디지털산업정보학회 논문지 제13권 제1호-2017년 3월
http://dx.doi.org/10.17662/ksdim.2017.13.1.059

사회적 이슈 관점에서 바라 본 사이버 테러 유형에 대한 위험 대응방안*

최 희 식**·김 현 규***

The Countermeasure for Threat of Cyber Terror in Sociological Perspective

Choi Heesik · Kim Hyunkyu

〈Abstract〉

In recent years, cyber terror that break into major institution's information system and destroy and paralyzed important information occurs frequently.

Some countries do dangerous acts such as train hackers and order hackers to hack important industrial confidential documents which are core of national competitiveness to reduce the competitiveness of the country and cause social confusion. In this thesis, it will study problems of cyber terror to help people to use Internet in web environment that safe from cyber terror and to avoid the risk from cyber terror such as malware and DDos.

This thesis is organized as following. In second chapter, it will look thorough the research that are related to cyber terror. In third chapter, it will study attack types of cyber terror. In fourth chapter, to defend from cyber violence, it will suggest safe solution. In fifth chapter, it will end with conclusion. Finally, to prevent urgent incidents like North Korean Cyber-attack, every Internet user must indicate their recognition on Internet security and it is significant to make a quick response treatment to create the safe online environment.

Key Words : Cyber Terror, Cyber Attack, Malignity Code

Ⅰ. 서론

최근 우리나라를 비롯하여 세계 각 국가의 정치권에도 해킹과 관련된 정보유출 및 해킹과 관련된 배후 논란이 끊이지 않고 있다. 세계 각 나라의 테러 행위는 사이버라는 커다란 가상공간의 정보 집합체를 대상으로 해킹 기술을 이용하여 해킹 공격자국이 갖지 못한 신기술 자료를 유출하여 경제적 이익을 취할 수 있는 빌미를 제공한다. 또한, 백악관, 청와대, 국정원과 같은 국가 기밀자료를 유출하여 정치적, 사회적으로 이용하여 공개하는 등 사이버 테러는 사회적으로 심각한 물의를 빚고 있다. 요즘은 기업뿐만 아니라 개인들도 일상의 많은 부분을 컴퓨터와 인터넷에 의존하고 있기 때문에 사이버 테러 위협에 노출되어 있다[1].

본 논문에서는 사이버 테러와 관련하여 국가 보안 침해와 최근 시사된 관련 사례를 중심으로 위협

* 본 연구는 2015년 삼육대학교 교내 연구비 지원으로 수행된 연구임
** 삼육대학교 컴퓨터학부 외래교수
*** 삼육대학교 컴퓨터학부 조교수(교신저자)

으로부터 안전하게 대처하여 사고를 미리 방지할 수 있는 위험에 대한 방안을 연구하여 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 사이버 테러와 관련된 사항에 대해서 살펴보고, 3장에서는 사이버 테러 공격유형에 대해서 알아보고, 4장에서는 사이버 폭력에 대응하는 안전한 방안을 제시, 5장에서 결론으로 마무리 하고자 한다.

Ⅱ. 관련연구

2.1 사이버 테러 정의

사이버 테러란 주요 기관의 정보 시스템에 침입하여 국가 기관의 중요 정보 등을 파괴하고 마비시키며 데이터베이스화되어 있는 산업, 군사, 행정, 인적자원 등 국가적인 주요 정보를 노리는 의도적 공격행위를 말한다. 또한, 네트워크에 구축된 사이버 공간을 이용하여 의도적으로 악성코드가 심어진 해킹 프로그램을 유포하여 특정 국가 및 사회 기관에 공격을 가하여 그들이 요구하는 자료를 유출하기도 한다. 사이버 테러는 무기를 사용하는 물리적 테러 공격과는 달리 IT 해킹 기술을 이용하는 비교적 적은 비용으로 상대방을 쉽게 공격할 수 있으면서 현실적으로 훨씬 더 심각한 문제성을 초래하기 때문에 사이버 테러 도발은 날로 심각해지고 있다[2].

