received March 23, 2015; Revised May 8, 2015; Accepted May 8, 2015

표 1. APT 공격 사례 및 피해
Table1. APT attack Cases and Damages

구 분	공격 목표	발견 연.월	피해 내용
듀큐	프랑스 등 8개국 6개 기업	2011.10	디지털 서명, 인증 및 시스템 정보
Stuxnet	이란 원자력 발전소	2011.07	원자력 발전시설 지연
Shady RAT	정부, IT업체 등 72개 조직	2011.07	DB, 이메일, 중요기밀
RSA해킹	EMC/RSA	2011.04	Secure ID
오로라	구글 등 200개 이상 기업	2010.10	소스코드, IP, 메일계정
나이트 드래곤	글로벌 석유화학업체	2009.11	디지털 서명, 인증파일,시스템 정보가 유출
포이즌 아이비	화학 및 군사기업	2011.10	설계, 제조 공정 등의 기밀 데이터를 탈취
Operation Red Octorber	정부 및 과학연구 기관	2012.10	계정 정보 및 개인 모바일 기기와 네트워크 장비 정보 등 내부 자료 수집

받기 원하는 사용자 요구사항의 증가로 인하여 더욱 각광받고 있다.

XaaS는 통합서버에 접속한 클라이언트가 자신이 원하는 서비스만 골라서 제공받는 방식으로 이루어지기 때문에, 서버 및 데이터의 보안적인 측면에서 보안 취약점에 분석 및 대응이 필수적으로 요구된다. 대표적인 예로, 지능형 지속 가능 위협(Advanced Persistent Threats, APT) 공격을 들 수 있다[1-6]. 최근 2014년 9월에 발생한 노르웨이의 대규모 석유 업체 해킹 공격이 있으며, 과거 2010년에는 이란의 핵발전 시설이 스턱스넷 (Stuxnet)이라는 신종 APT 악성코드에 의해 해킹 공격을 받아 핵원자로 원심분리기 중 20%가 작동 중단되는 사건이 있었다. 가장 최근 국내에서도 한국수력원자력이 APT 공격으로 추정되는 해킹 공격의 피해로 원자로 발전 시설의 설계 도면이 유출되는 사건이 발생하였다.

표 1은 과거 발생한 주요 해킹 공격 사례들이다. 이러한 신종 APT 공격들이 XaaS의 서비스 서버나, 데이터를 공격 대상으로 삼는다면, XaaS 서비스 시스템 및 사용자 단말기가 APT 악성 코드의 유포 대상이 될 수 있다. 그러나 현재로서 APT 공격으로부터 방어하는 완전한 솔루션은 아직 존재하지 않는다. 그러므로 침해 위험 요소를 사전 관리하고, 여러 보안 정책과 통합 관리를 통해 APT 공격 위험을 줄여야 한다. 또한 APT 보안 솔루션들도 과거의 방화벽, 샌드박스 등 단순 접근 차단방식의 솔루션을 넘어, 빅데이터 기반의 자료 분석 기술을 융합한 진화된 악성 코드 탐지 솔루션과, 지능형 보안 솔루션, 통합 보안 서비스를 내세워 APT 공격으로부터 조직 및 다양한 사회 서비스 주체들을 보호하고 있다.

Ⅱ. APT 공격 절차 및 분석

APT 공격은 여타 다른 악성 코드 및 해킹 기법들과는 다른 방법의 위협이다. 이 공격 방식은 목표물로 정한 특정 기업, 국가 주요 기관, 시스템 등을 장기적이며, 정교한 방식으로 공격한다. APT라는 용어는 2006년 미·공군이 인터넷 사용자를 공격하는 상황 속에서 국가의 역할을 설명하는 군사 용어로 처음 사용되었다. 이후 보안 업계에서는 정교한 목표 공격의 유형을 표현하는 용어로 APT를 사용하고 있다. 그림 1에서처럼 APT공격은 크게 4단계를 통해 진행된다.

(1) 정찰: 목표물의 취약점 파악 단계. 정찰 단계에서는 기본적인 취약점 조사부터, 심층적 취약점 스캔까지 진행된다.

(2) 진입: 정찰 단계에서 발견된 취약점을 이용, 목표물의 네트워크/시스템에 침입한다. 이 단계에서 정교한 공격 기술을 통해 시스템의 권한 획득도 가능하다.

(3) 권한 상승 및 제어권 획득: 침입 후 목표물의 주요 시스템에 대한 추가 권한 및 제어권 탈취를 시도한다.

(4) 지속적인 악용: 탈취한 권한을 통한 정보 해킹을 진행한다. 이 단계에서 발각될 확률이 높기 때문에, 일반적으로 장기적인 진행이 이루어진다.

