특집 07

국내 중소기업 보안 서비스 실태 및 수요분석

전덕조 ((주)씨큐비스타), 이일주 (동원대학교)

목 차 »

1. 서 론

최근 여러 해킹사고들로 인하여 기업들이 자사의 정보보호 체계를 재점검하고 대책을 마련하는데 분주하다. 기업의 정보보호 관리체계가 일정 수준에 도달해 있는 대기업 및 금융기관조차 해킹의 위협으로부터 자유로울 수 없는 상황인 것을 고려하였을 때, 상대적으로 정보보호 투자 전담인력이 부족한 중소기업의 경우 정보보호 대책이 미흡한 것은 필연적인 결과이다. 또한 2013년 국정감사 결과 정보보호 대책 수립이 미비한 기업은 대체로 중소기업으로, 개인정보보호법 등 관련법규가 요구하는 최소한의 정보보호 조치조차 제대로 이행하지 못하는 실정이다. 이렇듯 표면적으로 드러나는 중소기업의 부족한 정보보호 실태를 본 조사를 통해 명확하게 파악하고 향후 개발될 빅데이터 기반 사이버위협 예측. 분석 서비스에 대한 중소기업들의 실제 수요를 파악하여 정책적 활용성을 높이는 것을 목표로 본 조사를 실시하였다.

이 논문은 2013년도 한국 인터넷 진흥원의 지원으로 연구하였음

2. 조사개요

• 조사 내용 및 범위

본 조사는 국내 중소기업의 정보보호 기반 및 환경, 정보보호 대책, 침해사고 피해 및 대응활동, 기존 보안서비스 현황 및 문제점, 빅데이터 기반의 사이버 위협 예측/분석 서비스 수요를 파악할 수 있는 지표로 구성하였다.

본 조사의 주요 내용은 다음과 같다.

- 기업 내 정보보호 정책수립 및 정보보호 조직 구성 현황
- 기업 내 정보보호 장비 및 솔루션 보유 현황
- 침해사고 내용 및 영향
- 기존 보안서비스 현황 및 문제점

· 기존 보안서비스 개선사항
· 빅데이터 기반의 사이버 위협 예측/분석 서비스 수요 파악
· 선호하는 보안서비스 방식

• 조사 체계

· 조사 대상 : 종사자수 5인이상, 네트워크에 연결된 컴퓨터를 1대 이상 보유한 중소기업
· 조사 기간 : 2013. 10. 14 - 2013. 10. 25
· 조사 방법 : 방문 면접조사
· 조사 기관 : 여론조사전문기관 ㈜서던포스트

3. 중소기업 보안 서비스 실태 분석

3.1 정보보호 실태파악

· 정보보호 책임자 지정 현황

중소기업의 정보보호 책임자 지정 현황은 50.0%인 것으로 조사되었다. 업종별로는 '금융'에서 75.0%로 정보보호 책임자 지정이 가장 많이 되고 있는 것으로 조사 되었으며 다음으로는, IT(66.7%) > 제조(58.3%) > 설계/건설(57.1%) 등 순으로 조사되었다. 반면, '유통'의 경우 총 응답 사업체 중 7.1%만이 정보보호 책임자를 지정하

〈표 1〉 표본의 특성

구 분			%	구 분			%
전 체		(102)	100.0				
업종	IT	(42)	41.2	전담조직 운영여부	예	(38)	37.3
	미디어 출판/교육	(10)	9.8		아니오	(64)	62.7
	유통	(14)	13.7	정보보호 예산	300 만원미만	(15)	14.9
	금융	(8)	7.8		300-700 만원 미만	(34)	33.7
	의료	(9)	8.8		700-1,300 만원 미만	(29)	28.7
	제조	(12)	11.8		1,300 만원 이상	(23)	22.8
	설계/건설	(7)	6.9	침해사고 경험유무	예	(19)	18.6
연평균 매출	20억 미만	(28)	28.9		아니오	(83)	81.4
	20억 - 50억 미만	(27)	27.8	인터넷 속도	100Mbps	(63)	63.0
	50 - 100억 이하	(24)	24.7		500Mbps	(23)	23.0
	100억 이상	(18)	18.6		1Gbps	(14)	14.0
직원 수	10명 미만	(13)	12.7	선호 패키지 타입	수요 없음	(22)	21.6
	10-50명 미만	(30)	29.4		Lv1패키지	(28)	27.5
	50-100명 미만	(42)	41.2		Lv2패키지	(26)	25.5
	100명 이상	(17)	16.7		Lv3패키지	(26)	25.5