2.2 사이버 테러 종류

사이버 테러는 주로 국가 및 특정한 기관을 상대로 이어지는 경우가 많은데, 특히, 국가와 관련된 사이버전이 발생한 예를 살펴보면, 에스토니아가 옛 소련군 동상을 철거하는 문제가 발생하자 이를 못마땅하게 여긴 러시아의 극우 분자들이 해커를 모집하여 무자비하게 해킹을 감행한 사건이 있었다. 이로 인하여 여러 날 동안 에스토니아 정부기관 홈페이지 접속과 은행거래가 전면 중단되었다. 또한, 국가 기능이 일순간에 마비되는 사이버 테러가 발생한 경우도 있는데, 2008년 8월 남 오세티아를 둘러싼 영토 분쟁으로 무력충돌이 퍼지고 있는 그루지야 주요 정부 인터넷 사이트가 러시아 비즈니스 네트워크로부터 수차례 무차별 DDos 공격을 당해 정부기관 사이트가 초토화되어 마비되었다[3]. 우리나라와 관련된 사이버 테러 사례는 <표 1>과 같이 KBS, MBC, YTN 등 방송사 사이버 테러와 농협, 신한은행과 같은 주요 금융기관 사이버 테러를 예로 들을 수 있다. 사이버 테러를 일으키는 테러 집단은 사이버 테러 공격을 통해 전산망을 마비시키거나 자료 유출, 자료 삭제, 멀웨어와 같은 악성코드를 유포해서 그들의 목적을 달성한다.

<표 1> 사이버 테러 공격 유형 [14,17]

유형	설 명
멀웨어(Malware)	보통 악의적인 의도를 가지고 상대방의 컴퓨터를 파괴시키고 또는 데이터를 훔치는 목적을 가지고 Trojan과 worm을 포함한 악성 코드를 심어서 사이버 위협을 가함
DDos(Denial of Service attack)	감염된 좀비 PC로 특정 시스템을 다수로 공격하여 시스템을 마비시킴
악성코드 다운로드(Drive by Downloads)	상대방이 유도하는 특정 사이트를 방문하는 것만으로도 악성코드가 자동으로 다운로드 되게 하는 공격 방법으로 방문자 PC에 악성코드를 유포함
APT(Advance Persistent Threat)	특정 기업이나 조직 네트워크를 목표로 기밀정보를 빼내는 사이버 테러를 일으킴, APT는 공격 타깃이 정해지면 목표가 달성될 때까지 네트워크를 지속적으로 공격을 가하는 것이 특징임

2.3 국가별 사이버 테러

러시아가 옛 소련의 국가안보위원회(KGB) 후신인 연방 보안국(FSB)과 러시아군 정보총국(GRU) 두 기관을 통해 <그림 1>과 같이 미국 민주당 1명의 컴퓨터에 악성 소프트웨어를 심어서 이메일에 침투하는 해킹 사건 등이 있다. 최근의 국가별 사이버 테러는 상대 국가의 기밀정보 등을 빼내고 국가의 산업, 경제를 위협하는 유형의 사이버 테러가 빈번히 발생하고 있다. 사이버 테러를 일으키는 국가는 주로 러시아, 중국, 북한 등과 같은 국가가 연루되어 있다.

① 북한

북한은 최고사령부와 국방위원회, 노동당을 중심으로 7개 해킹조직 1700여 명의 인력을 운영하고 있다. 또한, 이 해킹조직을 지원하는 조직 및 인력만도 13개 4200여 명 수준이며 북한의 해킹은 한반도 평화에 대한 위협은 물론 전 세계를 위협하고 있다. 북한은 1989년부터 사이버 전 전담인력을 매년 100 명 이상 양성하고 있으며 미 국방성 자체 모의실험 결과 태평양 사령부 지휘통제소를 마비시키고 미 본토 전력망 피해를 유발할 정도의 사이버전을 치를 수 있는 역량을 갖추고 있다[4].