APT 공격의 특징은 목표물만 지속적으로 공격한다는 것이다. APT 공격은 잠복 기간이 길고, 다양한

그림 1. APT 공격 절차
Fig. 1. APT Attack Procedure

표 2. 통제의 주요활동
Table 2. Security Control Activities

유형	기술적(X)	관리적(Y)	물리적(Z)
예방(A)	방화벽(1), 암호화(2), USB보안(3), WIPS(4), DRM(5), AAA(6), 백신SW(7), 버전 패치(8), 인증(9)	정책수립(1), 보안서약(2) 업무분리(3), 보안경비(4), 보안교육(5), 운영매뉴얼(6), 취약점평가(7), 외부위탁(8), 권한부여(9), 모의훈련(10)	출입통제(1), 자물쇠(2), 생체인식(3)
탐지(B)	IDS(1), 감사로그(2), ESM(3), DLP(4), 무결성검증(5)	보안감사(1), 모니터링(2), 정보수집(3),	센서(1), 경보(2), CCTV(3)
교정(C)	백신SW(1), NAC(2), CheckPoint(3)	BCP수립(1), 백업/복구(2), 대책위원회(3), 사고분석(4)	DR센터구축(1), UPS(2) 항온항습(3), 전력이중화(4)

패턴의 공격 방식이 복합적으로 적용되기 때문에 일반적인 보안 정책으로 예방/대응하기 어렵다. 해커들은 이러한 공격의 특성을 이용하여 정치적 혼란 야기, 군사/금융/기술 스파이, 금전적 이익획득과 같은 다양한 목적으로 APT 공격을 수행하며, 그 대상으로 정부기관, 군사 조직, 주요 인프라 시스템, 금융 기관, 기업 조직, 정치 조직 등이 있다.

Ⅲ. APT 보안제품의 동향 및 분석

APT 공격의 위협이 XaaS 뿐만 아니라, 국가 기반시설, 금융 조직, 글로벌 기업에 까지 퍼지면서, 국내외 보안 기업들의 지속적인 연구/개발을 통해 현재 다양한 보안 제품들이 출시되었고, 빅데이터 기술의 발달로 정보 분석을 통한 보안 서비스와 통합 보안 관제 시스템 등이 등장했다.

국내 보안업체 A사의 솔루션은 기존의 악성 코드 분석기술과 탐지기술을 융합한 네트워크 기술을 기반으로 낮은 오진율의 서비스를 지원한다. B사의 솔루션은 엔드 포인트 보안 시스템, 포렌직 시스템, 악성코드 분석시스템 등 다양한 종류의 서비스를 지원한다. C사의 제품은 웹으로부터 서비스 받는 행위들을 분석/탐지하여 스피어피싱을 포함한 다양한 APT 악성 코드 공격으로부터 사용자를 보호한다. 이처럼 국내의 대부분의 솔루션들은 서버로부터 오는 데이터를 시그니처 기반 분석, 자체 악성코드 진단기법을 통하여 APT 공격으로부터 보호하고 있다.

현재 출시된 다양한 보안 솔루션들과 기법들도 APT 공격에 일부 대응하고 있으나, 기술적 대응 방안에 치중하고 있기 때문에, 다양한 공격 기법이 복합적으로 활용되는 APT 공격에 종합적으로 대응할 수 없다. 즉, APT 공격에 보다 효과적으로 대응하기 위해서는 효율적인 악성코드 탐지뿐만 아니라 사용자/기기 인증과 같은 신뢰도 향상 기술과 XaaS와 같은 서비스 보호를 위해서는 기술적/관리적 대응 방안을 함께 고려할 필요가 있다[7-9].

본 논문에서는 목표 대상인 XaaS의 보안 취약점을 분석하고, APT 공격 절차를 고려하여 효과적일 수 있는 보안 대책 방안을 제시한다.

Ⅳ. APT 공격 대응을 위한 내부 감사

XaaS는 크게 필요한 기능을 사용자가 다운로드하여 자신의 단말기에 인스톨하는 형태와 서버 상에서 작동하는 기능을 네트워크를 통해 온라인으로 이용하는 형태가 있으며, 최근에는 후자의 형태가 주류가 되고 있다. 이러한 서비스 방식과 APT공격의 공격 절차를 분석해 보았을 때 XaaS의 클라우드 서버보안에는 물리적인 보안장치와 보안정책을 포함한 총괄적인 종합통제정책이 구축·운용되어야한다. 즉, 표 2와 같은 보안 목적 달성을 위한 주요 예방, 탐지, 교정 통제정책이 종합적으로 요구된다. 그러나 기존의 APT 솔루션들에는 표 3과 같이 각각 중점을 두고 있는 통제유형들을 제외하고, 활성화되지 않은 정책유형도 존재하고 있다.

이에 XaaS를 APT 공격으로부터 보호하기 위해 요구되는 종합 통제 정책을 위한 정책 및 감사 방안을 제시한다.

표 3. 기업별 솔루션의 통제 정책 비교
Table 3. Security Control Comparisons of Enterprise Solutions

