http://www.calsec.or.kr/jsebs
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.19, No.4, Nov 2014, pp.195-204
http://dx.doi.org/10.7838/jsebs.2014.19.4.195

중소기업 유해트래픽 분석을 통한 보안관제 개선 방안

Improved Security Monitoring and Control Using Analysis of Cyber Attack in Small Businesses

홍준석(Jun Suk Hong)*, 임영환(Young Hwan Lim)**,
박원형(Won Hyung Park)***, 국광호(Kwang Ho Kook)***

초 록

최근 지능화 고도화 되고 있는 사이버 위협으로부터 중소기업을 보호하기 위해서는 24시간 예방・탐지・분석・대응 해 주는 보안관제가 필수적이다. 이러한 중소기업의 보안관제를 지원하기 위해 정부로부터 예산지원을 받아 중소기업기술지킴센터가 구축되어 운영 중이며, 현재 900여 개 중소기업에 대해 보안관제서비스를 지원하고 있다. 본 논문에서는 중소기업 기술지킴센터에서 보안관제서비스를 지원하고 있는 중소기업들의 이상트래픽에 대해 살펴보고 중소기업의 보안관제 개선방안을 제시하였다.

ABSTRACT

Recent, Secure the small and medium-sized enterprises from advanced and intelligence cyber threat, 24 hours of prevention, detection and analysis is essential. Small and Medium Business monitoring center is operated by government financial support to protect and prevent these threats. Currently it provides security to about 900 small and medium-sized enterprises. This paper studies abnormal and attack packets from small and medium-sized businesses[enterprises] which is monitored by Small and Medium Business monitoring center and provides improvement of security control for small and medium-sized enterprises.

키워드 : 보안관제, 중소기업, 보안위협
Security Monitoring System, Small Businesses, Security Threat

* Fist Author, Graduate School of Public and Information Technology, Seoul National University of Science and Technology(jun0817@dreamwiz.com)
** Graduate School of Public and Information Technology, Seoul National University of Science and Technology(yhlim@seoultech.ac.kr)
*** Department of Cyber Security, Far East University(whpark@kdu.ac.kr)
****Corresponding Author, College of Business and Technology, Seoul National University of Science and Technology(khkook@seoultech.ac.kr)
2014년 10월 28일 접수, 2014년 11월 20일 심사완료 후 2014년 11월 25일 게재확정.

1. 서 론

최근의 사이버 공격은 다양한 IT 기술과 공격방식을 기반으로 여러 보안위협을 생산해 특정 대상에게 지속적으로 공격하는 APT (advanced persistent threat) 공격과 인터넷 인프라가 지속적으로 확대됨에 따라 인터넷을 통한 악성코드 유입 급증과 다양한 SNS를 통해 공격 대상을 파악하거나 SNS 자체를 공격 경로로 이용하는 등 다양한 방식으로 사이버 공격이 이루어지고 있다[5]. 해킹 같은 사이버범죄 때문에 전 세계에서 매년 발생하는 경제적 손실 규모가 약 4,450억 달러, 우리 돈으로 450조 원에 이른다는 분석이 나왔다[2]. 이처럼 기업의 보안 실패는 피해를 당한 기업에 막대한 비용과 신뢰, 명성에도 손해를 끼쳐서 파산에까지 이르게 하여 기업 경영의 걸림돌이 될 수 있다[9]. 실제 정보가 유출되면 인건비, 수익 손실, 법적 보상금 등의 피해로 기업입장에서는 상당한 유무형적으로 피해를 입는다[3].

이제는 단순하게 해커가 실력과시 목적이 아닌 금전적 정치적 군사적인 목적을 가지고 해킹이 일어나고 있다[6].

