The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 6, pp.283-290, Dec. 31, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.6.283
JIIBC 2015-6-39

금융권 PC보안 위협 분석 및 대응방안에 관한 연구

A Study on Threat Analysis of PC Security and Countermeasures in Financial Sector

한경희*, 김인석**

Kyung-Hee Han*, In-Seok Kim**

요 약 산업혁명 이후 지식 정보화 사회로 발전되면서 기업 내부 정보의 가치는 갈수록 증가하고 있다. 특히 금융회사는 대부분의 내부정보가 개인정보나 금융거래 정보를 포함하고 있어 내부정보의 유출은 단순히 해당 기업의 업무 정보 유출 차원을 넘어, 궁극적으로 고객의 신뢰를 존립 기반으로 하는 금융회사의 특성상 기업의 영업기반이 한순간에 무너질 수도 있는 리스크가 걸린 문제이기도 하다. 최근 내부 정보의 대량 유출 사고가 다수 기업에서 발생하면서 금융회사를 포함한 많은 기업에서 기업의 주요 전략적인 정보와 함께 고객정보의 유출 사고를 예방하기 위해 많은 노력을 기울이고 있다. 본 논문에서는 금융회사에서 발생한 내부 정보 유출 사례와 금융회사에 내부 정보 유출 통제를 위해 구축한 주요 보안 체계 및 내부정보 유출 통제에도 불구하고 잔존할 수 있는 PC보안 취약점에 대해 설명하고, 사이버 침해 위협이 증가로 인한 사용자 PC 보안위협 대응방안에 대해 제시한다.

Abstract As society has evolved to the knowledge and information society, the importance of internal information of the company has increased gradually. Especially in financial institutions which must maintain the trust of customers, the disclosure of inside information is a big problem beyond the a company's business information disclosure level to break down sales-based businesses because it contains personal or financial transaction information. Recently, since massive outflow of internal information are occurring in several enterprises, many companies including financial companies have been working a lot in order to prevent the leakage of customer information. This paper describes the internal information leakage incidents occurred in the finance companies, the PC security vulnerabilities exists despite the main security system and internal information leakage prevention and suggests countermeasures against increasing cyber infringement threats.

Key Words : PC security threats, PC security threat countermeasures, Financial security incidents, Personal Information extrusion,

Ⅰ. 서 론

최근 개인정보 및 신용정보 유출로 인한 국가적·경제적 손실이 심각한 상태이며 이러한 유출은 특히 전·현직 직원 및 외부 협력업체 직원과 같은 내·외부 직원에 의해서 가장 빈번하게 발생하는 것으로 나타나고 있다.[1]

인터넷 정보통신 환경의 변화로 인해 사이버 침해위협이 증가하고 있고 해킹이나 도청과 같은 기술적인 방식 등 다양한 형태로 유출이 이루어지고 있다.[2]

또한, 사이버 공격의 대부분이 민간부분의 PC에 의해서 이루어지기 때문에 국가차원의 정보보호를 위해서는 민간부분의 정보보호가 필수적이다.

*정회원, 고려대학교 정보보호대학원 금융보안학과 금융보안정책전공
접수일자: 2015년 11월 15일, 수정완료: 2015년 12월 7일
게재확정일자: 2015년 12월 11일

Received: 15 November, 2015 / Revised: 7 December, 2015 / Accepted: 11 December, 2015
**Corresponding Author: iskim11@korea.ac.kr
Dept: Center for Information Security Technologies, Korea University

백신 S/W를 사용하지 않거나 검사를 제대로 수행하지 않고 보안 패치 등 예방 활동에는 소극적으로 악성코드에 감염위험이 있는 PC는 491만여 대 이상으로 7.7 DDoS 침해사고에 동원된 좀비 PC(11만 5천여 대)의 약 43배에 해당한다.[2]

2015년 2분기 맥아피 연구소 위협 보고서에 따르면, 사이버 범죄는 금융, 무역 시스템, 공급업체, 시장, 서비스 제공업체 및 비즈니스 모델의 확산과 더불어 성숙한 시장으로 성장했으나 사용자는 여전히 백신 업데이트, 소프트웨어 보안 패치, 비밀번호 관리, 그리고 중요한 자산 보호 방법에 최소한의 관심을 기울이지 않고 있는 점을 최대 이변으로 손꼽았다. 보안 산업은 수십 년 동안 지속적으로 이 점을 강조해왔지만 여전히 공격 성공 가능성이 가장 높은 맹점으로 남아 있다.[3]

이에 본 연구의 2장에서는 PC 보안 위협의 의의와 실태에 대하여 파악하고, 3장에서는 PC 보안 위협 대응제도 및 체계에 대하여 조사하고, 4장에서는 효과적인 PC 보안 위협 대응 요소에 대하여 연구한다. 자동점검 방안을 적용하여 PC 보안 위험요소를 줄이고, 보안수준을 높이는 방안을 제시하고자 한다.