고 있다고 응답하여 상대적으로 낮은 정보보호 책임자 지정률을 보인다. 연평균 매출별로는 '100억 이상' 매출을 올리는 사업체의 경우 66.7%의 업체가 정보보호 책임자를 지정하고 있는 것으로 답하였다. 그러나 '50억-100억 미만'의 매출을 올리는 사업체의 경우 상대적으로 낮은 41.7%로 조사되었다.

· 정보보호 전담조직 설치, 운영 현황 및 조직 구성원 수

국내 중소 사업체 중 정보보호 전담조직을 설치, 운영하는 사업체는 37.3%에 그쳐 다소 낮게 나타났다. 업종별로는 '금융'이 62.5%로 다른 업종에 비해 활발히 운영되는 것으로 나타났다. 그 밖에 제조(50.0%) > 의료(44.4%) > 설계/건설(42.9%) > IT(40.5%)등 순으로 정보보호 전담조직을 설치, 운영하는 것으로 조사되었다. 매출별로는 정보보호 전담조직을 설치, 운영하는 비율이 '100억 이상', '20억-50억 미만' 사업체에서 44.4%로 나타났다. 하지만, 매출 '20억 미만'의 업체는 정보보호 전담조직 설치, 운영하는 비율이 32.1%에 그쳐 상대적으로 낮게 조사되었다. 또한, 정보보호 전담조직의 구성원 수는 평균 3.6명으로 나타났으며 업종별로 살펴보면 유통(5.0명) > 금융(4.0명) > IT(3.9명) > 의료(3.7명) 등 순으로 파악되었다.

· 정보보호 방침 및 지침 수립 현황

정보보호 방침 및 지침이 수립되어 있는 사업체는 44.1%로 조사되었다. 업종별로는 '금융'(62.5%)'의 정보보호 방침 및 지침 수립률이 가장 높으며 사업체의 직원 수가'100명 이상'(64.7%)인 사업체에서 정보보호 방침 및 지침 수립률이 높은 것으로 나타났다.

· 연간 정보보호(보안)관련 예산

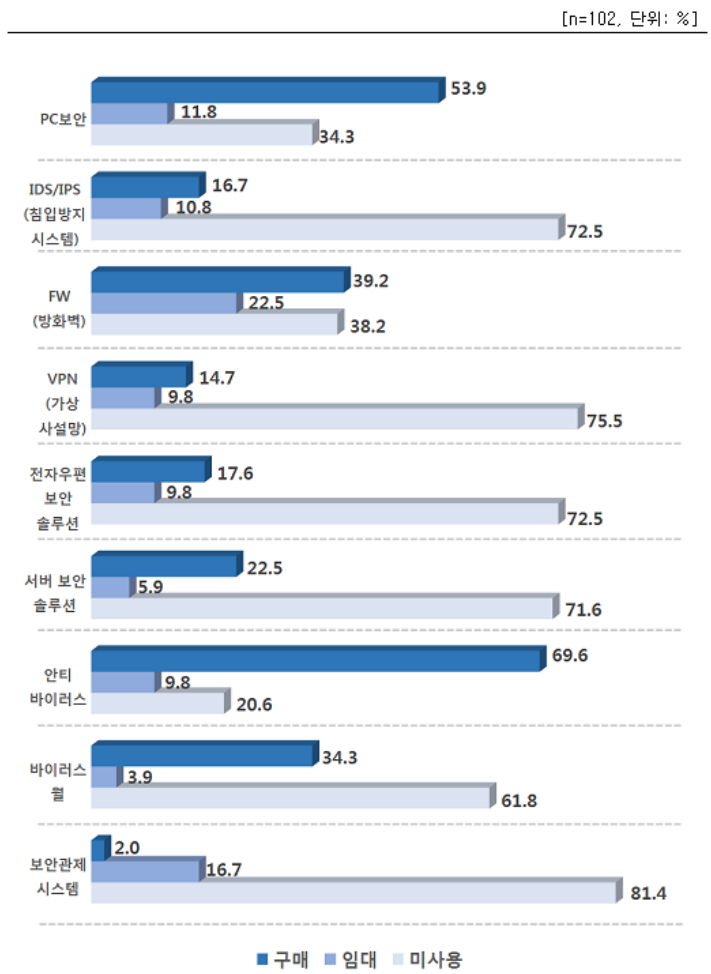
국내 중소 사업체의 연간 정보보호 관련 예산은 평균 1,878만원으로 나타났으며, 업종별로는 '금융(6313만원)'이 타 업종대비 많은 금액을 연간 정보보호 관련 예산으로 책정하고 있는 것으로 나타났다. 반면, '미디어/출판/교육(555만원)'이 가장 낮은 금액을 정보보호(보안)관련 예산으로 책정하고 있는 것으로 조사되었다. 매출별로는 사업체의 매출이 클수록 연간 정보보호(보안) 관련 예산으로 사용하는 금액이 높은 것으로 나타났다.