유형 / 기업	예방통제	탐지통제	교정통제
A 기업	○	○	○
B 기업	○	○	-
C 기업		○	-
D 기업	○	○	-
E 기업	-	○	-

표 4. 단말기 보안 통제를 위한 보안 감사 항목
Table 4. Checkup List for Device Security Control

보안 확인 사항	세부 보안 확인 사항	통제활동
1. 서버, 네트워크 장비, 보안시스템, PC 등 자산 중요도 또는 특성에 따라 OS, 소프트웨어 패치관리 정책 및 절차를 수립/이행하고 있는가?	- 패치담당자 및 책임자는 지정되어 있는가?	A-X-8
	- 특성에 따라 분리되어 있는가?	A-Y-3
	- 패치 정책 및 절차가 수립되어 있는가?	A-Y-1
	- 패치 정책 및 절차에 대한 갱신 프로세스가 확립되어 있는가?	A-Y-1
	- 패치는 주기적으로 이루어지고 있는가?	A-X-8
	- 특이 사항 발생 시 긴급 패치가 가능한가?	
	패치 관련 업체 및 제조사의 연락처는 준비되어있는가?	
2. 주요 서버, 네트워크 장비 등의 경우 설치된 OS, 소프트웨어 패치적용 현황을 관리하고 있는가?	패치 버전 및 패치 적용 일자를 문서화하고 있는가?	A-Y-6
	패치 현황은 관리/감독되고 있는가?	A-Y-6
	패치 현황감사를 주기적으로 시행하는가?	B-Y-1
3. OS 경우 패치 적용하기 전 시스템 가용성에 미치는 영향을 분석하여 패치를 적용하고 있는가?	OS 버전패치는 권한책임자의 승인을 통해 이루어지고 있는가?	A-X-8
	패치가 불가할 경우, 책임자에게 보고하여 조치하고 있는가?	
	패치로 인한 문제점 발생 시, 대응방안은 수립되어 있는가?	A-Y-1
4. 접근통제 및 백신보안 S/W를 사용하고 있는가?	접근통제 및 보안 S/W의 사용법을 정확히 숙지하고 있는가?	A-X-7
	접근통제 및 보안 S/W는 유지보수가 이루어지고 있는가?	
5. 블랙리스트, 화이트리스트 등의 악성코드 식별 정책을 운용하고 있는가?	악성코드 식별정책 및 솔루션을 운용하고 있는가?	A-X-7
	식별된 악성코드를 정상적으로 차단하고, 제거하고 있는가?	
	식별오류에 대한 대응방안을 운용하고 있는가?	A-Y-1
	신종 악성코드의 등장에 따른 식별 정책 갱신은 주기적으로 이루어지고 있는가?	
6. 외장하드, USB, CD 등 휴대용 저장매체 취급(사용), 보관, 폐기, 재사용에 대한 정책 및 절차를 수립 후, 이행하고 있는가?	휴대용 저장매체에 대한 취급, 보관, 폐기, 재사용 정책 및 절차가 수립되어 있는가?	A-Y-1
	휴대용 저장매체에 대한 사용허가 및 등록절차를 수립되어있는가?	
	허가 받지 않은 휴대용 저장매체에 대한 감사가 주기적으로 이루어지는가?	B-Y-1
	허가 된 휴대용 저장매체에 대한 관리가 체계적으로 이루어지고 있는가?	A-Y-6
7. 주요 정보시스템이 위치한 통제구역, 중요 제한구역 등에서 휴대용 저장매체 사용을 제한하고 있는가?	중요 제한구역의 보안출입절차가 이행 중인가?	A-Z-1
	중요 제한구역 내에 센서, 경보기, CCTV 등 물리보안 장치가 운용 중인가?	B-Z-2 B-Z-3
	불가피하게 휴대용 저장매체를 이용 시, 관리자의 관리감독이 이루어지고 있는가?	A-Y-6
8. 휴대용 저장매체를 통한 악성코드 감염 및 중요정보 유출 방지를 위한 대책을 마련하고 있는가?	USB 보안 솔루션 및 백신 솔루션을 사용하고 있는가?	A-X-3
	휴대용 저장매체내의 숨김 파일 표시를 표시하기, 보안스캔 후 사용하기 등, 관리 정책을 적용하고 있는가?	A-Y-1
	정보 유출에 대한 대응절차 및 범인 추적 프로세스가 구성되어 있는가?	A-Y-4

4.1 종합 통제를 위한 내부 감사

4.1.1 단말기 보안

이동 기억 장치 및 보조 기억 매체에서 파일을 옮기거나 인터넷, 이메일, P2P 등의 통신 서비스를 통해 다운로드 받음으로서 사용자 단말기 및 시스템에 악성 코드가 설치되는 경우, 공격자가 목표 시스템에 침투할 수 있다. 이러한 취약점은 APT 공격의 일차 목표인 단말기에 침투에 해당한다. 그러므로 단말기에 대한 보안의 통제가 필요하다. 표 4는 단말기 보안 통제를 위한 감사 항목을 나타낸다. 표 4와 같은 감사 활동은 기존의 단말기 보안 방안을 보완하고, 이를 통해 APT 공격의 일차적 접근 경로를 차단하는 효과를 강화할 수 있다.