북한의 소행으로 추정된 사이버 테러는 2013년 장거리 미사일 발사 후와 3차 핵실험 직후, 우리나라 주요 방송사와 금융기관 등을 상대로 3·20 사이버 테러와 같은 해 청와대 홈페이지를 해킹해 변조한 6·25 테러가 있다. 또한, 그 이듬해인 2014년에는 유엔의 북한 인권 의제 논의라는 국제사회 제재에 불만을 가지고 자행한 <그림 1>과 같은 한국수력원자력 해킹 사건 등이 있다[6].

<그림 1> 한국수력원자원 해킹 [9]

② 러시아

2009년 1월, 러시아 해커들은 키르기스스탄에 있는 미국 공군기지 사이트를 공격했다. 미국 연방수사국(FBI)과 국토안보부(DHS)는 러시아 정보당국이 미국 대선과 관련해 미국 정당 네트워크에 침투해 해킹을 자행했다. 또한, 러시아 해킹 단체가 'APT29'라는 스피어피싱 기법으로 미국 정당 관계자 1명의 계정에 접근하여 악성 소프트웨어를 유포하였다. 스피어피싱이란 주변 정보를 미리 염탐해 해킹 대상인 당사자로부터 믿을 수 있도록 지인을 사칭하여 이메일을 보내어 악성 코드를 감염시키는 수법을 사용하였다[7].

③ 중국

중국은 미국의 가스공급회사, 정유회사, 통신사업자, 은행, 보험회사 등의 정보 시스템에 침투하여 고객 수천만 명의 민감한 개인정보를 빼내었다. 해킹이 중국 소행으로 추정된 이유는 사이버 공격 시 과거 중국이 해킹할 때 사용하던 소프트웨어 기술과 같은 방법을 사용하였고, 중국 국가에서 사용하는 IP가 일치했기 때문이었다. 또한, 미국의 최대 병원 그룹 중 하나인 Community Health Systems도 중국 해커의 공격을 받아, 약 450만 명 환자의 사회보장

번호와 기타 개인정보가 유출되었다[8].

2.4 우리나라 주요 사이버 테러

최근 우리나라에서도 <표 2>와 같이 사이버 테러가 빈번하게 발생하여 여러 기관에서 피해가 발생하였다.

<표 2> 우리나라 주요 사이버 테러 [10]

발생년월	테러 유형	특징
09년 7월	DDos공격	청와대, 국방부, 옥션, 외환은행, 신한은행 등 국내 12개 사이트를 공격함
11년 .3월	DDos공격	청와대 등 정부공공기관 24곳과 주요 포털 및 금융사 웹사이트 16 개 사이트 등 총 40여 곳을 공격 함
11년 4월	농협 전산망 마비	관리업체 직원의 좀비PC를 활용 하여 농협 전산망에 접근하여 농협 전산망을 마비시킴
13년 3월	방송사·금융기관 전산망 마비	KBS, MBC, YTN 등 방송사와 신한은행, 농협은행, 제주은행 등의 상당수 컴퓨터를 공격하여 마비시킴
14년 12월	한수원 해킹	한국수자력원자력 설계도면 등 한국수력원자력의 내부 자료를 유출 함

Ⅲ. 사이버 테러 공격 유형

최근에 일어난 대부분의 사이버 테러들은 기업 내부 전산망에 연결된 모든 PC에 악성코드를 유포하여 시스템의 데이터 저장영역을 파괴하거나 자료를 유출한다. 또는, 주요 기관 및 기업의 전산망을 마비시키는 행위를 자행함으로써 사회적 혼란을 초래하기도 한다.

3.1 악성코드 유포

악성코드는 가장 널리 많이 사용되는 이메일, 메신저, 웹페이지 등 전달이 손쉽거나 이용자 접속이 많은 웹페이지를 통해서 주로 악성코드를 유포한다. 그러나 최근에는 주로 보안 방화벽이 약하거나 사용자 PC의 취약점이 드러나는 환경에 침투하여, 악성코드를 감염시키고 있으므로 피해가 커지고 있다. 하우리 보안 업체에 따르면 2016년에 몇몇 취업사이트와 파일 공유 사이트, 중소기업, 패션 사이트, 국방 및 국가보훈 관련 연구원에서 악성코드가 발견되었다[16].