· 정보보호(보안) 장비 및 솔루션 보유(사용) 내역

정보보호 장비 및 솔루션 중 국내 중소 사업체는 '안티바이러스' 제품이 69.6%로 가장 많은 사용경험이 있었으며, 다음으로 PC제품(53.9%) > FW방화벽(39.2%) > 바이러스월(34.3%) > 서버 보안솔루션 (22.5%)이 그 뒤를 따랐다. 정보보호 장비 및 솔루션 중 임대 경험이 가장 많은 것은 'FW방화벽 (22.5%)' 으로 나타났으며, 다음으로 보안관제시스템(16.7%) > PC제품(11.8%) > IDS/IPS침입방지 시스템 (10.8%) 등 순으로 조사되었다. 아울러, 중소 사업체는 보안관제시스템(2,449만원)에 가장 많은 정보보호(보안) 장비 및 솔루션 연간유지비용을 지출한 경험이 있는 것으로 나타났다. 반면, 바이러스월 (129만원)에는 가장 낮은 연간유지비용을 지출한 경험이 있는 것으로 조사 되었다.

· 최근 3년 이내 해킹, 바이러스 등으로 인한 침해사고 여부

중소 사업체 중 18.6%가 최근 3년 이내 해킹, 바이러스 등으로 인하여 침해사고를 경험한 것으로 조사되었다.



(그림 1) 정보보호(보안) 장비 및 솔루션보유(사용) 내역

· 해킹, 바이러스로 인한 침해사고 내용

악성코드감염으로 인한 피해사고를 경험한 횟수는 연간 2.8회로 가장 높게 나타났으며 영향 받은 시스템 대수 역시 4.7대로 가장 많은 시스템이 악성 코드감염으로 인한 피해를 입은 것으로 조사되었다. 반면, 웹 서버해킹으로 인해 피해를 입은 횟수는 연간 1.3회로 다소 낮게 나타났으며 영향 받은 시스템 대수 또한 1.3회로 가장 낮게 나타났다.

· 침해사고가 사업상 미친 영향

정보보안 침해사고 피해의 사업상 미친 영향은 '네트워크 일시마비 등 약간심각'이 47.4%로 조사되었으며, 그 다음으로 '일시적 불편등 약간의 영향 미침'이 31.6%, '거의 영향 없음'이 21.1%로 나타났다. 반면'사업의 일시중단, 주요정보 유출 등 매우 심각'으로 응답한 사업체는 없는 것으로 나타났다.

· 침해사고 피해 복구 시간

사업체의 정보보안 침해사고 피해발생 후 복구하는데 소요된 시간은 '1주일 미만'이 78.9%로 조사되었다. 그 다음으로 침해사고 피해 복구에 '약 1-2주일'이 소요된 사업체는 21.1%로 나타났다.

3.2 기존 보안 서비스 현황 및 문제점 파악

· 중소 사업체의 인터넷 회신 접속 속도(대역폭)

중소 사업체의 인터넷 회신 접속 속도(대역폭)은 100Mbps(63.0%)를 가장 많이 사용하는 것으로 조사 되었으며, 1Gbps를 사용하는 사업체는 14.0%에 그친 것으로 나타났다.