그러나 대기업과 다르게 보안전문인력 및 투자여력이 부족한 중소기업은 외부에서 내부 중요서버 및 임직원 PC 대상으로 악의적인 공격이 이루어졌는지도 확인이 불가능한 실정이다. 이러한 중소기업의 온라인상 불법 침입시도를 보호하기 위해 한국산업기술보호협회의 중소기업기술지킴센터는 2011년 10월부터 중소기업청의 지원으로 중소기업 기술지킴서비스(보안관제서비스・내부정보유출방지서비스, 악성코드탐지서비스)를 제공하고 있으며, 2014년 9월 현재 1,560여 개 중소기업에 기술지킴서비스를 제공 중이며 이중에서 보안관제는 924개 중소기업에 지원하고 있다.

중소기업기술지킴센터를 통해 보안관제서비스를 지원받는 중소기업의 유해트래픽을 2014년 1월부터 6월까지 분석하고 효과적인 운영방안에 대해서 연구한다.

2. 관련 연구

2.1 사이버 보안위협의 진화

1986년 브레인바이러스를 시작으로 사상 최악의 컴퓨터 바이러스 대란으로 평가되는 1999년 CIH 바이러스는 국내에서 수십만대의 기업기관 개인 PC를 불능상태로 만들었다. 2003년에는 전세계 22만 7천대의 시스템을 감염시킨 블래스터 웜이 기승을 부렸다. 이처럼 1980년대 후반부터 2000년대 초반까지는 웜바이러스에 의한 사이버위협이 주를 이루었다. 그러나 2000년대 후반부터는 악의적 해커들은 일반 사용자의 개인용 PC보다는 은행, 언론, 정부 대상으로 악성코드와 APT, 제로데이 공격, DDoS (Distributed Denial of Service)를 이용하여 그들이 가진 그 무엇인가를 빼어가거나 혹은 무력화시켰다[11].

2.2 기존 중소기업 보안관제시스템 기술

중소기업이 운영하는 보안관제시스템은 아래와 같이 주로 5가지의 시스템을 운영하고 있다.

- 침입차단시스템(Firewall System) : 내부의 네트워크와 인터넷과 같은 외부의 네트워크 사이에 진입 장벽을 구축하는 보안 시스템으로 들어오고 나가는 모든 패킷을 분석하고 검사하여 부적절한 패킷을 차단한다.
- 침입방지시스템(IPS, Intrusion Prevention System) : 침입탐지 기능을 통해 패킷을 검사하여 패턴 분석 후, 비정상 패킷이면 방화벽 기능 모듈로 차단을 수행하는 시스템이다.
- 통합보안시스템(UTM, Unified Threat Management) : 하나의 장비에 다양한 보안 기능을 제공하는 보안 시스템으로 방화벽, VPN, IPS, Website Filtering 등 기능을 제공한다.
- 차세대방화벽(NG FW; Next-Generation Firewall) : 전통적 방화벽 성능 한계 해소를 위한 메신저와 특정 웹사이트 접근 제한 등 애플리케이션 제어기능이 보안과 결합된 시스템이다.
- Anti DDoS 장비(Anti-Distributed Denial of Service Attack) : 지능화된 DDoS 공격 방어하는 시스템으로, 행동기반 탐지/방어와 시그네쳐 기반 탐지/방어, 자동학습에 의한 탐지/방어 기능을 사용한다[1].

2.3 기존 중소기업 보안관제 시스템 문제점

한국인터넷진흥원의 올 1월부터 6월까지 해킹처리 건수는 8,078건으로 작년 1월부터 6월까지 6,146건에 비해 30% 증가된 모습을 보이고 있다[7]. 이처럼 해킹은 끊임없이 발생하고 있으며 이를 통한 사이버 보안위협은 점점 증가하고 있다.

〈Figure 1〉 Hacking Monthly Report

중소기업청에서 중소기업을 대상으로 해마다 실시하고 있는 중소기업 기술보호 역량수준조사에 따르면 기술보호 관련 투자액은 응답기업 544개 중소기업 중 38% 중소기업에서 1천만 원 미만으로 투자하고 있으며, 네트워크 보안솔루션인 방화벽을 운영하고 있는 중소기업은 1,518개 중소기업 중 826개 기업으로 54.4%의 중소기업에서 방화벽을 운영하고 다. 보안관리 부서 및 관리자가 없는 중소기업은 575개 기업으로 전체 중소기업 중 37.9%를 차지하고 있는 것으로 나타났다[8].

