Journal of the Korea Academia-Industrial cooperation Society
Vol. 18, No. 9 pp. 464-472, 2017

https://doi.org/10.5762/KAIS.2017.18.9.464
ISSN 1975-4701 / eISSN 2288-4688

디지털 포렌식 기법을 통한 기업 정보유출에 대한 취약점 탐지 효율성에 관한 연구

박윤재*, 채명신
서울벤처대학원대학교 융합산업학과

A Research on the Effectiveness of the Vulnerability Detection Against Leakage of Proprietary Information Using Digital Forensic Methods

Yoon-Jae Park*, Myung-Sin Chae
Department of Convergence Industry, Seoul Venture University

요 약 ICT(정보통신기술) 융합보안 환경에서 수많은 기업들이 회사 내에서 생산되는 중요 자료인 제품정보, 제조기술, 서비스 매뉴얼, 마케팅 자료, 홍보자료, 기술적 자료들을 외부공개 및 공유를 위해 웹 시스템을 운영하고 있다. 이렇게 인터넷에 공개된 웹 시스템은 사이버 보안 관리에 매우 큰 영향을 주고 있고, 상시 취약점을 가지고 있어서 정보보호 솔루션과 IT 취약점 점검을 수행하고 있지만, 외부 환경에서의 취약점 탐지 관리에는 한계가 있다. 본 연구에서는 이러한 문제점을 개선하고자, 디지털 포렌식 기반의 시스템을 자체 구축하고 포렌식 기법을 활용하여 기업의 중요정보 유출 탐지에 대한 실증 연구를 수행하였다. 그 결과, 국내와 해외에서 운영하는 웹 시스템의 취약점으로 인하여 기업의 비밀자료 등 중요 정보가 노출된 것을 확인할 수 있었고 보안관리 개선 사항도 확인할 수 있었다. 결론적으로 최근 증가하는 해킹사고 대응으로 디지털 포렌식 기법을 적용한 시스템을 구축한다면 정보보안 취약 영역의 보안관리 강화와 사이버보안 관리체계 개선을 가져올 수 있을 것이다.

Abstract In the ICT (Information and Communication Technology) convergence security environment, a lot of companies use an external public web system for the external disclosure and sharing of product information, manufacturing technology, service manualsand marketing materials. In this way, the web system disclosed on the Internet is an important aspect of cyber security management and has an always-on vulnerability requiringan information protection solution and IT vulnerability checks. However, there are limits to vulnerability detection management in anexternal environment. In this study, in order to solvethese problems, we constructed a system based on digital forensics and conducted an empirical study on the detection of important information in enterprises by using forensic techniques. It was found thatdue to the vulnerability of web systems operated in Korea and overseas, important information could be revealed,such as the companies' confidential data and security management improvements. In conclusion, if a system using digital forensic techniques is applied in response to theincreasing number of hacking incidents, the security management of vulnerable areas will be strengthened and the cyber security management system will be improved.

Keywords : Convergence Security, Cyber Security, Digital Forensics, Information Leakage, Information Protection

1. 서론

디지털 산업 환경에 놓여있는 수많은 기업, 정부기관에서 반복적으로 발생하는 기밀문서 유출사고, 개인정보 유출 및 중요 컨텐츠 정보노출 등의 보안사고 원인을 보면, 대부분은 알려지지 않은 프로토콜, 위변조 파일 컨텐

*Corresponding Author : Yoon-Jae Park(Seoul Venture Univ.)
Tel: +82-10-5858-1987 email: tmvlem@gmail.com
Received August 21, 2017 Revised September 13, 2017
Accepted September 15, 2017 Published September 30, 2017

츠, 그리고 악의적 접근시도 행위로 정보 유출 사고가 지속적으로 발생한다. 또한, 정보유출 사고 영역을 보면 기존 정보보안 통제영역 아닌 외부 인터넷 환경을 통한 정보유출 사고가 증가함에 따라서 체계적인 대응 방안을 필요로 하고 있다. 이와 같은 외부적인 환경 문제로 기업에서는 연중 상시 취약점 점검체계 등을 도입하고 있지만, 외부 환경에서의 보안사각 지역에 대한 관리는 보안인력 부족, 시간과 공간 등의 제약 사항으로 통제가 매우 어려운 실정이다. 그래서 본 연구에서는 근본적인 해결책으로 정보유출 사고 발생 시 증거수집 및 사후 정보유출 증거 탐색에 국한하여 사용하는 디지털 포렌식 기법에 대한 활용과 필요성을 국내외 관련 연구문헌과 포렌식 전문가의 인터뷰를 통해 확인한 바, 국내 연구문헌 자료에는 포렌식 기법과 기술을 활용한 알려지지 않은 악성코드 탐지, 제어시스템 보안을 위한 비정상 행위 탐지, 포렌식 감사시스템 구축, 행위 기반의 보안관제 시스템 제안 연구가 진행되었다**[1-4].** 그리고 클라우드 컴퓨팅 환경에 적합한 디지털 포렌식 시스템 통합구축 방안과 효과적인 서비스 방안 등도 다양하게 연구되고 있는 것을 확인 할 수 있었다**[5]**. 해외 연구문헌 자료에서는 실시간 디지털 포렌식 탐구에서 분석 도구와 기능을 통한 실시간 분석 방법론을 제시하고 있으며, 병원 전상망의 범죄 데이터 요소에 대한 무결성 확보를 위한 포렌식 분석 및 활용 연구가 진행된 것을 확인할 수 있었다**[6-8].** 또한 포렌식 도구를 활용한 범죄 패턴 분석도구 모델에 관한 연구와 클라우드 컴퓨팅 환경에서의 디지털 포렌식 기법의 다양한 접근문제, 관리문제, 대용량의 처리 등 기존 연구에 다양하게 활용되고 있음을 고찰할 수 있었다 **[9,10].** 이 같은 디지털 포렌식 기법 연구는 그 범위와 응용이 다양하게 적용되고 있으나, 국내 기업들은 정보유출 취약점 관리에 직접적으로 활용하지는 못하고 있다. 국내 정보유출 방지 솔루션을 개발 보급하는 전문기업인 엑스큐어넷의 보안 전문가는 외부에 보안통제 사각지역에 대한 관리 부재와 외부 인터넷 환경의 취약점 탐지 솔루션은 국내 적용된 것이 없기 때문에 해킹공격이 지속적으로 나올 수 밖에 없는 취약한 구조임을 확인하였다. 디지털 포렌식과 해킹 전문가인 KASS 대표는 국내외 취약점 탐지결과를 종합적으로 볼 때, 한국 기업의 사이버 해킹공격 대응 수준은 60점 이하로 평가하고 있으며 외부 취약점에 대한 체계적인 관리대책이 필요한 것을 확인하였다.