- 종류 : 악성코드, 멀웨어
- 피해 : 악성코드로 내부 시스템을 공격하여 개인정보를 유출, 공인 인증서 탈취 등 System 파괴로 인한 전산망을 마비시킴

3.2 디도스(DDos) 공격

DDos(Distributed Denial of Service Attack) 공격도 악성코드와 함께 변칙적으로 해커의 테러 공격기법으로 꾸준히 이용되고 있는 공격 유형이다. DDos의 주요 공격 방법은 상대방 시스템에 대량의 접속을 시도하여 시스템 과부하를 일으켜서 시스템을 마비시키는 수법이다. 2009년 7월 7일 인터넷 대란은 대한민국과 미국의 주요 국가망과 금융권, 포털 사이트 등을 DDos에 의해 전산망 마비로 시스템이 다운된 사건이다[18]. 최근 DDos 공격은 '핵티비즘(hacktivism)' 성격이 강하게 작용하여 정치적, 사회적 목적으로 시스템을 해킹하거나 시스템을 무력화시키는 성격으로 변화되었다[11]. DDos의 변화된 공격으로 예를 들면, 공격자인 해커는 사전에 악성코드를 유포하여 특정 프로그램에 감염시킨 후, 타깃 서버가 정당한 신호를 받지 못하도록 교란과 방해작업으로 무력화시켜서 공격을 가담하게 된다[5].

<표 3> DDos 공격 과정

공격유형	특징
공격자(Attacker)	공격을 주도하는 해커의 컴퓨터
마스터(Master)	공격자에게서 직접 명령을 받는 시스템으로 여러 대의 에이전트를 관리하는 시스템
에이전트(Agent)	공격대상에 직접적인 공격을 가하는 시스템
피해(Victim)	피해 컴퓨터

- 종류 : Trinoo, TFN, tacheldraht, TFN2K
- 피해 : 다수의 시스템이 협력하여 하나의 표적 시스템을 공격하여 시스템을 마비시킴

3.3 파밍(Pharming)

파밍은 악성프로그램에 감염된 PC를 조작하여 사용자가 자신의 웹 브라우저에서 정확한 웹 페이지 주소를 입력해도 그들이 유도하는 가짜 웹 페이지에 접속하게 하여 중요한 정보를 훔쳐가는 수법이다. 21세기 첨단기술은 기업과 국가의 경쟁력의 핵심이다. 만약, 해커에 의해 국가 및 산업과 관련된 중요한 기밀 자료가 유출된다면 국가의 경쟁력을 떨어뜨리고 국가를 위기로 몰아넣고 사회적 혼란을 일으킬 수 있는 위험스런 요소가 있다.

최근 북한은 사이버 테러 공격 대상에 우리나라 주요 기관을 타깃으로 테러를 계획하고 있는 정황이 보이고 있으며 그들의 사이버 테러 음모는 우선적으로 국가적 산업 기반을 혼란시키거나 산업·군사기밀에 관련된 주요 문서를 탈취하기 위한 것으로 알려져 있다. 사이버안전국에 따르면 지난 2013년 3월 20일 북한 평양 류경동 소재의 IP가 우리나라 기업 및 기관을 대상으로 업무용 파일을 탈취한 사이버 테러 행위를 저지른 사실이 발견되었다[12].

- 종류 : 스미싱, 파밍
- 피해 : 내부 전산망에 침입해 16만 명의 고객들 신용카드 정보 및 직불카드 정보 유출

3.4 스피어피싱(Spear Phishing)

스피어피싱은 특정기관이나 기업의 내부직원을 표적으로 삼아 정부기관이나 해당 조직의 신뢰할 수 있는 기관에서 발신한 것처럼 사칭 위장하여 악성 이메일을 관련자들에게 전송시켜 감염시킨 후, 원격제어를 통해 기밀정보를 빼내는 대표적인 지능형 표적공격 수법이다. 최근에는 스피어피싱을 이용해 국방과학연구소(ADD), 한국수자력원자원, 철도기관과 정부 인사 스마트폰 해킹 등 국가 공공기관 뿐만 아니라 전 기관, 전 영역에 걸친 전 방위 사이버 공격이 자행된 사건이 보고되었다[13].