〈Table 1〉 Small Technical Competency Level Protection Investigation

Security Invest(criterion : million won)					
Section		0	~10	10~100	100~
large company	number	0	1	2	13
	%	0	2.3	4.7	30.2
small company	number	98	107	196	143
	%	6.5	7.0	12.9	9.4

Firewall Manage and Security Manager			
Section		Firewall Manage	Security Manager
large company	number	33	31
	%	76.7	72
small company	number	826	360
	%	54.4	23.7

이처럼 중소기업은 보안투자 여력 및 전문 인력 부족으로 외부에서 불법침입시도 발생 사실에 대해 인지도 할 수 없으며 인지하더라도 대처가 어려운 사항이다. 또한 야간이나 공휴일, 식사 등으로 인해 관리자가 자리를 비웠을 경우 온라인상으로 외부에서 불법침입시도는 확인 할 방법이 없다. 이러한 중소기업의 온라인상 불법침입시도를 24시간 모니터링 해 주는 보안관제서비스가 필요하며 지속적으로 외부에서 발생하고 있는 악의적인 행위 및 최신 보안위협에 대처하기 방안이 필요한 실정이다. 이를 해결하기 위해 중소기업기술지킴센터가 2011년부터 개소하여 중소기업에 무상으로 보안관제서비스를 제공하며 외부에서 불법침입시도 발생 시 통보 및 조치를 지원하고 있다.

3. 중소기업 유해트래픽 분석 결과

3.1 전체 이벤트 탐지 분석

중소기업기술지킴센터에서 2014년 1월~6월까지 총 6개월간 발생한 이벤트는 587억 여건 발생하였으며, 일일 평균 3.2억 건이 발생하였다. 탐지된 이벤트 중 99%는 방화벽기반으로 탐지 되었으며, 탐지된 이벤트중 55.39%는 중소기업기술지킴센터 보안정책에 의해 사전 차단되었다.

3.2 방화벽 차단 및 허용

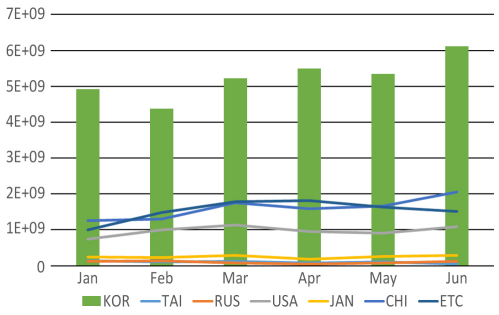
14년 1월부터 6월 전체 이벤트는 총 587억 여건이 발생하였으며, 2월부터는 방화벽 차

〈Table 2〉 Monthly Full Event Detection

Section		Event	Block		Allow	
			Fire wall	IPS	Fire wall	IPS
Jan	M.T	8,386,626,311	4,140,778,231	13,063,693	4,245,748,080	80,961,681
	D.A	270,633,107	421,406	421,406	136,959,615	2,611,664
Feb	M.T	8,616,746,318	4,730,100,772	6,886,931	3,886,645,546	32,161,573
	D.A	307,706,226	168,932,170	245,926	138,773,055	1,148,628
Mar	M.T	10,384,261,167	6,669,710,019	9,702,076	4,814,541,148	61,192,456
	D.A	334,976,844	179,668,065	312,970	156,307,779	1,973,950
Apr	M.T	10,127,744,686	6,881,276,478	5,858,160	4,246,468,108	60,040,573
	D.A	337,691,486	196,042,549	196,272	141,548,937	2,001,352
May	M.T	10,003,875,901	5,935,468,923	4,377,782	4,068,406,978	44,859,120
	D.A	322,706,674	191,466,739	141,219	131,238,935	1,447,068
Jun	M.T	11,218,602,781	6,275,667,695	2,480,119	4,943,035,086	43,738,656
	D.A	373,953,426	209,185,590	82,671	164,767,836	1,457,955

*M.T : Monthly Total, D.A : Daily Average.