· 정보보호(보안) 관련 서비스 이용률

정보보호 침해사고를 대비하여 현재 관련 서비스를 이용하는 중소 사업체는 22.5%에 그친 것으로 나타났다. 업종별로는 '금융(37.5%)'업체가 정보보호 관련 서비스를 가장 많이 이용하는 것으로 나타났으며, 그 다음으로는 '의료(33.3%) > 설계/건설(28.6%) > 제조(25.0%) 등 순으로 나타났다. 또한, 사업체의 직원 수가 많을수록 정보보호 관련 서비스 이용률이 높은 것으로 조사 되었다.

· 이용중인 정보보호(보안) 관련 서비스

정보보안 침해사고에 대응하고 예방하기 위하여 사업체들이 이용하는 정보보호 (보안)관련 서비스로는 '보안관제(43.5%)', '취약점점검(39.1%)', '보안컨설팅(8.7%)', '기타(8.7%)'의 순으로 나타났다.

· 보안서비스를 받은 기간

정보보호 서비스를 받고 있는 중소 사업체의 보안서비스를 받은 기간은 '1년 이상(81.0%)'가 가장 많이 조사되었으며 '1년 이하(9.5%)'와 '6개월 이하(9.5%)' 라는 응답 역시 나타났다. 또한 업종별로는 'IT(100%)', '금융(100%)', '설계/건설(100%)'가 1년 이상 보안서비스를 받아 온 것으로 가장 많이 응답 하였다. 반면 '유통' 업종의 경우 '6개월 이하(100%)'가 나타나 타 업체와는 대조적인 조사 결과를 보였다.

· 이용중인 보안 서비스의 종류와 비용

정보보안 침해사고 대응 및 예방을 위해 중소 사업체들이 이용한 경험이 있는 보안 서비스는 'IDC', '취약점점검', '보안관제', '방화벽', 'UTM' 등으로 조사 되었다. 아울러, 보안 서비스 비용은 'IDC(7,000만원)'이 가장 높은 것으로 나타났으며 '보안관제(1,233.3만원)', '취약점점검(1,125만원)', '게임가드(1,000만원)' 등 순으로 나타났다. 반면, 'UTM(300만원)'과 '호스팅(600만원)'에 대해서는 상대적으로 적은 서비스 비용을 지불하는 것으로 나타났다.

· 현재 이용하고 있는 보안 서비스 점검주기

현재 이용하고 있는 보안 서비스 점검주기는 '상시(50.0%)'가 가장 높은 응답률을 보였으며, '1년 2회'씩 보안 서비스 점검을 받는다고 응답한 비율 역시 31.8%로 상대적으로 높게 나타났다. 반면 '분기별 1회', '기타'로 응답한 비율은 각각 9.1%로 낮게 조사되었다.

· 보안서비스를 이용하지 않는 이유

현재 정보보호(보안) 관련 서비스를 이용하지 않는 사업체를 대상으로 보안 서비스를 이용하지 않는 이유를 물었을 때, '고비용(52.7%)' 문제로 응답한 비율이 가장 높게 나타났다. 그 다음으로는 '자체 해결(36.5%)', '관심 없음(5.4%)' 등이 뒤를 이었다.

· 보안 취약점(문제점) 발견 시 조치 방법

정보보호(보안) 서비스를 이용하지 않는 중소 사업체에게 보안 취약점(문제점) 발견 시 조치 방법을 물었을 때 '내부인력활용(52.7%)'가 가장 높은 응답을 얻었다. 다음으로, '외부전문업체활용(39.2%)', '발견된 적 없음(6.8%)' 등 순으로 나타났다.

· 기존 보안 서비스의 문제점 중 우선적으로 개선되어야 할 사항

기존 보안 서비스에 대해 가장 '비용문제(61.1%)'가 가장 우선적으로 개선되어야 할 사항으로 평가 되었으며 '침해사고 예방 및 사후조치 미비(14.7%)','사고원인 분석의 전문성 부족(14.7%)'가 개선이 필요한 사항으로 조사 되었다.