II. PC 보안 위협의 의의와 실태

2장에서는 PC 보안 위협 및 정보보안 사고사례를 통하여 문제점을 도출하고 기준 자료로 활용한다.

1. PC보안 위협

국내 주요 사이트는 실제 악성코드를 직접 유포하는 유포지로 사용되기도 하며, 악성코드 유포지 링크를 웹페이지 내에 가지고 있는 경유지로도 이용되고 있다. 특히 공격자들은 목표 PC를 감염시키기 위해 목표 대상이 자주 접속하는 정상적인 웹 사이트를 경유지로 이용하고 있다. 그리고 공격자들은 탐지를 회피하고 악성코드의 생존율을 높이기 위해 다단계로 경유지와 유포지를 구성하기도 한다. 또 지속적으로 경유지와 유포지를 변경하여 노출을 최소화해 악성코드 대응활동을 우회하고 있다.

2015년 10월 한국인터넷진흥원에서 발표한 악성코드 은닉사이트 탐지 보고서에 따르면, 악성코드유형 [그림 1]으로 공인인증서, 비밀번호 등 금융정보를 탈취 하는 악성코드로 71% 가장 많았고, 드롭퍼, PC정보유출 악성코드, 다운로더, 정보 유출(계정정보), 애드웨어, 해커가 원격지에서 좀비PC를 제어하는 목적으로 이용하는 악성코드 순으로 다양하게 나타났다.[4]

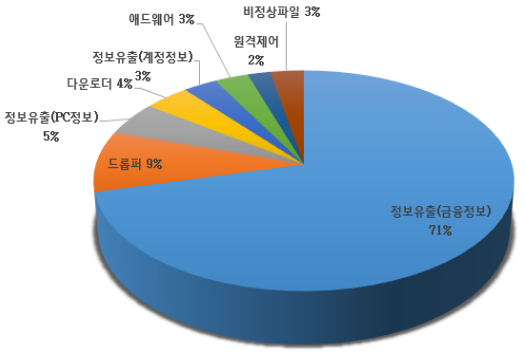

그림 1. 탐지된 악성코드 유형별 비율
Fig. 1. Ratio of Detected Malicious Code Types

2. 금융권 정보보안 사고와 PC 보안위협

2.1 금융권 정보보안 사고 사례

최근 수년간 외부로 부터의 해킹이나 공격에 의한 금융권에 막대한 피해를 입힌 사이버 공격 및 주요정보 침해사고 관련 사건을 분석하고자 한다.

표 1. 금융권 및 주요 기관 대형 해킹 사고
Table 1. Large-scale Hacking Incidents in Financial Sector and Major Institutions

시기	기관	사고 원인
2009.07	7개 금융회사	외부 해킹
2011.03	9개 금융회사	외부 해킹
2013.03	일부 방송사 5개 금융회사	외부 해킹
2013.06	69개 기관.업체	외부 해킹

2009년 7·7 분산 서비스 거부 공격(DDoS)은 공격에 사용된 웜 중 일부에서 감염된 컴퓨터의 하드 디스크를 파괴하는 코드가 발견되었으며, 2011년 3·3 DDoS 공격은 7·7 DDoS 공격보다 진화된 형태로 일정 기간을 두지 않고 하드디스크 파괴 명령을 받은 즉시 하드 디스크를 파괴하도록 설정되어 있었다.[5]

2013년 3·20 전산 대란은 주요 언론과 기업의 전산망이 마비되고 3만 2천여 대의 컴퓨터가 악성코드에 감염되어 피해를 입은 사건이다. 정상 파일로 위장한 악성코드가 기업 PC에 침투한 후 실행되어 전산망 마비를 시켰고, PC에 저장되어 있는 자료가 유출되었다.[6]

2013년 6·25 사이버 대란의 경우 기존 좀비PC를 이용한 공격과 달리, 공격자가 특정 웹사이트에 악성스크립트를 설치하고 사용자들이 이 사이트를 방문하면, 미리 설정해 놓은 웹사이트로 공격 트래픽을 발생시키는 방식이다.[7]