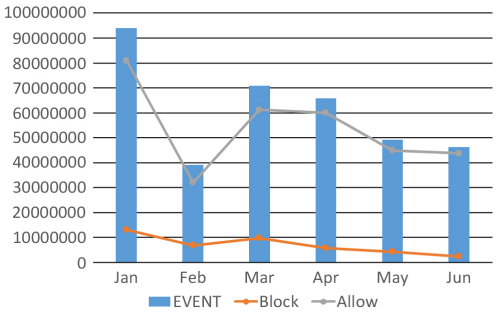
단 건수가 증가하였는데, 이는 중소기업기술지킴센터의 중소기업 지원기업 증가에 따른 트래픽 증가와 중소기업에서 발생하는 유해트래픽이 증가하였으며 이를 센터에서 차단 및 차단 요청을 하였다. 방화벽 기반으로 탐지되는 이벤트는 보안정책 설정으로 전체 55% 수준이 차단되고 있다. 평일 평균 3억~4억여건 이벤트가 발생하며, 주말 및 휴일에는 2억여건 전후로 이벤트가 발생한다. 일부 특정 기업에서 악성코드 발생, 외부로부터 DDoS 공격이 발생하여 평일 수준대비 1억 건 이상 발생하여 지킴센터에서 조치를 지원하였다.



〈Figure 2〉 Monthly Firewall Blocked

3.3 국가별 불법침입시도 분석

국가별 이벤트는 한국이 53.57%로 전체의 절반 이상이 탐지되었으며 중국 16.18%, 미국 9.9% 순으로 탐지되었고 기타 영국 등 810여개 기업에서도 다수 탐지되었다. 포트별 접근은 80/TCP가 전체의 31.3%로 가장 많았으며, 이는 웹서비스를 이용하기 위한 HTTP 포트로써 일반적인 인터넷 사용에 가장 많이 쓰이며, 다음으로 회선체크 목적의 0/ICMP, 도메인 네임 서비스 이용 목적의 53/UDP순으로 많이 탐지되었다. 한국의 불법침입시도는 스캐닝 관련 유해트래픽이 많았으며, 중국 및 미국의 불법침입시도는 웹 관련된 유해트래픽이 많이 발생하여 한국과 외국간의 공격유형이 달랐다.

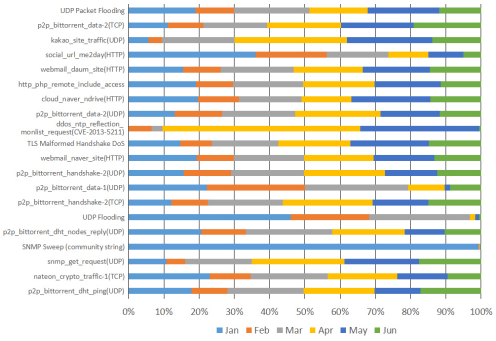


〈Figure 3〉 Regional Analysis Trespass Attempt

3.4 IPS 탐지 분석

IPS 룰에 의해 탐지되는 이벤트는 88%이상 UTM 장비에서 보안정책에 의해 차단되었으며, 중소기업기술지킴센터에서 지속적인 탐지룰 분석과 UTM 장비 제조사와 협조하여 보안정책을 최적화하여 유해 이벤트의 유입을 차단하였다. Torrent 사용자들 사이에 활성 유무 상태를 확인하는데 사용되는 p2p_bittorrent_dht_ping(UDP)가 22.9%로 가장 많이 탐지되었으며, 그 다음으로 SK Communications에서 개발한 네이트온 메신저를 탐지하는 nateon_crypto_traffic-1(TCP)이 11.9%를 차지하였으며, 네트워크 장비의 환경설정, 장비 및 네트워크 성능 통계 정보를 수신하기 위해 사용하는 SNMP 관련된 snmp_get_ request(UDP)가 11.7%를 차지하였으며 이들 세 이벤트가 전체 이벤트의 46.5%를 차지하였다. 이러한 중소기업에서 발생한 IPS 이벤트

분석 결과, 중소기업들은 P2P 파일 공유 제한, SNMP, 메신저 프로그램의 사용 제한이 없는 걸로 보이며, 이러한 보안정책이 미설정되어 있는 경우 특정사용자에 의한 네트워크 트래픽이 과다 발생할 수 있으며 SNMP의 보안설정이 되어 있지 않은 경우에는 DDoS 공격에도 악용 될 수 있는 위험이 있다[4].