표 5. 데이터 유출 방지를 위한 보안 감사 항목
Table 5. Checkup List for Data Security Control

보안 확인 사항	세부 보안 확인 사항	통제활동
1. 주요 데이터는 암호화를 통하여 보호되고 있는가?	암호화 알고리즘은 관련 법률을 충분히 만족시고 있는가?	A-X-2
	암호화의 안전성은 주기적으로 검증되고 있는가?	
	암호정책은 주기적으로 관리되며, 갱신되고 있는가?	
2. 암호키 생성, 이용, 보관, 배포, 복구, 파기 등에 관한 절차를 수립 후, 이행하고 있는가?	암호키 관리 담당자를 지정하고 있는가?	A-Y-6
	암호키 관련 절차 및 정책이 수립되어있는가?	A-Y-1
	암호키 사용 유효기간을 두고 운영 중인가?	
	암호키 유출시, 대응절차 관련 정책은 수립되어 있는가?	
	긴급 상황 시, 암호정책을 갱신 할 수 있는가?	
3. 암호키 생성 후 암호키는 별도의 안전한 장소에 소산 보관하고 암호키 사용에 관한 접근권한 부여를 최소화하고 있는가?	암호키를 안전한 장소에서 백업하여 사용 중인가?	C-Y-2, A-Y-6
	암호키를 웹서버에 저장할 시 물리적으로 분리된 서버에 저장하고 있는가?	
	암호키 저장장소는 체계적인 접근통제가 이루어지고 있는가?	A-Z-1
	암호키 접근권한을 가진 인원의 결원 시, 해당 권한을 회수, 폐기하고 있는가?	A-Y-6
4. 데이터 유출방지 솔루션을 사용하고 있는가?	데이터 유출방지 솔루션의 사용법을 숙지하고 있는가?	B-X-4
	솔루션의 로그를 주기적으로 확인하고, 특이사항을 보고하고 있는가?	A-Y-6
	데이터 유출방지 솔루션은 주기적으로 유지보수가 되고 있는가?	

앞서 언급한 것처럼 단말기 보안은 APT 공격의 일차 목표인 침투를 방어하는데 가장 중요한 요소이다. 이를 효과적으로 대응하기 위해서는 표 4의 각 점검사항에 대응되는 통제 활동에서 보여지 듯, 예방 통제가 가장 중요하고 효과적인 통제이다. 그러므로 OS의 보안패치통제, 제한구역 내 접근통제, 휴대용 저장매체통제 등의 효과적인 통제정책을 수립하고, 이를 주기적으로 점검하는 활동이 필요하다.

4.1.2 핵심정보 암호화 및 데이터 유출방지

대부분의 APT 공격의 최종 목표는 핵심 정보의 탈취이기 때문에, 핵심 정보에 대한 직접적인 보안은 APT 공격 대응의 중요한 요소 중 하나이다. 따라서 XaaS 등의 클라우드 서버를 이용하는 서비스들의 주요 데이터는 기본적으로 암호화하여, 정보 유출이 발생하더라도 공격자들이 이에 대한 해독하기 불가능하게 또는 매우 어렵게 하는 것이 중요하다. 이를 위한 통제로서 표 5의 보안 감사를 진행한다.

표 5의 암호화 기능과 DLP 등의 데이터 유출방지 시스템을 활용하는 것은 다양한 형태로 데이터 유출을 시도하는 APT 공격으로부터 데이터를 보호하는 안전장치가 될 수 있다. 특히, 데이터 유출 방지는 예방, 탐지, 교정의 모든 통제 요소와 관련이 된 것으로, 표 5의 보안 점검 항목에 대응하는 암호화, 데이터 유출방지 통제 활동들은 APT 공격에 효과적으로 대응하기 위해 필수적으로 요구된다.

4.1.3 보안 관리 및 운영

APT 공격은 표적이 되는 대상의 보안 체계를 바탕으로 여러 취약점을 분석하여 공격한다. 이에 대응하기 위해 XaaS와 같은 클라우드 서비스 서버를 운영하는 조직의 데이터에는 중요도에 따라 차등화 된 접근통제를 운영하고, 접근하는 인원을 최소화해야한다. 또한 접근통제 강화를 위해 접근인원에 대해 2가지 이상의 중복 인증을 운용해야 한다. 표 6은 보안 관리를 위한 감사 항목을 나타낸다.

금융권 및 기업 조직에서 자주 발생하는 정보 유출 사건들은 대부분 내부 보안운영절차 미흡, 주요 데이터에 대한 접근통제 미흡 때문에 발생한다. 주요 보안 데이터는 항상 철저한 접근통제에 의하여 이루어 져야하며, 보안 담당자 및 책임자의 역할 및 책임이 강조되어야 한다. 이에 표 6의 보안 점검 항목에 대응하는 보안 관리 정책 및 절차, 철저한 보안 운영관리를 통하여 정보 유출을 차단하고, APT공격에 대해 사전 대응하는 것에 중점을 두고 있다. 또한, 표 6의 감사를 통해 취약점을 조직 스스로 분석하고 평가하여, 문제점들을 조기에 발견하고 해결할 수 있으며, XaaS 서버의 좀비 계정 문제를 효과적으로 해결 할 수 있다.