아래 [표 2]와 같이 주요정보 침해사고를 분석해 보면, 공격자는 주로 이메일을 이용하여 메시지 본문 내용에 포함시키거나 첨부 파일의 형태로 데이터를 기업 외부로 전송하거나, 주요 정보를 프린터 출력, 스마트폰을 이용한 사진촬영, 카드형 USB 저장장치에 복사, 내부직원, 외부업체 직원 등 내부와 외부를 연결해 주는 인터페이스 및 매체관리 보안 솔루션의 부재로 인한 취약점을 이용하였음을 발견하였다.[3]

표 2. 금융권 개인정보 유출 사고
Table 2. Personal Information Breaches in Financial Sector

시기	기관	구분	피해규모(건)	유출경로
2011.8	S 카드	내부직원	80만	프린터 출력
2011.10	H 카드	내부직원	9만7천	이메일
2011.12	I 캐피탈	내부직원	5천8백	프린터 출력 사진촬영
2012.05	M 화재	내부직원	16만4천	USB 복사
2013.12	S 은행 C 은행	협력업체 내부직원	13만	USB 복사 프린터 출력
2014.1	K 은행 L 카드 N 은행	협력업체	1억4백만	USB 복사

2.2 금융권 PC 보안 위협

미래창조과학부와 한국인터넷진흥원에서 2014년 기업부문 정보보호 실태조사 조사 자료에 의하면, 정보시스템 보안 점검을 수행하는 사업체의 취약점 점검 항목은 'PC 취약점'이 72.6%로 가장 높았고, 다음으로 '네트워크 취약점'(49.5%), '운영체제 취약점'(41.2%) 순 이었다.[8]

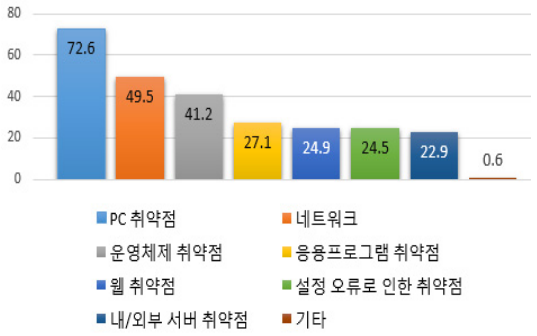

그림 2. 취약점 점검 항목(복수응답)-취약점 점검 수행 사업체
Fig. 2. Vulnerability Check Items (Multiple Responses) In Vulnerability Check Performing Enterprises

또한, 보안패치 업데이트를 자동 또는 수동으로 실시하는 비율은 '로컬 서버'가 80.1%로 가장 높았으며, '네트워크 서버'가 66.4%, '직원 개인용 PC'가 64.2% 순으로 조사되었다.[8]

3. PC보안 위협 대응 현황

한국인터넷진흥원에서 2014년9월 최근 피싱, 파밍 기법을 이용한 금융정보탈취 동향 자료에 따르면, 악성코드 감염 대응방안을 다음과 같이 제시하고 있다.[9]

① 소프트웨어를 항상 최신 보안 업데이트를 적용
② 백신 프로그램을 항상 최신으로 업데이트하고 주기적으로 백신 점검한다.
③ 출처가 불분명한 파일이나 불법 프로그램을 사용하는 경우 파일을 함부로 열어보지 않는다.
④ 지나치게 많은 정보를 요구할 때는 파밍 악성코드를 의심 한다.
⑤ 보안성이 높은 OTP를 사용하는 것을 권장한다.
⑥ 이메일 필터링으로 대량 피싱 공격 제거한다.

Ⅲ. PC 보안 위협 대응제도

3장에서는 금융 및 개인정보와 관련한 제도를 분석한 바, 현재 금융회사들이 준수하고 있는 국내 법률 중에서 최근 가장 사고가 많았던 개인정보 유출 및 PC 보안 위협과 관련된 법령에 대해 분석하여 문제점을 도출하는데 기준 자료로 활용한다.

1. PC보안 위협 대응에 관한 법령

1.1 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정보통신망 이용촉진 및 정보보호 등에 관한 법률 및 같은 법 시행령에 따라, 정보통신서비스 제공자등이 이용자의 개인정보를 취급함에 있어서 개인정보가 분실·도난·누출·변조·훼손이 되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 기술적·관리적 보호조치의 최소한의 기준을 정하는 것을 목적으로 한다.