〈Figure 4〉 IPS Detection Analysis

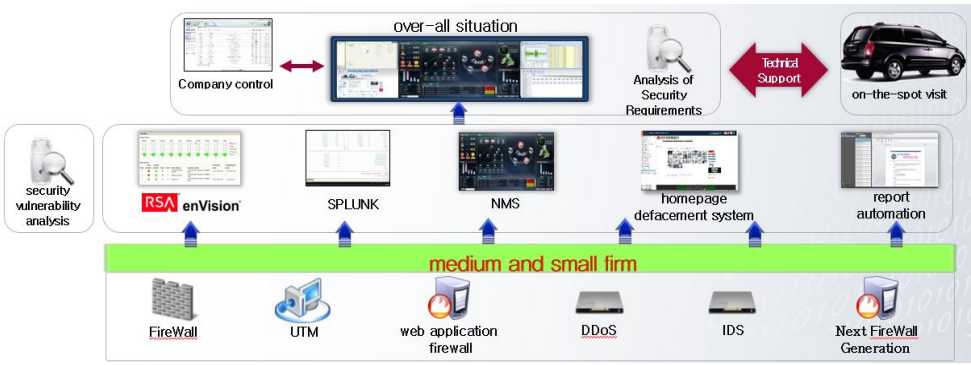
3.5 중소기업기술지킴센터 유해트래픽 대응 결과

중소기업기술지킴센터에서는 유해트래픽을 탐지 할 경우 해당 중소기업에 메일 및 SMS, 유선을 통해 통보하고 있으며 조치가 어려운 중소기업의 경우 원격 및 현장방문을 통한 조치를 지원하고 있다. 2014년 1월~6월까지 1,501건의 이상징후에 대해 통보하였다. 또한 지킴센터에서 탐지한 이벤트 내역을 확인 한 결과를 바탕으로 중소기업기술지킴센터에서는 중소기업 환경에 맞는 보안정책을 수립하여 P2P 및 메신저 사용을 제한하도록 권고하고 있으며, 시스템 및 네트워크의 보안설정 및 취약점을 주기적으로 점검하여 통보하고 있다. 이러한 중소기업들의 노력이 더해진다면 온라인상으로 외부에서 중소기업의 내부 중요 시스템 및 임직원 PC 대상으로 불법침입을 방지하는데 큰 효과를 거둘 수 있을 것이다.

4. 중소기업 보안관제서비스 한계 및 발전방안

4.1 중소기업 보안관제서비스 한계

고객정보가 유출된 옥션(2008), SK컴즈 사고(2011), 최근에 발생된 애플 아이클라우드의 해킹 사고(2014)는 보안관제를 실시하지 않아서 발생한 문제가 아니다. 이들 기업 모두 보안관제는 실시하고 있지만 관제대상과 범위가 네트워크 영역으로 한정되어 있고 단순하게 외부로부터의 불법침입 시도만 탐지하는 보안관제체계가 사고의 원인일 수 있다. 이러한 보안관제 체계로는 제로데이 공격이나 내부 임직원 PC 대상으로 APT 공격, 사회공학적 공격 등에는 대처가 어려운 상황이다. 중소기업 대상 사이버 위협도 과거처럼 단순 네트워크 불법침입 시도를 통해 이루어지는 경우보다는 이메일 및 USB 등의 악성코드 감염을 통한 기술유출 등 중소기업 네트워크 망을 통한 다양한 사이버 위협이 이루어지고 있다. 중소기업기술지킴센터에서는 중소기업이 보유하고 있는 네트워크 보안장비 또는 임대장비로부터 시스템 로그를 수집하여 센터의 통합로그분석시스템을 통해 이상징후를 분석하여 이상징후 발생 시 중소기업에 통보하고 있으며, 중소기업에서는 통보된 상황에 대해서 시스템 분석 및 대응조치를 수행하는 방식으로 보안관제 모니터링 체