- 종류 : 스피어피싱
- 피해 : 국방과학연구소(ADD), 한국수자력원자원, 철도기관 및 정부기관 등과 같은 기관망

3.5 랜섬웨어(Ransomeware)

랜섬웨어는 이메일 등으로 유포되어 랜섬웨어를 첨부한 이메일을 열어보는 순간 시스템이 감염되어 저장된 데이터가 통째로 삭제되는 등의 치명적인 손상을 입히게 되므로 사회 기반시설과 같은 곳에 특히 피해가 크다. 한 치과 의원에서도 환자의 예약, 보험금 청구, 청구서 발행을 포함한 운영 시스템이 랜섬웨어에 감염되어 접근할 수 없다고 보고했다. 그 다음 날은 랜섬웨어에 감염된 시스템이 또 다른 환자 시스템의 파일을 암호화시키고 의료 장비들까지 마비시켰다[15].

- 종류 : 록키 랜섬웨어, 크립토락커
- 피해 : 농협, 신한은행 전산망 마비

VI. 대응방안 제시

인터넷에 대한 이용률이 생활 속에서 자리매김하면서 사이버 테러가 세계 여러 나라 및 우리나라에서도 빈번하게 일어나고 있다. 사이버 테러는 감염된 좀비형태의 PC로 과부하를 일으키는 DDos에서 특정 기관을 무력화 시키고 노리는 지능형 표적 공격으로 전환되어가고 있다. 즉, 미 국무성의 미사일 방어 자료와 같은 중요한 정보를 훔치는 정치적·이념적·경제적 또는 군사적 목적을 위해 사용되기도 한다. 세계 여러 나라에서는 북한이 사이버 테러에 대한 위협적인 존재 가치가 다분한 나라로 분류하여 사이버테러에 대한 도발이 예상되기 때문에 완벽한 대비책으로 사이버 테러 공격에 대비하기를 권고하고 있다. 4장에서는 이미 시사 보도 된 사이버테러 유형적 사례에 대한 문제점을 분석하여 위험으로부터 대처하기 위한 대응방안을 제시하고자 한다.

4.1 악성코드 유포 대응

악성코드의 목적 의도는 사용자의 동의도 없이 사용자의 컴퓨터에 침투하여 파일을 손상시켜서 피해를 유발하도록 만들어졌다. 그러나 최근 악성코드는 사용자가 많이 사용하는 웹사이트, 이메일의 첨부된 파일을 실행하면서 또는 감염된 파일을 다운로드하면서 감염되므로 그 피해에 대한 파장이 아주 크다. 우선적으로 악성코드에 대한 감염 피해를 줄이기 위해서는 업데이트된 최신 백신프로그램을 통해 악성코드 감염여부를 주기적으로 검사해야 되며 수상한 웹사이트나, 모르는 이메일 등은 접근 차단과 함께 무조건 삭제하여 열어보지 않도록 주의하도록 한다.

또한, 웹사이트의 팝업광고를 통해서도 악성코드에 감염될 수 있기도 하는데 이런 경우를 대비해 브라우저 확장 기능 중에서 광고차단 기능 및 애드블럭 기능을 사용하길 권장한다. 만약, 해커에 의해 웹사이트가 악성코드 유포지가 된 웹사이트라고 판단되면, 신속히 사이버침해신고센터에 신고하고 차단해야 하며 악성코드 피해 확산을 줄이기 위해 일시적으로 웹페이지를 폐쇄하는 것도 좋은 방법이다.