1.2 개인정보보호법

개인정보보호법 시행으로 인하여, 기업에서는 고객의 개인정보를 취급함에 있어 기술적·관리적·물리적 안전성 확보 조치를 해야만 한다. 고객정보가 유출 시 대응 절차도 가지고 있으며 개인정보유출 가능성을 항상 열어두고 주기적인 교육 및 점검을 해야 한다. 또한, 협력업체에 제공하고 있는 개인정보에 대해서는 정기적으로 방문해서 협력업체의 정보보호 수준을 점검 하고 개선사항을 도출해야한다.

1.3 신용정보의 이용 및 보호에 관한 법률

신용정보회사 등은 신용정보의 정확성과 최신성이 유지될 수 있도록 신용정보 등록·변경 및 관리 등을 하여야 하고, 신용정보 전산시스템에 대한 제3자의 불법적인 접근, 입력된 정보의 변경·훼손 및 파괴 그 밖의 위험에 대하여 마련해야 할 기술적·물리적·관리적 보안대책의 구체적인 기준을 준수해야 한다.

2. 금융권 PC 보안 위협 대응체계

2.1 추진체계

2.1.1 금융 감독 체계

현행 우리나라 금융 감독 체계는 기획재정부, 한국은행, 금융위원회, 금융감독원, 그리고 예금보험공사로 구성되어 있다. 현행 금융 감독 체계에서 각 조직의 역할을 살펴보면 다음과 같다.

기획재정부는 거시경제정책과 국제금융정책을 총괄하고, 한국은행은 거시건전성 감독업무 수행을 위하여 금융감독원과 자료 공유 및 금융기관 검사 및 공동검사를 요구할 수 있다. 금융위원회는 금융정책과 감독정책을 동시에 수행하고 있다. [10]

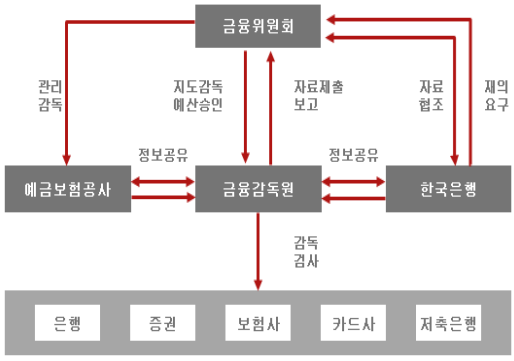

그림 3. 금융 감독 시스템
Fig. 3. Financial Supervision System

2.1.2 사이버 위협 시 추진체계

현재 금융권 사이버 위협 대응기관으로는 국가사이버안전센터(National Cyber Security Center, NCSC), 금융위원회, 금융감독원, 금융ISAC으로 구성되어있다.

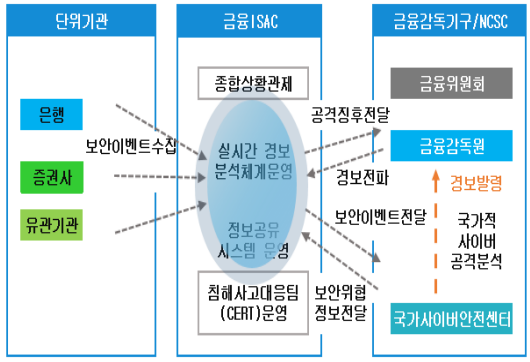

그림 4. 금융권 해킹, DDoS공격 사이버 위협 대응 체계
Fig. 4. Cyber Threat Response System against Hacking and DDoS attacks in Financial Sector [11]

국가사이버안전센터는 사이버보안에 대한 국가차원의 종합적·체계적인 대응 목적으로 설립 되어, 사이버공격 탐지 시 금융감독원 및 금융위원회에 경보발령을 내린다.[12]

금융ISAC은 침해위협 예방 및 침해사고 대응방안으로 금융회사 및 전자금융업자 요청에 따른 침해사고 원인분석, 초동조치, 대응방안 강구, 피해확산 및 재발 방지 대책 수립 전파 업무를 수행한다.[13]

2.2 근거 및 주요내용

전자금융감독규정에 근거하여, 정보기술부문 안정성 확보 조치 기술적 활동 준수하기 위한 PC 보안 점검사항 및 정보보호 대응방안에 대해 확인해 본다.[14]

제12조(단말기 보호대책)를 준수하기 위한 대응방안은 표3과 같다.