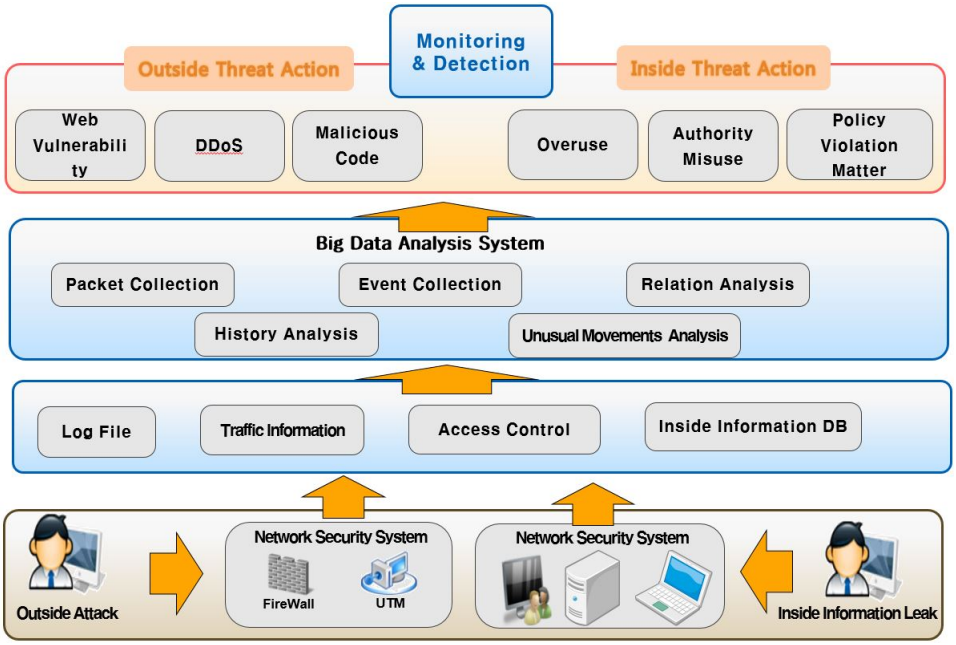
〈Figure 5〉 Security Monitoring System of Small and Medium Business Monitoring Center

계가 이루어지고 있다. 이러한 보안관제체계는 보안관제체계 구축예산, 보안 전문인력 등을 중앙 관제센터에서 제공하므로 예산 효율성과 부족한 보안인력 수급 문제 해결 측면에서 효과적인 특징이 있으나, 이러한 이상징후에 대해 단일 네트워크 보안장비만으로부터 발생하는 로그 수집을 통해 분석 및 통보하여 실제 해킹 여부에 대해 분석도 어렵고 상관관계분석이 어려운 실정이다.