표 6. 보안 관리를 위한 보안 감사 항목
Table 6. Checkup List for Security Management Control

보안 확인 사항	세부 보안 확인 사항	통제활동
1. 정보시스템 운영을 위한 운영절차를 수립하고 있는가?	문제 발생 시 운영 매뉴얼에 따른 절차식 훈련이 주기적으로 이루어지고 있는가?	A-Y-6
	운영절차는 그 효율성을 충분히 검증받았는가?	
2. 각종 정보시스템 운영절차를 목록으로 관리하고 주기적인 내용 검토를 하고 있는가?	운영절차를 관리하는 관리 담당자가 지정되어 있는가?	A-Y-6
	운영절차를 주기적으로 확인하고, 숙지하고 있는가?	
	운영절차를 대외비 문서로 지정하여 보관하고 있는가?	A-Y-6
	운영절차 문서를 백업하여 안전한 곳에 보관하고 있는가?	C-Y-2
3. 정보시스템 운영을 외부 위탁하는 경우 운영절차(매뉴얼) 수립 여부를 확인하고 있는가?	외부 위탁업체는 충분한 경험과 실력이 있는 곳인가?	A-Y-6 A-Y-8
	외부 위탁업체가 운영절차를 준수하고 있는지 주기적으로 감사하고 있는가?	
	수립 및 운영상황을 알기 위해 외부업체로부터 적절한 보고를 받고 있는가?	
4. 보안시스템 관리자 등 접근이 허용된 인원을 최소화하고 비인가 접근을 엄격하게 통제하고 있는가?	접근 허용 인원을 체계적으로 관리하고 있는가?	A-Y-6
	접근권한을 가진 인원의 결원 시, 그 권한을 회수, 폐기하고 있는가?	
	보안시스템의 접속로그를 주기적으로 분석하여 비인가 접속시도를 확인하고 있는가?	B-X-2
5. 2가지 이상의 인증 체계를 복합적으로 사용하고 있는가?	인증 체계는 사용에 적합하며, 안전한가?	A-X-9
	채택한 2채널 인증방식은 안전성을 검증받았는가?	
6. 주요 데이터의 접근 통제는 권한을 통해 체계적으로 이루어지고 있는가?	권한부여는 계급과 업무에 맞게 이루어 졌는가?	A-Y-9
	접근통제는 두 가지이상의 방식으로 운영되고 있는가?	A-Z-1
7. 주기적으로 취약점 자체 평가를 운영하고 있는가?	정보시스템의 중요도에 따라 진행하고 있는가?	A-Y-6
	취약점 자체평가에 따른 결과를 문서화하고 있는가?	A-Y-7
	취약점 자체평가는 올바른 담당자와 절차에 따라 진행되고 있는가?	
8. 내부 정보 유출 방지 보안 정책 및 보안제품을 사용하고 있는가?	정보유출에 따른 대응절차는 수립 후, 이행하고 있는가?	A-Y-1
	올바른 보안제품 사용법을 숙지하고 있는가?	B-X-4
	내부정보 유출에 대한 대응 절차가 구성되어 있는가?	A-Y-6
9. 보안 최고 책임자(CISO)와 보안 관련 담당자의 역할 및 책임을 정의하고 있는가?	보안 최고책임자는 총괄적인 보안업무 충분히 이해하고, 이행하고 있는가?	A-Y-6
	보안 실무자는 최고 책임자의 관리 업무를 충실히 이행하고, 책임을 다하고 있는가?	

4.1.4 내부 보안 교육 강화

APT공격에 대응하기 위해 조직원들의 보안 교육도 진행해야한다. 서버운영에 참여하는 내부직원이 서버보안에 관한 지식이 부족하다면, 취약한 요소가 되어 공격자에게 스피어피싱, 사회 공학적 공격 등의 APT공격을 받을 것이다. 이에 조직원들 모두가 APT 공격에 대응하기 위해 보안 교육에 참여해야 한다. 다음 표 7의 감사를 통해 조직 내의 보안교육이 잘 이루어지는지 확인한다.

IT기술이 발달함에 따라 다양한 IT 서비스를 제공받는 요즘, 이를 이용한 해킹기법들이 다양해지고 있다. 이에 따라 조직 내부의 정보유출보안을 위한 조직원의 보안교육과 침해사고 발생 시, 그 피해를 최소화하기 위한 내부 대응절차 등이 중요해지고 있다. 이를 반영하여 표 7은 조직 내의 보안교육 관리, 보안교육 대상관리, 교육 시행평가, 모의훈련 등의 보안 점검 항목을 통해 조직원들의 보안 인식 강화를 점검한다. 특히, 중요한 정보에 접근이 가능한 내부 조직원들의 교육을 통제하여, APT 공격의 첫 단계인 공격자 침투를 사전에 효과적으로 예방할 수 있다.

표 7. 내부 보안 교육을 위한 보안 감사 항목
Table 7. Checkup List for Internal Security Education Control