표 3. 단말기 보호대책에 따른 대응방안
Table 3. Countermeasures in Accordance with the Terminal Protection Measures

점검사항	단말기를 무단으로 조작하지 못하도록 조치
	정산한 사용자인가의 여부를 확인할 수 있는 기록 유지
	보조기억매체 및 휴대용 전산장비에 접근하는 것을 통제
대응방안	사용자 계정을 설정하고, PC보안을 통해 계정관리 및 일정기간 이후 패스워드 변경 유도
	접근제어시스템 등을 이용하여 계정별 권한을 부여하고 사용자 계정의 접근기록 유지
	PC보안 및 네트워크 제어 시스템을 이용하여 접근을 통제하고 접근기록 유지

전자금융감독규정 제13조(전산자료 보호대책)를 준수하기 위한 대응방안은 표4 와 같다.

표 4. 전산자료 보호대책에 따른 대응방안
Table 4. Countermeasures According to the Electronic Data Protection Measures

점검사항	개인별 사용자 계정 관리
	작업권한에 따른 외부인계정 관리 및 통제
	전산자료의 보유현황 관리 및 책임자 지정
	전산자료 보유현황 및 관리실태 점검 및 책임자 확인
대응방안	PC보안 및 보안OS를 통한 계정관리
	자료유출방지 시스템 및 DB보안을 통한 전산자료 관리
	DRM 시스템 및 개인정보필터링 시스템을 통한 단말기내 주요정보 통제

전자금융감독규정 제16조(악성코드 감염 방지대책)를 준수하기 위한 대응방안은 표5와 같다.

3. 소결

금융 IT감독·검사 추진방향이 금융회사가 자율적인 IT 보안 체계를 확립할 수 있는 기반을 조성함으로써 금융소비자 보호 및 편의성을 제고하려는 노력과 금융회사들이 준수해야할 보안 원칙만 규정하고 구체적인 방안은 보안지침 등으로 정하도록 하여 금융회사 자율성 및 책임성을 강화하도록 규제 패러다임의 변화가 있으나, 현재로서는 기술적 보안운영에만 초점이 맞춰진 컴플라이언스 중심의 보안의 한계점이 있다.[15][16]

표 5. 악성코드 감염 방지대책에 따른 대응방안
Table 5. Countermeasures According to the Information Processing System Protection Measures

점검사항	악성코드 검색프로그램 등으로 진단 및 치료 후 사용
	악성코드 검색 및 치료프로그램은 최신상태로 유지
	악성코드 감염에 대비하여 복구 절차를 마련
	중요 단말기는 악성코드 감염여부를 매일 점검
	악성코드 확산 및 피해를 최소화하기 위하여 필요한 조치
대응방안	안티바이러스 시스템 운영
	외부유입파일 보안관리 시스템 운영
	패치 시스템 운영

Ⅳ. 효과적인 PC 보안 위협 대응 요소

1. PC 보안 위협 대응 개선 방안

금융회사의 보안시스템의 종류는 약 60개 정도로 추정된다. DDoS 차단 시스템과 같은 특별한 용도를 제외하고는 모두 “기밀성” 보장을 위한 것으로 내부 정보 유출 통제와 직접 혹은 간접적인 관련이 있다. 그중에서도 대표적인 내부 정보 유출 통제를 위한 PC측면의 보안솔루션 및 방안은 다음과 같다.

가. PC 보안 프로그램

PC보안시스템은 PC에서 내부 정보가 외부로 유출되는 것을 차단하기 위한 솔루션을 의미하는 것으로 사내에서 발생하는 대부분의 내부 정보가 유출되는 사고가 업무용 PC를 경유지로 한다는 점을 감안할 때 가장 핵심적인 보안 시스템이라고 할 수 있다. 보안 정책에 따라 해당 PC에서 USB, SD, CF 메모리, CD, DVD 등의 이동형 저장 장치에 대한 읽기/쓰기 통제(매체 제어), PC에서 파일 공유 통제, 인터넷 게시판에 글을 올리거나 외부로 메일 전송 시 파일 첨부 통제 등을 기본 기능으로 하며, 제품에 따라 특정 프로그램(프로세스)의 실행을 제한하거나 반대로 특정 프로그램만 실행할 수 있

도록 제한할 수도 있는 등 다양하게 확장될 수 있다.