4.2 중소기업 보안관제서비스 발전 방안

중소기업기술지킴센터는 중소기업의 보안관제라는 목적성을 가지고 보안관제를 수행하고 있으며, 국내외에서 사례를 찾아 볼 수 없을 정도로 다양하고 많은 중소기업에 대해 보안관제 지원을 하고 있다. 이러한 중소기업 보안관제가 더욱 발전해 나가기 위해서는 다음과 같은 발전방향을 모색할 필요가 있다. 첫째, 빅데이터 분석 기술을 적용하여 보다 효과적인 모니터링과 분석·대응체계를 구현하여야 한다. 빅데이터 모니터링 시스템은 보안장비 및 중요 DB와 같은 내부 시스템과 출입통제시스템 CCTV 등과 같은 물리 보안시스템으로부터 발생하는 각종 로그를 지킴센터에서 수신하여 트래픽 정보, 접근 제어 정보, 각종 DB정보에 대해서 패킷분석, 이벤트 분석, 히스토리 분석, 연관분석, 이상패턴 분석, 최신위협 분석 등을 실시하여 외부위협 및 내부유출에 대해 대응할 수 있는 체계를 구성할 수 있다. 또한 이런 분석된 정보는 많은 정보들을 텍스트 형태로 나타내는 것이 아닌 대시보드를 통해 다양한 검색 방식, 군집화, 추적관리, 지역분포 등을 통해 의미있는 값들을 시각화하여 보다 다양하고 정밀한 분석정보를 모니터링 요원들에게 제공하여 다양한 이상징후 정보에 대해 중소기업에 통보 해 줄 수 있다. 빅데이터를 활용한 보안 분석(big data security analytics)은 국내 다양한 업종의 중소기업에서 발생하는 보안데이터 분석 기술을 통해 중소기업기술지킴센터에서 고도의 모니터링과 정밀분석을 통해 기존에 해결하지 못한 사이버 공격 위협 분석을 가능하게 할 것이다. 둘째, 다양한 상황으로부터 발생한 정보를 취합하고 상호연관성을 처리하는 상황인식 지능형 보안관제체계가 필요하다.

최근의 사이버 위협은 매우 빠르게 발전하고 있으며 기존의 보안관제나 백신에 탐지되지 않도록 숨김 기능, 백신 우회 기능 등을 이용하여 최신의 Zero-day 공격에는 대응하기 어려운 측면이 존재한다. 이러한 새로운 사이버 위협으로부터 효율적으로 탐지 대응하기 위해서는 탐지 패턴과 일치할 경우 공격으로 판단하는 패턴기반 탐지와 지속적인 네트워크 특성 및 사용자 정보 등을 학습시켜 기존에 발생되지 않은 이상한 행위 탐지 시 공격으로 간주하는 행위기반 탐지를 접목시킨 상관분석 체계가 구성되어야 한다. 사용자의 접근 권한, 자산정보, 시스템 취약점, 중요정보 처리 현황, 최신 외부 위협 정보 등을 통해 각종 이벤트에 대한 비정상 조건들을 잘 정의하여 특정조건들에 대한 분석을 통해 이상징후 분석을 실시하는 상황인식 기반 보안관제 체계가 가능하다. 셋째, 물리적 보안과 기술적 보안이 융합된 융합보안관제체계가 수립되어야 한다. 최근 물리적 보안과 IT 보안이 점점 융합되고 있는 추세이다. 네트워크 및 시스템 보안시스템과 물리 보안시스템이 이중으로 구성되어 관리되는 형태가 아닌 하나로 통합되어 관리되는 체계가 융합보안관제체계이다. 이러한 융합보안체계를 통해 네트워크 및 내부 시스템으로 발생하는 내부임직원의 이상행위에 대해 출입통제시스템과 CCTV 등 물리보안시스템과 연계하여 보안시스템으로부터 IP, 네트워크 사용현황, 시스템 접속 기록 등에 대해 확인하고 물리보안시스템을 통해 해당 시간의 출입자 정보, 출입시간 등에 대해 조합하여 정밀한 분석과 효과적인 원인 추적이 가능하다.



〈Figure 6〉 Big Data Security Analysis System

5. 결 론

현재 지능화, 고도화 되고 있는 사이버 위협으로부터 기업이 보안에 지원하는 비용과 보안 전문인력이 부재한 중소기업을[10] 사이버 상에서 보호하기 위해서는 정부 지원을 통한 중소기업기술지킴센터의 보안관제서비스가 반드시 필요하다. 이를 통해 보안전문인력이 24시간 보안관제를 실시하여 이상징후 발견 시 통보 및 조치 지원이 필요하다. 이처럼 중소기업기술지킴센터는 정부의 예산 지원을 통해 중소기업에게 저비용・고효율의 보안을 제공하는 등 순기능 요소가 있다. 본 논문에서는 중소기업 보안관제를 실시하고 있는 중소기업기술지킴센터의 보안관제를 통해 중소기업에 제공하는 보안관제서비스에 대해 효용성에 대해 기술하였다. 또한 중소기업기술지킴센터의 보안관제 한계를 통해 중소기업의 보안관제 개선방안도 제시하였다. 중소기업기술지킴센터가 설립목적에 맞게 중소기업의 온라인상 기술유출 방지 지원을 강화해 나가기 위해서는 중소기업 환경에 적합한 빅데이터 분석 기술, 상황인식 지능형 보안관제체계, 융합보안관제체계에 대한 마스터플랜과 지속적인 연구가 필요하다.