4.2 디도스 공격 대응

DDos 공격은 대부분 DNS의 보안이 열악한 시스템이 노출되어 공격 대상에 포함된다. 과거 DDos 공격은 주로 상대 시스템에 접속을 폭주하여 시스템을 과부하 시킨 뒤, 마비되도록 하여 중대한 자료까지 유출하는 사고를 유발했다. 무엇보다 DDos 공격을 사전에 탐지 및 예방하기 위해서는 시스템 보안에 대한 강화는 필수적이고 변칙된 DDos 공격에 대비해야 한다. 변칙된 DDos 공격이라 함은 공격 방식이 기존 공격방식에 비해 훨씬 짧아지고 공격 패턴도 랜덤하게 다양한 변화를 주기 때문에 보안 업체에서도 이를 가름하기가 어려우므로 피해가 증폭될 수 있다. 그러므로 기존 DDos 보안 솔루션으로는 새로운 지능형 DDos 공격에 대응하기가 더욱 어려워지게 된다. 다양하게 변화된 DDos에 대응하기 위해서는 가장 기본적으로 현 보안 솔루션이 제대로 동작하여 실시간으로 IP 자동 탐지가 가능한지, 침입에 대한 필터링과 차단에 대한 제어가 가능한지를 점검한다. 또한, 문제적 네트워크로부터 서버를 안정되게 운영하기 위해서 물리적 망분리, 서버가상화기반 망분리, 클라이언트기반 망분리를 서버 운영 기반에 따라 2, 3개로 분리하여 서버 망을 별도로 운영

하는 것을 적극적으로 권장한다. 또한, 외부 네트워크 액세스에 대해서는 실시간 모니터링을 통해 비정상 패킷에 대해서는 패킷을 추적하고 이를 필터링으로 제어가 가능한지도 반드시 점검해 보아야 한다.

4.3 자료 유출 대응

자료 유출은 대부분 업무 시스템의 장애를 초래하여 업무 진행을 못하게 방해하고 대외 적인 서비스의 사용을 중단케 하여 자료를 유출을 강행한다. 지금까지 대부분의 자료 유출 사고는 사고 대응에 대한 체계가 신속하지 못하고 관리 수준이 미흡한 수준이어서 그 피해가 더욱 컸던 것으로 분석되었다. 사이버 테러에 의한 자료 유출은 앞에서 설명한 악성코드 유포, DDos에 의한 기본적 대응방안과 유사하다. 조사된 자료에 의하면 고객정보 유출 및 기업의 특급 기밀 자료 유출은 대부분 내부 수행자에 의한 경우로 기업 경영에 심각한 재정적 타격을 주었다. 산업 기밀 정보 및 핵심 기술 자료를 내부직원으로 부터 보호하기 위해서는 우선 산업기술과 같은 내부 기밀문서 이용 제한에 대한 통제가 특별히 관리되도록 강화되어야 한다. 무엇보다 보안 책임자는 내부 전산실 이용에 관한 제한적 규정을 철저히 이행하도록 해야 하며 자료 접근·열람·이용에 대한 내부 규정 방침을 적극적으로 홍보할 필요가 있다.

현재 국가 정세가 시기적으로 안정되지 못한 요즈음, 국가 중요 기밀자료 및 산업 설계자료 등의 관리는 무엇보다 중요하다. 만약, 국가 기밀 및 기관 주요 자료가 유출된다면 국가 경쟁력을 떨어뜨리고 사회적 혼란을 일으킬 수밖에 없다. 그러므로 정부의 관리자 및 보안 관계자는 자료관리에 대한 중요성을 인식하고 철저한 보안의식 고취와 함께 더욱 강화된 보안 활동에 신경을 써야 한다.

4.4 긴급 대책 운영반 구축

2014년 한국수력원자원 산업제어시스템이 해킹당하여 국가가 위기에 빠질 수 있는 위험한 상황이었으며, 이에 국가 기관 전산망 보안 관리가 얼마나 소홀했는지를 말해주는 계기의 사건이었다. 우리나라 기관 망은 북한과 대치되어 혹시나 방송국, 기간 통신망, 수자원, 에너지, 전력과 같은 국가 산업 망이 북한해커에 의해 무력화된다면 전국의 산업 망이 마비될 수 있는 아주 위험한 상황이 연출될 수도 있다. 위에서 살펴본 한수원 사태가 재발하지 않도록 예방 방지하기 위해서는 정부 기관을 주측으로 민·관·군에 대한 합동 사이버안전센터와 같은 긴급 전담 비상대책 운영반 신설이 필요할 듯싶다. 구체적인 업무별 분장 부서는 보안사고 대책반, 비상사태 복구반, 망 분리 구축반, DB 백업/복구 반, 침해 분석반, 암호 해독반 등과 같은 IT 보안과 관련된 전담반을 주축으로 세부적으로 구성해야 하며 무엇보다 북한군과 관련된 사이버테러 전에 대비하는 전담요원 양성도 시급하다고 본다.