국내의 보안 침해사례 보고서에서도, 윈도우 시스템 폴더 및 파일 등을 공유하기 위해 사용되는 프로토콜인 SMB 원격코드 실행 취약점을 이용한 신종 랜섬웨어가 752% 증가하는 등 외부의 취약한 경로를 통한 사고가 매년 증가하고 있으며, ‘16년 한국인터넷진흥원의 윈도우 침해사고 유형 및 사례 보고서에서도 웹, 이메일, 서비스를 통한 침해사고 증가를 보고하고 있다. 그리고 한국침해 대응센터의 ’17년 렌섬웨어 침해 사고를 분석한 결과, 미국 및 유럽의 경우 위장 이메일을 통해서 70% 이상 감염되고, 국내도 74%의 침해 사고의 원인으로 매우 높게 나타나고 있었다. 특히 스마트폰이 비즈니스에 활용되면서 기업의 중요정보 유출사고 증가로 더더욱 포렌식 기법에 대한 기업 활용도가 이 높아지고 있는 실정이다. 이러한 정보보안 취약점을 탐지하고 그 필요성에 부응하고자 본 연구에서는 디지털 포렌식 기법을 활용한 시스템을 직접 구축하고, 기업, 정부 등을 점검하여 발견된 실제 취약점 사례 통해서, 현 보안관리 사각 지역에 대한 관리의 중요성과 사이버보안 위협 대응을 위한 효율적인 보안 관리체계 개선에 관하여 보고하고자 한다 **[11-13].**

본 논문은 전체 4개의 장으로 구성되어 제1장 서론 부분에서는 연구의 배경 및 목적에 대해서 다루고 있으며, 제2장 관련연구에서는 디지털 포렌식 기법에 대한 활용과 실험설계방법 제시, 그리고 측정방법과 탐지의 필요성을 살펴보았다. 제3장은 결과 및 고찰 부분으로 2장에서 살펴본 디지털 포렌식 실험 측정을 통해서 발견된 국내외 실제 탐지 결과를 도출하여 효율적인 보안관리체계와 취약점 개선 방안을 제안한다. 마지막으로 제4장에서는 결론과 함께 본 논문이 제시해 주는 시사점과 효과성에 대한 부분을 제안하고 있다.

2. 관련연구

2.1 실험설계방법

디지털 포렌식 기법을 활용한 정보유출 취약점 탐지는 기존 정보보안에서 관리하는 취약점 관리 영역이 아닌 외부 사각지역에 대한 취약점 탐지와 보안 관리의 필요성을 검증하기 위해서 설계하였다. 이를 위한 검증 솔루션 구축 검토를 위해 전문 기업과의 몇 차례 선행 연구를 진행하였다. 그 결과 외부 네트워크상의 프로토콜

을 분석해 내는 IP연관분석과 지역연관분석, 기업의 오피스 문서, 콘텐츠, 문서 정보 등의 첨부 파일을 추적하는 컨텐츠 분석 적용이 가능하며, 각종 빅 데이터를 이용한 상관관계 분석으로 이상 징후 탐지에 활용할 수 있으며, 파일 사용이력 추적, IP간 관계 기반의 연구인 “미국의 카지노 횡령사건 분석과 포식 수사기술의 활용 연구” 사례를 통해서도 취약점 탐지 솔루션 설계가 가능함을 확인하였다**[14-16].** 그러나 관련 솔루션 설계는 장시간 소요와 높은 비용 투자로, 본 연구에서는 소액 투자로 실제 기업에서 구축 가능한 유사 실험설계 시스템을 구축하여 검증을 하였다. 본 시스템은 디지털 포렌식 가상서버(VM) 환경 기반으로 크게 리눅스와 윈도우 환경으로 나뉘어서 구축했으며, 취약점 탐지를 위한 데이터 확보를 위해 웹사이트카피어 프로그램을 사용하여 데이터의 손실을 막고 중복 저장하는 미러링 환경을 설정하였다. 그리고 미러링 과정에서 확보된 데이터의 관련 링크의 데이터 미러링이 되도록 스파이더 기능을 활성화하여 Deep 링크 탐색을 수행하고, 필터링으로 원하는 결과 리포트를 얻기 위해 빠른 검색 속도와 다양한 검색 방법이 제공하는 프로그램인 Everything과 하드디스크의 모든 파일 및 폴더 인덱싱을 통해서 원하는 파일과 폴더를 검색해 주는 프로그램 ASR(Actual Search & Replace) 프로그램을 적용하였다. 이렇게 구축된 디지털 포렌식 가상서버 환경의 구성도는 Fig. 1과 같다**[17].**

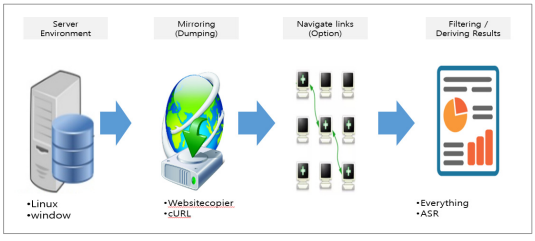

Fig. 1. Digital forensic virtual server environment configuration diagram.