보안 확인 사항	세부 보안 확인 사항	통제 활동
1. 정기적인 직원 보안교육이 이루어지고 있는가?	보안교육은 적절한 내용을 담고 있는가?	A-Y-5
	보안교육에 대한 직원들의 평가는 양호한가?	A-Y-5
	정기 교육에 참여하지 못하는 인원들에 대한 추가교육을 진행하고 있는가?	
2. 보안 교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 보안교육 계획을 수립하고 있는가?	연간 보안교육계획안은 당해 1/4분기 이내에 수립하고 있는가?	A-Y-5
	보안교육 계획안은 보안 최고책임자와 상의하여 수립되고 있는가?	A-Y-6
	교육계획안의 그 기간과 대상, 내용, 방법은 적절하게 이루어 졌는가?	A-Y-5
3. 보안 정책 및 절차의 중대한 변경, 조직 내부, 외부 보안사고 발생, 보안 관련 법률 변경 등 발생 시 이에 대한 추가 교육을 수행하고 있는가?	추가 교육을 진행하기 위한 사전 계획절차가 수립되어 있는가?	A-Y-1
	추가 교육 전, 변경된 사안이나, 절차에 대한 정보를 사전 전달하고 있는가?	A-Y-6
	추가 교육은 변경된 사항과 재고점을 충분히 전달하고 있는가?	A-Y-5
4. 보안 교육대상에 정보보호 관리체계 범위 내 정보자산에 직접적, 간접적으로 접근하는 임직원 및 외부인을 모두 포함하고 있는가?	보안 교육대상을 목록으로 작성하여, 주기적으로 갱신, 관리하고 있는가?	A-Y-5
	보안 교육대상은 정보자산에 접근하는 내부인, 외부인을 총괄적으로 포함하고 있는가?	
	보안 교육대상자 선별을 위한 명확한 기준을 가지고 있는가?	
5. IT 및 보안 조직 내 임직원은 보안과 관련하여 직무별 전문성 제고를 위하여 필요한 별도의 교육을 받고 있는가?	별도의 교육은 보안 담당자 및 책임자와 상의하여 구성, 진행하고 있는가?	A-Y-5
	별도의 교육은 임직원의 담당업무별로 차등된 내용을 제공하고 있는가?	
	별도의 교육은 충분히 검증받은 기관 및 강사의 교육인가?	
6. 교육시행에 대한 기록을 남기고 교육 효과와 적정성을 평가하여 다음 교육 계획에 반영하고 있는가?	교육평가서는 올바른 질문들로 구성하며, 보안 담당자와 책임자의 허가를 통해 작성되는가?	A-Y-5
	교육의 평가기준은 명확하며, 문제점을 도출 할 수 있는가?	
	교육평가를 통해 얻은 기록을 충분히 분석하고 있는가?	
	교육평가자료는 문서화하여, 저장, 관리하고 있는가?	C-Y-2
7. 임직원 및 외부자 신규 채용 계약 시, 업무 시작 전에 보안교육을 시행하고 있는가?	업무 전 보안교육은 적정 시간동안 진행되며, 관련 법률에 따라 구성되어 있는가?	A-Y-5
	업무 전 보안교육은 보안규정위반, 보안사고의 위험성을 포함하고 있는가?	
	교육 외에 보안 서약서 작성 등, 다른 방법을 함께 시행하고 있는가?	A-Y-2

4.1.5 침해사고 준비도

침해 사고 준비도는 사고 비용을 최소화하기 위해 잠재적인 침해 흔적을 신속히 수집하고 분석 할 수 있도록 사전에 준비를 갖추는 것을 의미한다. APT 공격은 정교하기 때문에 사고에 준비되지 않은 경우, 그 피해 사실을 파악하는 것에 매우 오랜 시간이 걸릴 수 있다. 이를 효과적으로 준비하고 전사적 차원의 준비를 위해 표 8의 감사를 시행한다.

대부분의 보안은 사고의 가능성을 낮추기 위한 사전적인 투자지만, 침해 사고 준비도 는 사고가 발생했을 때 이를 효과적으로 대응하는 방법이다. 표 8에서 나타나 듯, 침해 사고 준비도는 교정 통제 뿐 만 아니라 예방 및 탐지 통제와도 밀접한 관련이 있다. 그러므로 침해 사고 준비도를 단순히 사고 대응 방법으로만 간주해서는 안 된다. Table 8의 감사를 통해 공격에 대한 탐지 및 대응을 위한 대책이 수립되어 있는지 점검하고, APT 공격 발생 시, 신속하고 적절한 대응을 통해, APT 공격에 효과적으로 대응할 수 있도록 한다.

4.1.6 형상 관리 및 데이터 백업 관리

이상 징후가 발생했을 때 대부분의 조직에서는 이상 징후를 분석할 만한 침해사고 분석 팀이 없기 때문에 저장장치를 포맷을 하여 대응을 한다. 그러나 이상 징후의 중요도에 따라 최소 3개월은 저장장치에 보관하여야 한다. 또한 사전에 항상 데이터를 백업하여 추후 만일의 침해사고 시 빠른 복구를 진행해야 한다. 이를 위해 표 9는 형상 관리 및 백업을 위한 감사 항목을 나타낸다.

전사적 데이터들의 중요성이 높아지면서, 이들의 저장, 백업 또한 중요하게 되었다. 이는 추후 발생하는 문제로부터 원활한 복구를 돕고, APT 공격의 원인

표 8. 침해 사고 준비도에 대한 보안 감사 항목
Table 8. Checkup List for Computer Emergency Response