나. 보안USB 시스템

보안 USB 솔루션은 사용자 PC에서 USB 메모리 읽기 기능은 일반적인 USB 메모리에서 모두 호환 가능하지만, 저장 기능은 하드웨어 또는 소프트웨어적으로 자체 암호/인증 기능이 내장된 특정 USB 메모리 기기만 사용 가능토록 해주는 것으로, 사용자가 USB 메모리를 분실했을 때 외부 취득자가 그 속에 저장된 자료를 읽지 못하도록 제한하는 기능을 제공한다.

다. 문서보안(DRM)

DRM은 암호화 기술을 이용하여 디지털 콘텐츠의 불법적 접근과 복제를 방지하는 기술로, 상업적으로는 영화, 음악, 이미지 등의 디지털 콘텐츠를 보호하는 기술로 활용하고 기업 내부에서는 디지털 형태의 문서 자료가 임의로 유출되는 것을 차단하는 용도로 활용한다. DRM은 암호화 기술을 기반으로 문서에 대한 인증 및 권한부여, 문서등급 및 사용자 권한에 따른 열람 및 복사제어, 웹화면 복사방지, 출력 시 워터마크 삽입 기능을 제공하고, 기능의 확장 여부에 따라 노트북 사외반출, 문서 반출절차 등의 승인 프로세스를 구현할 수 있다.

라. 개인정보 검색 솔루션

사용자 PC내 고객정보가 포함된 자료를 자동으로 검색해서 중앙 관리자 및 PC 사용자에게 통보하여 사용자가 불필요한 자료를 직접 확인 후 삭제하고 업무상 필요한 자료는 따로 모아서 체계적으로 관리할 수 있도록 지원해주는 솔루션이다.

마. 하드디스크, 백업 테이프의 데이터 영구삭제

하드디스크가 포함된 PC/서버나 백업 테이프, 메모리 저장장치 등이 업무 종료나 고장, 용도 폐기되어 외부로 반출될 경우 그 속에 저장된 자료를 영구히 삭제하여야 한다.

2 자동점검 방안

매년 정책과 절차를 검토할 수 있는 데이터 위험 관리 프로세스를 규정한다. 위험을 평가하고 규정 준수를 관리할 수 있는 위험 관리 소프트웨어를 도입하는 방안을 고려해야 한다. 자동 운영체제 업데이트를 활성화하거나 운영체제 업데이트를 주기적으로 다운로드하여 운영체제를 알려진 취약성에 대해 패치 적용된 상태로 유지한다.

미래창조과학부와 한국인터넷진흥원에서 진행한 국내 인터넷 이용자들의 '2014 인터넷 이용환경 현황' 조사 결과, PC 운영체제(Operating System, OS)의 경우 MS사의 윈도우즈(Windows)를 97.76% 사용하고 있는 것으로 파악되었다.[17] 이에 금융권의 대부분 PC 사용자가 윈도우즈 운영체제를 사용하고, PC 보안 프로그램 및 문서 암호화 프로그램을 설치·운영에 기반 하여 중요한 보안 업데이트, 바이러스 점검, 보안정책관리 등에 대한 자동점검 방안에 대해 살펴본다.

윈도우즈 시스템이 종료할 때나 리부팅 할 때 응용프로그램들을 종료시키는데 이때 'WM_QUERYENDSESSION'은 메시지로서 사용자가 세션을 끝내려고 할 때나 임의의 프로그램이 시스템 셧 다운 시스템 콜의 하나를 호출 했을 때 응용프로그램으로 보내진다.

PC 종료 버튼 클릭 이벤트가 발생했을 때 바이러스 점검 프로그램을 사례로 사용 방법을 알아본다.

[사용자 사용 방법]

① 사용자가 PC 종료 버튼을 클릭 시 화면보호기를 띄운다.
② 사용자가 PC를 즉시 종료할 것인지, 재부팅해서 바로 사용 할 것인지 여부를 선택하도록 한다.
③ PC를 즉시 종료 요청 시 보안점검을 수행한다.
④ 보안점검 수행 시 바이러스 프로그램 업데이트, 바이러스 점검 및 보안 정책 적용을 수행한다.
⑤ 점검이 종료되면 PC를 자동 종료한다.

바이러스 발견 시 사용자 요청을 기다리지 않고, 자동치료되도록 설정한다. 이와 같은 방법 적용 시 근무시간에 부재중인 사용자 PC의 경우에도 누락하지 않고 보안점검이 가능하다. 실제 운영 결과, 백신 업데이트 및 바이러스 점검, 문서 암호화 수행 확률이 15% 향상되었다.