2.2 측정

실험 검증을 위해서 주로 사용한 측정 도구는 구글독스, 웹사이트카피어, cURL, Everything, ASR, 넷스파커 측정 도구를 활용하였다. 구글독스 기법을 사용하여 보안에 취약한 사이트 리스트를 수집 하였으며, 발견된 취약 사이트에 대해서 미러링을 할 수 있도록 웹사이트카피어, cURL 도구를 적용하였다. 이렇게 수집된 미러링 데이터에 대해서는 1차적으로 사용자 컴퓨터에 설치된 파일 및 폴더 문서 등을 쉽고 빠르게 찾아주는 프로그램인 Everything 도구를 사용하여 중요 파일들을 검색 및 필터링하고, 2차는 ASR 프로그램을 활용하여 연관된 DATA 파일을 찾아 해당 파일의 위치 경로를 파악하여 쉽게 정보를 확인하였고, 레지스트리 분석과 웹 히스토리 분석이 가능하도록 설계하여 측정하였다. 그리고 본 연구의 측정 결과와 취약점 수준을 Table과 Fig로 표현하기 위해서 취약점 분석도구이면서 스파이더, 크로울러 기능을 제공하는 넷스파커를 활용하여 XSS(Cross Site Scripting)취약점, CVSS(Common Vulnerability Scoring System)코드, CWSS(Common Weakness Scoring System) 코드 등 취약점 코드 및 패치 방법을 확인하고 측정하였다**[18].**

2.3 탐지 필요성 확인

본 연구의 실험에서는 디지털 포렌식 기법이 정보보안에서 도입과 적용이 필요하다는 것을 확인하기 위해서 웹 사이트와 컴퓨터 코드의 보안 취약점 찾는 기술인 구글독스 기법을 활용하여 취약한 사이트를 발굴하고 취약점을 분석한 결과를 도출하였을 뿐만 아니라, 도출된 취약한 사이트 URL에 대해서 보안 관리의 필요성과 보안 대책 방안을 제시하기 위해서 디지털 포렌식 도구인 넷스파커를 통한 셀프 진단으로 CVSS와 CWSS 등의 취약점 탐지결과 보고서를 연구결과에 반영하였다. 그 결과 외부 환경에 대한 통제 관리를 하지 않을 경우에 네트워크, 시스템, 어플리케이션 등의 DB접속을 통해서 중요 정보가 유출되는 치명적인 취약점이 지속적으로 발생한다는 것을 탐지하게 되었다. 그리고 수많은 학생들의 개인정보를 취급 관리하는 고등 교육기관 사이트의 경우 개인정보영향평가 점검 대상임에도 불구하고 여전히 점검하지 않고 있다는 것이 확인되어, 취약점 자동화 점검툴인 넷스파커를 활용하여 취약점을 탐지한 결과로 **Table 1**과 같이 취약점을 확인하였다. 이에 고등 교육기관의 웹 사이트에 대해서도 조속히 법적 요구사항인 개인정보영향평가의 수행과 보안 관리체계 수립의 필요성도 확인되었다. 또한 공격자가 원격에서 웹 서버에 명령을 수행할 수 있도록 작성된 웹 스크립트 파일을 웹셸 업로드 후 DB의 중요 정보를 탈취할 수 있는 취약점도 탐지되어 웹 서버에 대한 보안 취약점 관리의 중요성을 제시하였다**[19].**

Table 1. Vulnerability assessment results of higher education institutions

Breakdown	problem	Instance	Committed
Critical	3	64	63
Important	5	125	68
Middle	4	98	0
lowness	11	11	2
Information	14	14	7
Sum	37	312	140