보안 확인 사항	세부 보안 확인 사항	통제활동
1. 정기적으로 감사와 위협요인에 대한 정보를 수집하고 있는가?	보안감사와 위협요인 수집은 주기적으로 이루어지고 있는가?	B-Y-1
	정보 수집을 통해 보고서를 작성하여 저장하고 있는가?	B-Y-3
	보안감사 및 위협요인수집 담당자 및 책임자가 지정되어 있는가?	B-Y-1
	주요 데이터에 대한 무결성 검증은 주기적으로 이루어지는가?	B-X-5
2. 대응절차는 체계적으로 구성되었으며, 운용되고 있는가?	피해위치와 중요도에 따라 대응절차가 적절하게 구성되었는가?	A-Y-6
	대응절차는 조직에 맞도록 주기적으로 갱신되고 있는가?	
3. 침해사고를 모니터링 하고 신속하게 대응할 수 있도록 모니터링 및 대응 방법, 절차, 대응 조직 및 인력, 보고 및 승인 방법 등을 포함한 중앙 집중적인 대응체계를 수립하고 있는가?	침해사고 대응을 위한 모니터링은 데이터 중요도에 따라 알맞은 주기로 이루어지고 있는가?	B-Y-2
	침해사고 대응방법 및 보고, 승인 방법은 올바르게 수립되어있으며, 절차상에 문제가 없는가?	A-Y-6
	침해사고에 대한 대응체계는 보안 최고책임자를 중심으로 중앙 집중적인 체계를 이루고 있는가?	A-Y-9
	대응체계는 긴급 침해사고 시, 빠르게 대처할 수 있는 유연성을 가지고 있는가?	A-Y-1
4. 침해사고 대응절차에 관한 모의훈련계획을 수립하고 이에 따라 주기적으로 훈련을 실시하고 있는가?	모의훈련에 참여하지 못한 인원에 대한 추가 관리가 이루어지고 있는가?	A-Y-10
	모의훈련은 적절한 주기를 가지고 시행되고 있으며, 상황에 따라 추가 훈련을 배정하고 있는가?	
	모의훈련을 통해 발견한 미비사항 및 계획오류 등을 통해 대응절차를 갱신하고 있는가?	
5. 침해사고 분석을 통해 얻어진 정보를 활용하여 유사 사고가 재발하지 않도록 대책을 수립하고 필요한 경우 침해사고 대응절차 등을 변경하고 있는가?	침해사고 분석 데이터는 객관적이고, 사실적인 정보만을 담고 있는가?	C-Y-4
	재발방지를 위해 대책위원회를 구성하여 회의를 진행하며, 위원회 구성은 보안 담당자 및 최고책임자를 포함한 경영진으로 이루어져 있는가?	C-Y-3
	재발방지대책은 충분한 회의를 통해 도출한 내용을 기반으로 하는가?	
	대응절차 변경 시, 기존 절차와 상반되거나, 문제점을 야기하지 않는가?	A-Y-1

을 파악하거나 법적 대응에 활용된다. 특별히, 각 보안 감사 항목에 대응하는 통제 활동에서 나타나 듯, 형상 관리 및 백업은 교정 통제와 밀접한 관련이 있다. 이는 APT 공격이 발생했을 때, 피해를 최소화 하고, 신속히 서비스를 정상화하기 위해 중요한 요소임을 나타낸다. 이에 표 9의 보안 점검 항목에 대응하는 시스템 형상요소 저장, 올바른 백업정책, 백업장소관리 등의 통제정책을 통하여 APT공격에 대응한다.

4.2 보안 감사 분석

종합 감사 항목은 ISMS를 기반으로 구성하였으며, 제안하는 보안 감사는 기존 솔루션에서 다루지 않았던 내부 직원 교육, 휴대용 저장장치, 주요 데이터 접근통제, 모의훈련 등의 예방 및 교정 통제정책을 포함하여 종합적인 대응 방안이 마련되었는지 확인 할 수 있도록 제안되었다. 특히, 그림 2에서 보여지 듯, 표 2의 예방/탐지/교정 통제정책의 핵심 활동을 대부분 점검하도록 구성 하여 그 안전성을 높였다. 제안된 보안 감사는 통제 활동의 예방 통제 72%, 탐지 통제 72%, 교정 통제 81%를 각각 구성에 포함하고 있다.

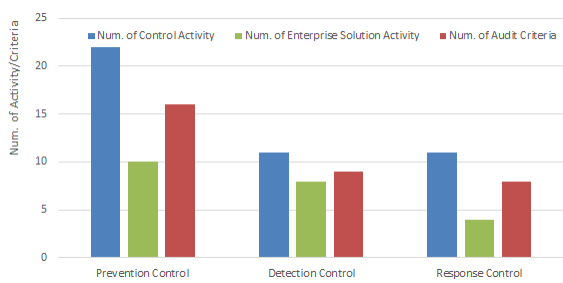

그림 2. 보안 감사 항목 구성 분석
Fig. 2. Security Criteria Analysis

V. 결 론

사물인터넷시대에 접어들면서 스마트폰과 웨어러블 디바이스 등을 통해 언제 어디서나, 사용자가 원하

표 9. 형상 관리 및 백업에 대한 보안 감사 항목
Table 9. Checkup List for Backup Control

보안 확인 사항	세부 보안 확인 사항	통제활동
1. 시스템의 형상요소를 주기적으로 문서화 하여 저장하고 있는가?	형상요소 관련 문서 저장 시, 저장장소는 안전한 곳인가?	C-Z-1
	형상 요소 문서는 백업정책을 적용하고 있는가?	A-Y-1
	문서화된 형상요소는 주기적으로 관리되고 있는가?	A-Y-6
2. 시스템 변경 및 실현상황을 기록하여 데이터로 저장하고 보관하고 있는가?	기록한 데이터는 적절한 장소에 보관·저장하고 있는가?	C-Z-1
	기록한 데이터를 분석하여, 차후 시스템 변경에 반영하고 있는가?	C-Y-4
3. 백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구절차를 수립 후, 이행하고 있는가?	백업 및 복구절차는 올바르게 수립되어 있는가?	A-Y-1
	백업을 진행 할 시, 정보의 중요도를 고려하여 진행하고 있는가?	
	백업 대상과 주기, 방법 등은 적절한가?	
4. 중요정보가 저장된 백업매체의 경우 재난에 대처할 수 있도록 백업매체를 물리적으로 떨어진 장소에 소산하고 있는가?	백업장소는 자연재해에 대한 대책 및 접근통제가 이루어지고 있는가?	C-Y-1
	주기적인 관리대장에 따라 소산 여부를 실시하고 있는가?	A-Y-1
	불가피하게 소산장소를 변경해야 할시 즉시 변경이 가능한가?	A-Y-6
	재난상황에 따라 소산장소에 피해 발생 시, 이에 따른 대응 절차가 확립되어있는가?	C-Z-2 C-Z-3 C-Z-4