References

[1] Ahn, S. J., Lee, K. H., and Park, W. H., “Security Monitering and Control,” Ehanmidia, pp. 212-244, 2014.

[2] Center for Strategic and International Studies, “Net Losses : Estimating the Global Cost of Cybercrime,” Mcafee, 2014. 6. 9.

[3] Han, C. H., Chai, S. W., and Yoo, B.-J., “A Quantitative Assessment Model of Private Information Breach,” Journal of Society for e-Business Studies, Vol. 16, No. 4, pp. 17-31, 2011.

[4] Hyun, T. W., “Attack Method and Countermeasure using SNMP Vulnerability,” Dongseo University CNSL, 2009.

[5] Inca Internet Inc. Ltd, “2014 year security report,” 2013. 11. 29.

[6] Kim, C. H., “Security Threat and Countermeasure of financial transactions,” Privacy Security Conference, 2010.

[7] KISA, “Internet Incident Response Report,” 2014.

[8] Korea Technology and Information Promotion Agency for SMBs, “2013 Small and Medium Business Technology Security and Research,” 2013.

[9] Lee, Y. and Larsen, K. R., “Threat of Coping Appraisal : Determinants of SMB Executives’ Decision to Adopt Anti-Malware Software,” European Journal of Information Systems, Vol. 18, pp. 177-187, 2009.

[10] Nho, M. S. and Lee, S. Y., “Industrial Security of Small and Medium Business Research,” Korea Association for Public Administration, Vol. 44, No. 3, pp. 239-259, 2013.

[11] Park, S. T., “2013 year Main Incident Case and Response,” 2013 Hacking Defance Work shop, 2013.

저 자 소 개

홍준석 (E-mail : jun0817@kaits.or.kr)
2012년 성균관대학교 정보통신대학원 정보보호전공 (공학석사)
2013년~현재 서울과학기술대학교 IT정책대학원 산업정보시스템 (박사과정)
한국산업보안기술협회 중소기업기술지킴센터 관제운영팀장
관심분야 보안관제정책, 침해사고대응, 중소기업 보안

임영환 (E-mail : yhlim@seoultech.ac.kr)
2008년 서울과학기술대학교 산업대학원 정보산업공학과 (공학석사)
2011년~현재 서울과학기술대학교 IT정책대학원 산업정보시스템 (박사과정)
현대오토에버 SI인프라팀 근무
관심분야 보안관제정책, 정보보안감사, 융합보안

박원형 (E-mail : whpark@kdu.ac.kr)
2002년 서울과학기술대학교 산업정보시스템공학과 (공학사)
2005년 서울과학기술대학교 정보산업공학과 (공학석사)
2009년 경기대학교 정보보호학과 (이학박사)
2011년 서울과학기술대학교 산업정보시스템공학과 겸임교수
현재 극동대학교 사이버안보학과 조교수/학과장
관심분야 보안관제기술, 윈도우포렌식, 산업보안

국광호 (E-mail : khkook@seoultech.ac.kr)
1979년 서울대학교 산업공학사
1981년 서울대학교 대학원 산업공학 (석사)
1989년 미조지아 공과대학교 대학원 산업공학 (박사)
1989년~1993년 한국전자통신연구원 선임연구원
1993년~현재 서울과학기술대학교 기술경영융합대학
글로벌융합산업공학과 교수
관심분야 정보보호, 정보통신, 산업보안