3. 결과 및 고찰

3.1 국내취약점

본 연구에서는 디지털 포렌식에 사용하는 기법의 종류인 구글 고급검색(해킹방법)기법, 웹 취약점 점검 방법인 SQL 인젝션 기법, 취약점 분석도구 등 을 활용하여 구축한 시스템을 기반으로 실제 취약점을 탐지하여 어떠한 취약점이 존재하는지를 분석하여, 정보보안의 사각지역을 파악하고, 정보유출 문제점을 개선하고자 국내의 취약점을 도출하였다. 특히, 대기업, 병원, 정부기관 등 중요 정보를 가지고 있는 곳을 대상으로 취약점 점검을 한 결과를 보면 대기업에서 중요하게 관리되는 비밀 표기된 문서 Fig. 2와 같이 인터넷에 고스란히 노출된 것을 확인하였으며, 해당 문서에 대한 기업을 대상으로 한 취약점을 점검한 결과 31%의 취약점을 확인되었다**[20].** 국내 병원은 소프트웨어가 구 버전이기 때문에, 공격에 치명적인 취약성 코드인 CVE-2013-6449 등이 확인되었고, 사용자의 활성세션 하이재킹, 피싱공격 수행, 데이터 가로 채기와 중간자 공격을 수행이 가능한 크로스사이트 스크립트 공격 위협이 확인되었으며 전체적인 취약율이 48%로 확인되었다**[21].** 정부청사본부 사이트(www.chunsa.go.kr)의 취약점 점검결과 Fig. 3과 같이 보안통신(SSL) 방식이 약한 암호화로 활성화된 취약점이 발견되었고, 일자리위원회(www.jobs.go.kr)와 국내학회를 대상으로 점검을 수행한 결과를 보면 Table 2와 같이 최근 오픈한 일자리 위원회 사이트에서는 사용자 및 관리자 정보를 획득이 가능한 상태로 확인되었으며, 국내 학회의 경우는 회원 정보를 통째로 탈취가 가능한 SQL 인젝션 취약점을 보유하고 있는 치명적인 취약점을 각각 확인 할 수 있었다. 이렇듯 대표적인 국내 기업과 기관들에 대하여 취약점을 조사한 결과만 보더라도 최우선으로 관리해야할 기업과, 정부 기관 등 외부 환경에 놓여있는 취약점에 대한 관리가 잘 이루어지지 않고 있기 때문에 최근에 발생되는 해커의 공격은 지속적으로 증가할 수 밖에 없음을 보여주고 있다.

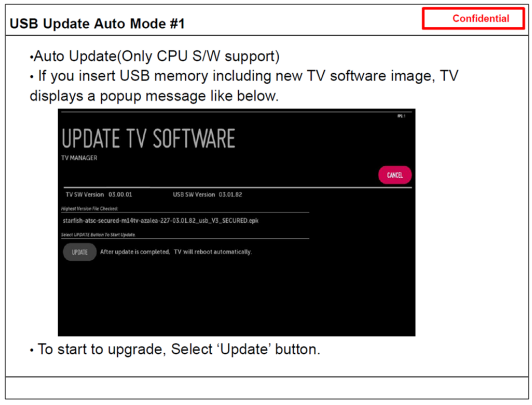

Fig. 2. Secret document of the leaked company.

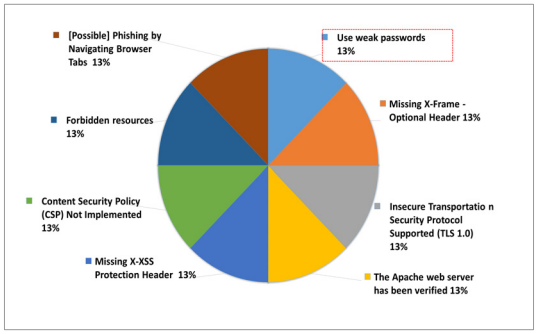

Fig. 3. Government administration office information leak vulnerability detection result.

Table 2. Report on vulnerability of government job commission & Domestic Society

1) government job commission

Breakdown	problem	Instance	Committed
Critical	1	3	3
Important	7	26	23
Middle	2	2	1
lowness	10	13	2
Information	12	12	4
Sum	32	56	33

2) Domestic Society

Breakdown	problem	Instance	Committed
Critical	3	4	2
Important	4	32	13
Middle	2	2	1
lowness	11	11	4
Information	13	13	5
Sum	33	62	26

기업 정보유출 탐지 결과에서도 제품정보 디자인, 설계 도면이 포함된 서비스 매뉴얼이 외부 사이트에 공개 노출 등 기업에서 중요 정보가 외부 노출되어 있다는 것은 확인할 수 있었다**[22].** 이와 같은 탐지 결과는 임의로 선정된 소수의 대상 사이트를 선정하여 측정한 결과이기 때문에 외부에 시스템을 운영하는 기업, 병원, 정부 등 관련 정보보호 관리 책임자는 중요 정보의 유출 가능성을 두고, 기업의 사내 정보뿐만 아니라, 외부 환경에 노출되어 있는 정보에 대한 통제 방안을 수립해야 하겠다. 이 외에 구글 검색 기법을 이용한 실험 검증을 위해서 구글해킹 기법으로 검색창에 “intitle : index of 이력서” 입력해 탐색된 결과물을 살펴보았다. 그 결과 화면 리스트에서 Fig. 4의 “Index of /bbs/files/notice” 파일 서버가 탐지되었으며, 서버 내 폴더 리스트에 쉽게 접속이 가능한 상태였으며, 수 많은 디렉토리를 통해 획득한 파일을 열어보면 교환학생 명단, 학번, 생년월일, 이름 등 1, 2등급 이상의 개인정보 파일을 다운로드 할 수 있는 취약점을 발견하였다. 이러한 취약점을 보유한 서버는 대학교에서 운영하는 파일 서버로 외부에서 학교 내부 정보를 누구나 접근 가능한 상태로 구글에 노출된 것이 탐지된 것이다. 국내외로 공동으로 교환학생 제도를 운영하는 대학교에서 개인정보 유출 사고가 발생하게 된다면 학교에 부정적인 영향이 미치게 됨을 물론이거니와 접근통제 취약점을 통해서 학교 전체 자료에 대한 해킹공격, 랜섬웨어 공격으로 중요 자료가 손상되는 큰 보안 사고가 이어질 수 있기 때문에 사전점검 및 문제점을 조속히 개선하여야 하겠다.