는 곳에서 편리하게 서비스를 받을 수 있게 되었다. 이 덕분에 현재 우리는 XaaS라는 편리한 서비스를 이용하게 되었다. 그러나 사용자가 쓰기 편리한 만큼 취약점들도 많고, 이를 노리는 APT 공격과 같은 악성 공격들도 함께 증가했다. 과거의 APT 공격은 주요한 통제활동인 예방/탐지통제로 방어해왔다. 하지만 앞으로는 APT의 공격대상이 과거 국가기반시설, 금융조직, 글로벌 기업의 서버에 그치지 않고, XaaS와 같은 클라우드 서비스서버를 통해 사용자 단말기 까지 퍼질 것이며, 그 공격 방법도 다양해 질 것이다. 본 논문에서 APT의 공격 절차 및 각각의 보안 감사 항목과 통제 정책과의 연관성을 조사한 결과, 기존의 탐지통제에만 치중된 대응방식으로는 차세대 APT 공격에 대하여 대응하기 어려울 것으로 파악하였다.

이에 안전한 XaaS를 위해 기술적/관리적 보안방안이 필요성과 종합 통제 정책을 위한 정책 및 감사 방안을 제시하였다. 해당 감사 사항은 ISMS 인증기준을 기반으로 구성하였으며, 기존의 APT 공격 대응 솔루션들이 탐지통제에 치중된 반면, 제안된 보안 감사는 내부 직원 교육, 휴대용 저장장치, 주요 데이터 접근통제, 모의훈련 등의 예방 및 교정 통제정책을 포함하여 종합적인 통제 및 대응이 가능하도록 제안되었다. 특히, 주요 통제 활동 중, 예방통제 72%, 탐지통제 72%, 교정통제 81%를 포함하도록 구성하여 종합적인 감사가 가능하도록 구성하였다. 이를 통해 차세대 APT에 대해 종합적인 대응이 가능하며, XaaS를 포함한 다양한 IT서비스를 안전하게 사용 할 수 있다.

References

[1] J.-H. Sim, J.-K. Jung, H.-J. Kim, I.-K. Kim, and T.-M. Chung, “Survey on the recent advanced persistent threat solutions,” in *Proc. KICS Conf.*, pp. 769-770, Nov. 2013.

[2] T. Mustafa, “Malicious data leak prevention and purposeful evasion attacks: An approach to advanced persistent threat (APT) management,” in *SIECPC*, pp. 27-30, Apr. 2013.

[3] Y.-H. Kim and W. H. Park, “A study on cyber threat prediction based on intrusion detection event for APT attack detection,” *Multimedia Tools and Applications*, vol. 71, no. 2, pp. 685-698, Jul. 2014.

[4] Russel Miller, “Advanced persistent threats: Defending from the inside out,” *CA-Technologies*, Jul. 2012.

[5] S.-C. Goh, *A study of APTs(advanced persistent threat) penetration detect for security operation data and big data*, National Security Research Institute, vol. 2014, no. 022, Oct. 2014.

[6] S.-H. Lee and M.-S. Han, *Study of defense method through APT(Advanced Persistent Threat) penetration path analysis in Industrial Network-Focusing on Stuxnet Case-*, Korean Association for Industrial Security, Dec. 2014.

[7] K.-H. Kim and M.-J. Choi, "Linear SVM-based android malware detection and feature selection for performance improvement," *J. KICS*, vol. 39C, no. 8, pp. 738-745, 2014.

[8] M. Kim, "Security analysis and enhancement of tsai et al.'s smart-card based authentication scheme," *J. KICS*, vol. 39B no. 1, pp. 29-37 2014.

[9] J. Lee, J. Park, S. W. Jung, and S. Jung, "The authentication and key management method based on PUF for secure USB," *J. KICS*, vol. 38B no. 12, pp. 944-953, 2014.

이 선 호 (Sun Ho Lee)

2014년 12월~현재: 라온 시큐어 인턴 사원

2010년 2월~현재 : 수원대학교 정보보호학과 학사 과정

<관심분야> 정보보안, 네트워크 보안, 산업보안

김 대 엽 (DaeYoub Kim)

2000년 2월 : 고려대학교 수학과 박사

2000년 2월~2002년 8월 : 시큐아이 정보보호연구소 차장

2002년 9월~2012년 2월: 삼성전자 종합기술원 전문연구원

2012년 3월~현재 : 수원대학교 정보보호학과 조교수

<관심분야> 콘텐츠 보안, 미래 인터넷 보안, 난독화, 포렌직