3. 데이터 유출 사전 대응 방안

PC보안솔루션의 로그분석을 통한 개인정보 유출 차단을 위한 정책 연구에서 언급한 바와 같이 의심행위자를 지정하고 별도 관리함으로 사전에 개인정보유출 차단하는 시나리오를 구성해 보고 통제하면 데이터 유출을 사전에 예방하는 효과가 있을 것이다.[18]

표 6. 데이터 유출 사전 대응 방안
Table 6. Preemtive Countermeasures for Data Leakage

데이터 관리 구분	대응방안
데이터 분류	민감도, 유형, 중요도에 따른 분류
데이터 소유자 배정	데이터 소유자 데이터 자산 현황 파악
데이터 출처 확인	자산 현황 관리 시스템 및 네트워크 아키텍처
데이터 흐름 확인	데이터 이동 현황을 파악할 수 있는 실시간 데이터 흐름 모니터링
규제 및 보안 통제 확인	자사에 적용된 규제 요건과 요구되는 보안 통제 수단 파악
데이터 보호 상태 확인	데이터 암호화 정책
데이터 접근 방식 검토	데이터 접근 추적 및 인증 절차 변경 관리
의심행위자 분석 시나리오 작성 및 통제	이상행위탐지 기준 마련 및 통제

[의심행위자 이상행위 탐지 기준]
① 일간 개인정보조회자가 10페이지 이상 출력
② DRM 복호화 임계치를 분석한다.
③ 메일 발송 이력 임계치를 분석한다.
④ 출력이력 시계열 분석한다.

개인정보를 10건 이상 조회하고 DRM 복호화를 1건 이상 진행한 후 해당 내용을 메일로 첨부하여 사내/외로 발송하거나 출력한 인원에 대한 점검 및 상관분석 한다. 임계치 및 문서 복호화 건수는 회사마다 적합한 기준을 설정한 후 모니터링 및 통제한다.

4. 사전예방

예방 및 탐지 비용을 늘려서 사전 예방 조치하는 것이 그 무엇 보다 우선이다. 지속적으로 이상행위에 대하여 탐지해야한다. 다음은 예방방안에 대해 살펴본다.

① 내부통제 시스템 모니터링을 해야 한다.
② 의심 행위자에 대하여 디지털 포렌식 기반으로 주기적 또는 비주기적 불시 점검을 수행해야한다.
③ 계약 업체에 대해서도 마찬가지로 주기적, 불시적으로 체계적인 관리 시스템을 마련하여 점검·관리해야 한다.
④ 정보보안 교육 대상을 고려한 교육을 통하여 개인정보보호의 인식수준을 높여 차후 개인정보 유출을 예방할 수 있도록 조치해야 한다.[19]

V. 결 론 및 향후 발전 방향

본 논문은 금융권을 중심으로 발생한 해킹 및 고객정보 유출 사고 사례를 분석하고, PC 보안 위협 요소 및 대응 방안 등에 대해 알아보았다. 금융회사의 경우 제조업체와 달리 각 영업점 및 내방객에게 USB 메모리나 휴대폰 반입 사전 점검 등의 강력한 통제를 가하는 것은 쉽지 않다. 금융회사의 경우 현실적으로 가능한 수준의 물리적 통제의 한계를 보완하기 위하여 관리적 통제 및 다양한 기술적 통제가 더욱 중요한 보안 활동의 요소가 될 수 있다.

금융회사에서는 자사의 정보유출 예방을 위해 보안체계를 개선하는 등 지속적으로 많은 노력을 기울이고 있으나 보안 관련 다양하고 많은 솔루션이 도입되면서 보안성은 강화되었으나, 사·내외 사용자들의 업무 피로도와 불편은 가중되어 업무 생산성에 악영향을 주는 한계를 가지고 있다. 특히, 가장 많은 규제를 받고 있는 금융권 사용자의 생산성과 내부 보안의 접점을 찾아야 하는 보안 관리자에게는 균형의 미학이 요구된다.

PC 보안 위협 및 컴플라이언스 대응방안으로 PC 보안 솔루션 도입 및 적용도 중요하지만, 사용자 편의 및 효율성을 고려한 통합 점검 방안에 대한 지속적인 연구가 필요하다고 생각한다.