마지막으로 네트웍 포렌식 기술로 SQL 인젝션 기법을 활용한 것으로 웹 시스템 취약점 유무분석, 침투시도, 웹 서버탈취, 서버 컴퓨터 탈취 순의 시나리오 기반으로 탐지하여 웹 서버의 자료유출, 서버장악, 바이러스 및 악성코드 유포, 관리자계정 삭제, 페이지 변조 등의 기법을 활용하여 국내 대학원 대학교의 사이트에 대한 취약점 유무 분석을 수행한 결과, DB를 구성하는 테이블과 컬럼을 발견할 수 있었으며, 탐지 결과에 교직원 개인정보, 홈페이지 관리자 계정, 관리자 접속 정보가 노출되어 Table 3과 같이 이메일과 아이디와 관리자 IP의 정보 획득으로 APT 공격 취약점이 발견 되었다**[23].**

延大学号	科技学号	姓名	生日	专业
20250*****	024*****	郑**	1982****	护理学
20250*****	024*****	金**	1983****	护理学
20340*****	031*****	李**	1984****	生物工程
20340*****	031*****	金**	1984****	建筑学
20340*****	031*****	廉**	1984****	通信工程
20340*****	032*****	姜**	1984****	信息管理与信息系
20340*****	032*****	金**	1984****	信息管理与信息系
20340*****	032*****	朴**	1983****	信息管理与信息系
20340*****	032*****	朴**	1984****	信息管理与信息系
20340****	032*****	金**	1985****	国际经济与贸易

Fig. 4. Index of / bbs / files / notice search results.

Table 3. APT attack target information

ID	REG-DATE	IP ADDRESS	ADMIN_NAME
BVS	2015-02-09	112.216.73.51	BVS
-	2015-02-09	113.130.67.214	Hong*dong PC
-	2015-04-10	112.221.157.139	DAE*CAM*&#1
-	2016-0301	124.50.90.166	Ahn*=$

3.2 해외취약점

본 연구에서 발견된 해외 탐지사례에서는 디지털 포렌식의 기본이 되는 기법으로 구글 검색(inurl: lg smartphone leaked)으로 점검한 결과, 기업에서 중요하게 관리되어야 할 제품의 디자인, 스펙이 해외 사이트에서 Fig. 5와 같이 인터넷에 노출되는 사고를 확인 되었으며, 해외에서 운영하는 웹 사이트에 대해서 테스트 목적이 중단되면 비활성화 시키거나, 삭제를 해야 함에도 불구하고, 로그인 화면을 보여줌으로써 외부 공개된 인터넷 환경에서 쉽게 내부 인트라망에 접근이 되어 해킹 사이트로의 표적 대상으로 활용되는 취약점이 확인하였다. 그리고 해외 제품 홍보용 사이트 구축 운영을 위해 이미지 공유 서버로 활용하는 FTP 서버에 대해서 접근 경로를 포함된 문서가 Fig. 6과 노출되어 있을 뿐 아니라, 로그인 접근통제 설정이 취약한 ID(Admin)로 설정되었으며, 패스워드 미 설정으로 누구나 쉽게 로그인 접속하여 서버에 등록된 기업의 모든 자료를 다운로드 받을 수 있는 상태로 취약한 시스템이 발견되었다. 이 시스템은 글로벌 비즈니스를 위한 마케팅, 홍보 사이트(SNS

등) 개발을 위해 외주용역 체결로 제작한 웹 시스템으로써 보안관리 소홀로 해당 기업에서 중요하게 관리하는 제품정보(이미지, 도면 등)를 누구나 다운로드가 가능한 상태로 방치되고 있었다. 특히, 블로그 등 홍보 사이트에 대해서 구글봇, 해커의 공세로 개인 정보가 탈취되는 네트워크 위협과 기업의 중요정보 유출 사고도 증가함을 알 수 있다. 현재 관련 취약한 FTP 서버에 대한 적절한 조치를 진행하여, 로그인이 불가한 상태이지만, 동일 취약점 및 사고 예방을 위한 다른 수많은 글로벌 지역의 보안취약점 관리 실태점검 및 조치는 진행되지 못하고 있다**[24-26].**

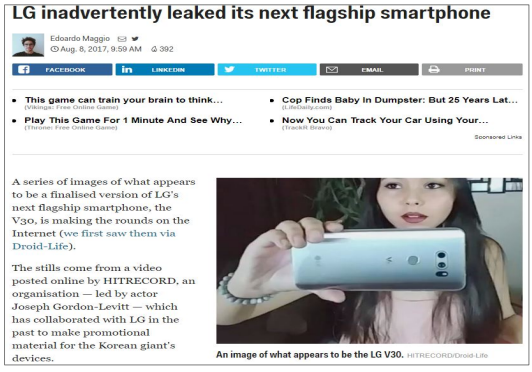

Fig. 5. LG inadvertently leaked its next flagship smartphone[27].

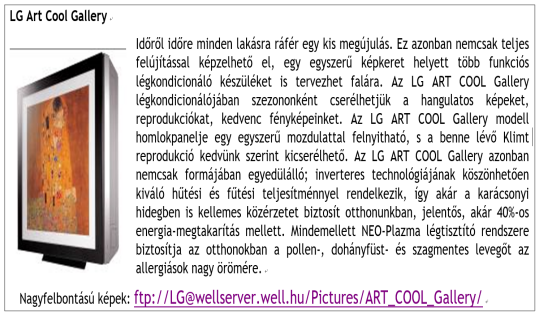

Fig. 6. Document exposing FTP server access path.