4.5 금융 전산망 대응

대체로 우리나라 전산 금융망은 그 어느 기관보다도 해킹 및 악성코드 등에 안정적이고 보안 솔루션도 제대로 가동되고 있다고 인식하고 있다. 그러나 금융 전산망이 북한 해커에 의해 해킹되었을 경우, 제대로 금융 보안 솔루션이 작동되었는지 아니면 외부 IP 침입에 대한 분석이 제대로 되었는지를 다시 한 번 점검해 보도록 해야 한다. 금융 대란 시 제대로 된 보안 솔루션이 정상적으로 작동만 되었더라도 금융 전산망 대란에 대한 피해는 아마도 어느 정도 최소화되었을 것이다. 당시는 아마도 침해에 대한 대응이 다소 지연되었거나 사건에 대한 분석이

늦었기 때문에 연속적인 금융 사고가 발생하였다고 보이고 있다. 본 논문에서는 서버 운영에 있어서 망 분리 솔루션을 강력히 제안한다. 대부분 전산망에서 이 방법을 인지는 하고 있지만 금전적인 부분과 번거로운 부분으로 인해 대부분 이행하지 못하고 있는 것이 안타까운 현실정이다. 더 큰 금융 사고를 당하지 않고 예방하는 차원에서 금융 전산망 운용 시스템은 당연히 서버 분리 운영과 백업 서버가 실시간으로 제대로 운영되고 있는지를 반드시 확인하고 실천해야 하길 제안한다.

<표 4> 위험 대응방안 제시

위험 요소	대응방안
악성코드	보안과 관련된 악성코드 DB업데이트가 최근 3개월 이내에 이루어졌는지를 확인하고 최근 시사된 악성코드를 탐지할 수 있는지 여부를 확인한다.
애드블럭	브라우저 자체에서 애드블럭 기능을 통해 광고를 차단하는 경우와 광고에 대한 부분을 강력하게 차단할 수 있는 어플을 설치하여 운영하도록 한다.
네트워크 망	업무용 PC기반과 클라우드 기반에 대한 서버를 별도로 구축하여 운영하되, 특히 클라우드 기반의 외부 액세스 자료 업무에는 강력한 암호화된 보안 솔루션을 도입하여 함께 운영한다.
비정상 패킷	비정상 트래픽의 흐름을 탐지하는 실시간 모니터링과 비정상 패킷 탐지에 대해서는 필터링으로 차단하고 추적기능과 제어 기능을 동시에 수행한다.
랜섬웨어	랜섬웨어 의심이 가는 이메일은 열어보지 않거나 접근을 자제한다. 또한, 기관내 서버 운용에 있어서는 데이터를 동기화하고 실시간으로 백업을 받고, 외부와 연동되어 액세스되는 저장장치 영역에 대해서는 암호화를 통해 접근 통제 영역을 강화한다.