본 논문에서는 PC 보안성이 지속되도록 PC측면 보안대책과 중요한 보안 업데이트, 바이러스 점검, 보안정책관리 등에 대한 자동점검 방안을 적용하여 PC 보안 악성코드 감염으로 인한 위험을 감소시키는 사례에 대해서 제시하고 있다. 또한, 데이터 유출 사전 대응 방안으로 DRM 등 솔루션 적용 뿐 만아니라, 데이터의 흐름, 소유자, 출처, 규제, 보안 통제, 접근방식, 의심행위자 이상행위 탐지기준 등 마련하여 사전 모니터링 방안에 대해 설명하고 있다. 본 본문에서는 PC 보안 솔루션 전체에 대한 통합 점검 방안에 대해 제시하지 못하는 한계점이 있다. 향후 PC 보안 솔루션을 확대하여 점검하는 방안에 대한 연구가 필요하다.

관리적 통제방안으로 정보보호 관리 절차 및 보호대책을 체계적으로 수립 및 운영·관리하기 위한 정보보호 관리체계를 도입을 일부 의무대상 금융회사에서 확대 운영이 필요하다. 또한, 기업의 정보보안 정책에 따라 가용성과 기밀성의 경계에 있는 정보보안 활동을 하기 위해서는 사전에 직원들의 정보보안 인식제고가 선행되어

야 하고, 기업의 보안성을 강화하기 위해서는 보안 업무가 회사 전략상 중요한 업무로 인식되어 정보보호 강화 활동을 통해 보안 위험을 감소 및 사고 예방 방안으로 '기업 보안평가 공시제도'에 도입 방안 등에 대한 연구가 필요하다.[20]

References

[1] http://journal.kiso.or.kr/?p=4142

[2] https://ko.wikipedia.org/wiki/3%C2%B720_%EC%A0%84%EC%82%B0_%EB%8C%80%EB%9E%80

[3] McAfee Threat Report Aug 2015

[4] National Internet Development Agency of Korea, "Trend reported monthly malware detection concealment site book", Oct 2015

[5] http://www.fnnews.com/news/201103062129305359?t=y

[6] http://www.ddaily.co.kr/news/article.html?no=106117

[7] http://www.yonhapnews.co.kr/bulletin/2013/07/16/0200000000AKR20130716134852017.HTML

[8] Ministry of Science, ICT and Future Planning, National Internet Develpment Agency of Korea, "2014 Information Security Survey (Enterprise edition) Final Report", Dec 2014

[9] Financial information using deodorant recent phishing, pharming techniques Trends, National Internet Development Agency of Korea, Internet infringement Response Center, Sep 2014

[10] Jong-Hoon, Kim, "Understanding of financial supervision", Apr 2015

[11] http://www.fsec.or.kr/business/finance_control.jsp

[12] http://service1.nis.go.kr/

[13] http://www.fsec.or.kr/business/menace_information.jsp

[14] Financial security Institute, "Financial data protection trends.", Aug 2015

[15] Jeong-Deok Kim, "Financial security innovation opportunities and autonomous security system implementation Success", Oct 2015

[16] Jae-sam Lee, Jae-tae Moon,, "A study of administrative regulations about personal informations" legal research 58th, Jun 2015

[17] National Internet Development Agency of Korea, "Internet Development Agency, National Internet Use the environment Survey", Feb 2015

[18] Hyun-tak Chae, "PC security solutions, security policies through log analysis suggested: Personal Information Leak Prevention", Korea Institute of Information Security and Cryptology, Oct 2014

[19] Sung-baek Han, "Countermeasures in the financial sector for the APT attacks", Korea Institute Of Information Security And Cryptology, Feb 2013

[20] Bo Kim, "Needs and considerrations of corporate security assessment (Focusing on financial companies)", The Journal of The Institute of Internet, Broadcasting and Communication (JIIBC), VOL. 14 No. 6 pp. 273-280, 2014.

저자 소개

한 경 희(정회원)

- 2000년 5월 ~ 현재 : 신영증권 IT센터
- 2014년 3월 ~ 현재 : 고려대학교 정보보호대학원 금융보안학과 금융보안정책전공 석사과정

<관심분야 : 전자금융보안, 정보보호 정책, 개인정보보호 등>

김 인 석(정회원)

- 2008년 고려대학교 정보경영공학과 박사
- 2009년 ~ 현재 : 고려대학교 정보보호대학원 교수
- 現 FDS산업포럼 회장, 한국사이버정보전학회 운영위원 등

<관심분야 : 전자금융보안, IT감사, 전자금융법규 등>