3.3 사이버보안 관리체계 개선

디지털 포렌식 기법 활용으로 외부의 보안 취약점 위험 요소에 대해서 상시식별/분석/측정/모니터링/검토 할 수 있는 시스템을 구축하여 이상 징후 탐지 기능을 지원하고 관리함으로써 보안 리스크 위험을 분석하고 평가할 수 있어야 한다. Fig. 6은 ISO 31000에서 요구하는 리스크를 포렌식 기법을 활용하여 사전에 분석, 위험도를 평가하여 조정 관리하는 시스템으로 기업의 정보보안 위험관리를 위한 방법론 및 도구분석 연구로 위험관리 프로세스를 보여준다. 이처럼 정보보안 취약점 관리를 위해서는 “리스크 분석관리 시스템”을 구축하여 상시 점검이 수행되어야 하나, 기업에서는 당장 피해가 없다고 해서 방치될 경우, 기업은 취약점의 보안관리 실패로 회사 전체 시스템에 대한 해킹공격 등 큰 피해를 초래할 수 있는 사고 발생 원인이 되기 때문에 정보보안 책임자 및 담당자의 면밀한 분석과 함께 보안관리 체계 적용을 위한 준비가 필요하다.

4차 산업혁명 시대에 확산되는 “사물인터넷 기반의 제조 시스템에 대한 사이버물리 공격 추론에 대한 연구“ 내용을 살펴보면 공격자가 디지털 파일을 조작함으로써 부품의 물리적 특성을 조정하고 기계적 수치를 변경시켜서 제조비용을 증가시키고, 안전과 생명을 위협함에 따라서 잠재적인 사이버물리 공격 위험을 이해하고, 식별하여 시스템을 보호할 수 있는 방법을 제시하고 있는 것을 알 수 있다. 따라서 현재 지속적인 보안 위협에 따른 사후 관리적 정보보호 관리체계는 기획・설계 단계부터 정보 보호를 고려한 전 영역의 정보보안 관리체계로 개선이 수반되는 새로운 정보보호 패러다임 접근이 필요하다.

특히, 외부 환경에서의 보안 관리의 어려움과 전문 인력의 부족한 부분을 해소하고 효과적으로 통제 관리하려면 Table 4의 연구 결과와 같이 정보유출 취약점 탐지 서비스와 품질 향상의 기회를 효율적으로 제공하는 ‘버그바운티’ 제도 도입이 절실하게 필요함은 물론이거니와, “사이버보안 관리체계”의 구조적 개선이 필요함을 알 수 있다**[28-30].**

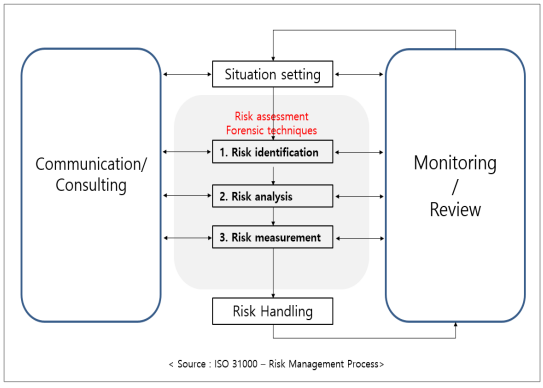

Fig. 6. Risk analysis management system diagram.

Table 4. Bug bounty operational efficiency comparison table

Classification	Google Chrom		Mozilla Firefox	
	Self-excavation	Bug Bounty	Self-excavation	Bug Bounty
Number of vulner- abilities	263	371	48	148
Expenditure cost	547,500	393,161	547,500	444,000
Expenditure cost per vulnerability	2,082	1,060	11,406	3,000

Note: In the case of self-discovery spending costs, the security team staff will be charged $ 500 * 365 days * 3 days per day.

3.4 취약점 평가체계 도입

본 연구에서 발생되는 대외 환경에서 발생되는 취약점에 대해서 상시 보고체계가 필요하고, 우선순위를 통해서 지속적인 보안 관리의 유효성이 보장되어야 한다. 이를 위해서는 취약점에 대해 측정하고 효율적인 위험 수준 평가 관리를 통한 최적의 보안 관리체계 설계가 가능하도록 CVSS 취약성 평가관리 방법을 적용한 IT보안 거버넌스와 리스크 관리를 위한 정보보호 관리체계 개선이 진행되어야 하겠다. 글로벌 비즈니스를 진행하는 아마존웹서비스에서는 CVSS 버전 2.0을 사용하여 잠재적 취약성을 지속적으로 평가하며, 평가 결과의 점수는 문제의 심각도를 수량화하여 대응에 대한 우선순위를 지정하고 관리하고 있다**[31-33].** 또한, 아마존웹서비스에서는 사용자가 보고한 보안 우려 사항을 우선적으로 조사하고 완화하는 작업에 대한 진행 사항을 계속해서 공지하고 통보하는 절차를 준수하고 관리한다. 따라서 국내 기업에서도 보안 취약점의 심각성을 판단하여 중요 약점 및 취약점을 대한 우선적인 대응을 하는 것이 중요하며 이를 판단하기 위한 중요도 평가 척도가 요구되고 있다. 2014년 “보안취약점 중요도 정량평가 체계 연구” 결과처럼 소프트웨어의 보안취약점 평가 체계를 시범적으로 연구 적용하여 정량적으로 산출 할 수 있는 중요도 정량평가 체계를 마련한 것처럼 본 연구에서도 마찬가지로 아래 평가 요소별로 선정된 평가척도(출현도: 파급 범위, 대상 분포, 시스템 중요도: 피해의 심각성, 기술적 영향: 침해 형태, 공격 난이도: 접근 벡터, 권한 요구도, 상호작용 정도, 침해 가능성, 대응 난이도: 교정 난이도, 외부 제어의 효과, 및 발굴 수준: 발굴 난이도, 문서 완성도)를 활용하여 기업의 정보유출 취약점에 대한 상시 평가 체계를 마련하여 정량적인 자료를 통해서 정보유출 취약점 관리 평가체계가 구축되어야 한다**[34,35].**

4. 결론

디지털 포렌식 기법을 활용한 기업 정보유출의 취약점 탐지 효율성 연구를 통하여 기업에서는 정보 보호를 위한 일회성 모의해킹, 취약점 점검의 한계를 극복하고, 정보유출 취약 지역에 대한 보안 관리체계 적용을 통해서 다음과 같은 시사점과 효과를 기대할 수 있다.