Ⅴ. 결론

본 논문에서 살펴본 바와 같이 사이버 테러는 해커공격 때문에 각종 악성코드 및 DDos와 같은 공격이 네트워크를 통해서 홈페이지, 이메일, 모바일 디바이스 환경에서 사회 공학적 문제를 일으키고 있다. 정황적으로 북한의 사이버 테러 도발 행위가 추정되고 있는 시점에서 사이버 테러에 대한 대비는 훨씬 더 철저한 준비를 많이 해야 한다. 현재 사용하고 있는 보안 솔루션의 문제점 실태를 다시 한 번 파악하고 신종 악성코드를 제대로 탐지할 수 있는지에 대해서 점검 해 보는 것이 좋을 듯싶다. 본 논문에서는 민·관·군 긴급 대책 운영반 구축과 같은 사이버안전센터 설립 운용과 국내 대학과 연계된 사이버 IT 전문 인력 양성도 국가적인 측면에서 더욱 고려해볼 것을 제안하였다. 특히, 대규모 사이버 테러 공격 비상사태에 대비하기 위해 정부 및 각 기관 언론 통신망과의 원활한 공조 체계를 이루어서 국가 비상대책 운영에 빨간 색 불이 들어오지 않도록 미리 대책을 세우는 것도 함께 제안하였다. 지금은 시기적으로 볼 때 국민 모두가 하나 되어 사이버 테러에 대한 안보 의식을 고취하고 사이버 국가 재난에 비상 체제를 굳건히 다져야할 절대적인 시기라고 본다.

참고문헌

[1] 신현조, 이경복, 박태형, “인적 및 직무특성과 보안교육 이수율 및 사이버테러 대응과의 연관성 분석,” 디지털산업정보학회, 제10권, 제4호, 2014년, p. 98.

[2] 곽병선, “사이버테러 대응을 위한 법체계 검토,” 한국법학회, 제59집, 2015년, p. 2.

[3] 김태계, “사이버테러 범죄 대응에 관한 제도적 문제점과 대책,” 한국법정책학회, 제14집, 제3호, 2014년, p. 1346.
[4] 정기석, “최근의 사이버테러에 대한 대응방안,” 정보보안 논문지, 제12권, 제1호, 2012년, p. 92.
[5] 권양섭, “사이버 범죄 처벌규정의 문제점과 대응방안,” 한국법학회, 제53집, 2014년, pp. 186.
[6] http://www.voakorea.com/a/3443836.html
[7] http://www.hani.co.kr/arti/international/america/776799.html#csidx5440747dcd90c4789e3152d9f13112a
[8] http://www.dailysecu.com/news/articleView.html?idxno=7673
[9] http://www.hankookilbo.com/m/v/8ef329feb1db439cbac47c6fdb3825a5
[10] www.nars.go.kr\’이슈와논점’\제640호\2013년4월18일
[11] http://www.zdnet.co.kr/news/news_view.asp?artice_id=20141022172754&type=det&re=#csidx6e88e2365fed2518b91f5d4f16108c3
[12] http://www.itworld.co.kr/slideshow/86276#csidx615b2c1176b76c7a91d6ab57cf225f7
[13] http://www.etnews.com/20161013000198
[14] http://quickbooks.intuit.com/r/technology-and-security/8-types-of-cyber-attacks-your-business-needs-to-avoid
[15] http://www.itworld.co.kr/howto/101250
[16] http://www.boannews.com/media/view.asp?idx=49946
[17] http://www.dailysecu.com/news/articleView.html?idxno=131
[18] 서우석, 박대우, 전문석, “TCP/IP Layer별 공격 패턴 분석에 기반한 CFC를 이용한 DDoS 방어 알고리즘 연구,” 디지털산업정보학회, 제 6권, 제4호, 2010년, p.118.

■ 저자소개 ■

최 희 식
(Choi Heesik)

2008년 3월~현재
삼육대학교 컴퓨터학부 외래교수
2002년 2월 숭실대학교 컴퓨터학과(공학박사)
2006년 2월 숭실대학교 컴퓨터공학과 (공학석사)

관심분야 : 정보보안, 클라우딩컴퓨터, IoT 핀테크 금융보안
E-mail : dali3054@ssu.ac.kr

김 현 규
(Kim Hyunkyu)

2012년 9월~현재
삼육대학교 컴퓨터학부 조교수
2010년 2월 한국과학기술원 전산학과 (공학박사)
2000년 2월 울산대학교 전산학과(공학석사)
1997년 2월 울산대학교 전산학과(공학사)

관심분야 : Database, Data Stream Processing, MapReduce
E-mail : hgkim@syu.ac.kr

논문접수일 : 2017년 02월 01일
수 정 일 : 2017년 02월 15일(1차), 02월 28일(2차)
게재확정일 : 2017년 03월 03일