1. 디지털 포렌식 기법의 활용과 응용으로 외부 취약점 탐지 시스템을 구축하여, 국내외 외부 인터넷 환경에서의 정보유출 경로를 제공하는 치명적 취약점이 존재하고 있음을 확인할 수 있었고, 외부 보안관리 사각지역에서 발생하는 정보유출에 대한 보안관리 강화가 필요함을 알 수 있었다.
2. ICT(정보통신기술) 융합보안 환경과 CPS(사이버 물리시스템) 환경의 정보보호체계에 대한 개선 방안을 확인할 수 있었고, 기존 정보보호 관리체계에 네트워크와 비즈니스 보안 환경에 미치는 잠재적인 위험에 대한 영향 및 발생 가능성을 CVSS 취약성 지수제 시스템 관리를 적용하면 보다 효율적인 사이버 보안관리체계 수립이 가능하다.
3. 기업의 한정된 보안내부 조직 구성원만으로는 외부 환경에 대한 취약점 탐지 및 관리체계를 구축하는 것은 현실적으로 어렵다. 따라서 외부의 포렌식 전문 기관과의 협업 또는 전문 해커를 통한 취약점 탐지 서비스와 품질 향상의 기회를 제공하는 ‘버그 바운티’ 제도의 검토와 도입이 필요함을 확인하였다.
4. 본 연구에서는 정보보안 외부의 취약점 리스크 관리의 중요도와 개선 방안을 중심으로 연구가 진행되었을 뿐 다양한 포렌식 기법을 활용하지 못한 한계가 있다. 향후 보다 다양한 포렌식 기법을 활용한 정보보호 관리 체계를 준비한다면 지속적으로 발생되는 취약한 사이버보안 영역을 관리하는데 효과적으로 기여할 것으로 기대된다.

References

[1] J, H, Lee, S. J. Lee, "A Study on Detection of Unknown Malicious Code Using Digital Forensic Technique", The Journal of the Institute of Information Security, vol. 24, no. 1, pp. 109-112, 2014.
DOI: http://dx.doi.org/10.13089/JKIISC.2014.24.1.107

[2] Y. Y. CHO, M. J. Kim, G. H. Park, M. P. Hong, J. Kwak, T. S. Sohn, "A Study on Network Forensics based on Visualization for Detection of Abnormality Behavior", The Journal of the Institute of Information Security, vol. 27, no. 1, pp. 25-37, 2017.
DOI: https://doi.org/10.13089/JKIISC.2017.27.1.25

[3] Y. H. Kim, "Implementation of Audit System Applying Forensic Analysis Technique to Network Node", The Journal of Korea Society of Electronic Commerce, vol. 14, no. 3, pp. 170-180, 2017.

[4] J. S. Hong, Nio Park, W. H. Park, "Zombie PC Detection System Model Using Active Forensic Technology", Journal of Korea Society of Electronic Commerce, vol. 17, no. 3, pp. 117-128, 2012.
DOI: http://dx.doi.org/10.7838/jsebs.2012.17.3.117

[5] Y. Y. Shin, S. M. Shin, "An Empirical Study on Large-scale Digital Forensic Service", Korea Information Security Society, vol. 1, no. 2, pp. 83-100, 2010.

[6] M Rafique, MNA .Khan, "Exploring Static and Live Digital Forensics", IJSER, vol. 4, no. 10, pp. 1048-1051, 2013.

[7] A Akbal, and E Akbal, "Digital forensic analysis through Firewall for detection of information crimes in hospital networks", MIPRO, vol. 40, pp. 506-509, 2017.
DOI: https://doi.org/10.23919/MIPRO.2017.7973478

[8] J. J. Jung, C. M. Lee, "Trend Analysis of Korean Fingerprint Recognition Research Using Network Analysis", Fusion Security Journal, vol. 17, no. 1, pp. 15-30, 2017.

[9] N Jain, N Bhanushali, S Gawade, and G Jawale, "Physical and Cyber Crime Detection using Digital Forensic Approach", IJAIIT, vol. 3, no. 1, pp. 834-841, 2017.

[10] Deoyani Shirkhedkar, Sulabha Patil, "Analysis of Various Digital Forensic Techniques for Cloud Computing", IJARCS, vol. 5, no. 4, pp. 104-107, 2014.

[11] H. G. Moon, S. C. Park, "Establishment of Integrated Management System for Vulnerability Diagnosis for Enhancing Corporate Security", Korean Communications, vol. 31, no. 5, pp. 39-40, 2014.

[12] J. K. Kim, "Types and Cases of Windows Infiltration". pp. 6-8, KISA, 2016.

[13] P Sundresan, N Sujata, V Cindy De, S Sitifazilah, B Samy, and G Narayana, "Comparative Studies on Mobile Forensic Evidence Extraction Open Source Software for Android Phone", Advanced Science Letters, vol. 23, no. 5, pp. 4483-4486, 2017.
DOI: https://doi.org/10.1166/asl.2017.8922

[14] Michael Cohen, Darren Bilby, Germano Caronni, "Distributed forensics and incident response in the enterprise", Digital Investigation vol. 8, no. 0, pp. S101-S102, 2011.
DOI: https://doi.org/10.1016/j.diin.2011.05.012

[15] Kyung Hee University, "Correlation Analysis", [Internet]. 2016, Available From: https://klas.khu.ac.kr/common/downloadFile.do?fileId=FIL_16051115271311714bb4. (accessed Aug, 18, 2017)

[16] K. A. Lee, J. W. Park, "Casinos Embezzlement Case Analysis and Prediction Research", Journal of the Institute of Electronics and Communication Engineers vol. 6, no. 1, pp. 2-3, 2011.

[17] HTTrack, "Website copier", [Internet]. 2017, Available From: https://www.httrack.com/(accessed July 30, 2017)

[18] S. J. Oh, K. H. Kim, "A Study on Security Flaw Analysis Vulnerability Using Registry Parsing", The Institute of Electronics Engineers of Korea, Conference Proceedings, pp. 287-290, 2016.

[19] D. H. Lee, J. W. Lee, J. G. Kim, "OWASP TOP 10 Security vulnerability verification method for multitenancy - based web sites", Fusion Security Journal, vol. 16, no. 4, pp. 43-51, 2016.

[20] LGE, "Firmware Update Confidential document", [Internet]. Available From : http://partner.lge.com/fr/portal/download/download/mobileExternalFileDownload.lge?fileId=GwxUQbA9lqELW8sD9jz3A&content=manual. (accessed July 30, 2017).

[21] kbobath, "Cross-site scripting threats", [Internet]. 2017, Available From: http://www.kbobath.com/upload/. (accessed July 30, 2017).

[22] ManualsLib, "External site exposure of the manual", [Internet]. 2017, Available From: https://www.manualslib.com/l/lg+sevice+manuals.html. (accessed July 30, 2017).

[23] Haibin Hu, "Research on the technology of detecting the SQL injection attack and non-intrusive prevention in WEB system", AIP Conf Proc vol. 1839, no. 1, pp. 1-8, 2017.
DOI: http://dx.doi.org/10.1063/1.4982570

[24] LGE, "European R&D Testbed access site", [Internet]. Available From: http://eurd-test.lge.com/index.php?send_ok=1. (accessed July 30, 2017).

[25] SolarWinds Worldwide, "Access control settings for vulnerable FTP server", [Ienternet]. Available From: http://wellserver.well.hu. (accessed July 30, 2017).

[26] Y. J. Park, J. H. Jung, "A Study on Security Threats and Countermeasures in SNS Environment", Korea Science and Research Society, vol. 6, no. 3, pp. 204-221, 2012.

[27] Businessinsider, "LG inadvertently leaked its next flagship smartphone" Available From: http://uk.businessinsider.com/lg-v30-accidental-leak-2017-8. (accessed August 19, 2017).

[28] J Bhattacharjee, A Sengupta, MS Barik, C Mazumdar, "An analytical study of methodologies and tools for enterprise information security risk management", IGI Global, pp. 1-20, 2017.
DOI: http://dx.doi.org/10.4018/978-1-5225-2604-9

[29] Y Pan, J White, DC Schmidt, A Elhabashy, L Sturm, J Camelio, and C Williams, "Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems", IJIMAI, vol. 4, no. 3, pp. 1-11, 2017.

DOI: https://doi.org/10.9781/ijimai.2017.437

[30] KISA, "S/W New Vulnerability Notification Award Management Guide", Available From: https://www.krcert.or.kr/download.do?path=consult&name=160617_Guide.pdf&orgName=. (accessed August 18, 2017)

[31] G. H. Han, TK Nguyen, H. CHO, S. H. Hwang, C. H. Im, “Cost effective active security inspection framework for web application vulnerability analysis”, Information Processing Society, vol. 5, no. 8, pp. 189-196, 2016.

[32] Umesh Kumar Singh, and Chanchala Joshi, “Quantitative security risk evaluation using cvss metrics by estimation of frequency and maturity of exploit”, WCECS, vol. 1, pp. 19-21, 2016.

[33] Losonczi, Peter, Pavel Necas, Norbert Nad, “Risk management in information security”, J management ,vol. 1, pp. 77-80, 2016.

[34] Amazon, “Investigate vulnerabilities in Amazon Web Services”, Available From: https://aws.amazon.com/ko/security/vulnerability-reporting/. (accessed July 30, 2017).

[35] J. S. Ahn, B. M. Chang, E. Y. Lee, "A Study on the Critical Evaluation System of Security Vulnerability", Journal of the Institute of Information Security, vol. 25, no. 4, pp. 3-10, 2015.
DOI: http://dx.doi.org/10.13089/JKIISC.2015.25.4.921.

박 윤 재(Yoon-Jae Park) **[정회원]**

- 2003년 10월 ~ 2017년 6월 : LG 전자 정보전략/보안팀
- 2012년 2월 : 서울과학종합대학원 산업보안MBA (경영학 석사)
- 2015년 3월 ~ 현재 : 서울벤처대학원대학교 융합산업학과 박사과정
- 2016년 9월 ~ 현재 : 서울과학종합대학원 산업보안MBA 겸임교수

<관심분야>
정보통신, 사이버보안, 융합보안, 사물인터넷, 블록체인

채 명 신(Myung-Sin Chae) **[정회원]**

- 2003년 7월 : U of Illinois at Chicago, 경영정보시스템 (경영학 박사)
- 2004년 3월 ~ 현재 : 서울벤처대학원대학교 교수

<관심분야>
디지털 비즈니스, 디지털 마케팅, 공유경제, 핀테크