3.3 빅데이터 기반 신개념 보안서비스 수요조사

· 빅데이터 기반의 사이버 위협 예측분석 서비스 패키지 수요

중소 사업체의 빅데이터 기반의 사이버 위협 예측분석 서비스 수요를 패키지 별로 살펴보면 'LV1 패키지(IP 평판기반서비스)'가 27.5%로 가장 높은 수요를 나타내며 그 다음으로는 'LV2 패키지(LV1 +악성코드 분석 서비스) (25.5%)', 'LV3 패키지(LV1 + LV2 + 네트워크 통신 이상분석 및 종합 상관분석 서비스) (25.5%)' '수요없음(21.6%)'의 응답률을 나타냈다.

하지만, 빅데이터 기반의 사이버 위협 예측분석 서비스 패키지는 유료로 판매가 이루어지는 점, 최소가격이 연간 150만원으로 책정되어 있다는 점을 고려하였을 때 현재 최소한의 정보보호(보안) 장비 및 솔루션을 보유(사용) 하고 있는 사업체에서 실제 수요가 발생할 것으로 예상된다. 따라서, 실제 수요를 예측하기 위해서는 본 항목을 F/W(방화벽) 보유 경험이 있는 사업체를 대상으로 분석해 볼 필요성이 존재한다.

방화벽을 보유(사용)한 경험이 있는 사업체를 대상으로 빅데이터 기반 사이버 위협 예측 분석 서비스 패키지 수요를 파악해 본 결과 'LV1 패키지(28.6%)'가 가장 높은 수요를 보였으며 'LV2 패키지(27.0%)' = 'LV3 패키지(27.0%)' 순으로 나타났다. 이는 전체업체를 대상으로 수요를 파악하였을 때보다 각 1.5% 상승한 결과이며 '수요없음'의 경우 4.1%가 하락한 17.5%로 나타났다. 업종별로 살펴보면 'LV1 패키지'에 대한 수요는 '제조(50.0%)', '설계/건설 (66.7%)'에서 높게 나타났으며 'LV2 패키지'에 대한 수요는 '미디어(50.0%)', '유통(62.5%)', '의료(50.0%)' 업종에서 높게 조사되었다. 또한, 'LV3 패키지'에 대한 수요는 '유통'과 '의료'를 제외한 모든 업종에서 25.0% 이상으로 고르게 나타났다.

· IP평판 기반 서비스에서 가장 중요한 요인

IP평판 기반 서비스에서 가장 중요한 요인으로 '위험IP 접속의 근거 및 내용 (48.8%)'가 가장 많은 응답을 얻었으며 그 다음으로는 '위험 외부IP의 접속여부 (35.0%)', '위험 외부IP의 위험도 수준(16.3%)' 등 순으로 조사되었다. 또한, 선호패키지 타입별로 살펴보면 'LV1 패키지'를 선호하는 중소 사업체의 경우 '위험IP 접속의 근거 및 내용(42.9%)', '위험IP 접속여부(42.9%)'가 가장 중요하다고 응답하였으며 'LV3 패키지'를 선호하는 사업체 역시 '위험IP 접속의 근거 및 내용(46.2%)', '위험IP 접속여부(42.3%)'가 가장 중요하다고 대답 하였다. 반면, 'LV2 패키지'를 선호하는 사업체의 경우 '위험IP 접속의 근거 및 내용(57.7%)'가 가장 중요하며 그 다음으로는 '위험

외부IP의 위험도 수준 (23.1%)'가 중요하다고 응답하였다.

방화벽을 보유한 경험이 있는 사업체를 대상으로 살펴보면 '위험IP 접속의 근거 및 내용(46.2%)'가 가장 중요한 요인으로 판단되었으며, 그 다음으로는 '위험 외부IP 접속여부(42.3%)'등 순으로 조사되었다. 선호 패키지별로는 'LV1 패키지'를 선호하는 사업체의 경우 '위험 외부IP 접속 여부(55.6%)'가 가장 중요하다고 응답하였으며 'LV2 패키지'를 선호하는 사업체의 경우 '위험IP 접속의 근거 및 내용(58.8%)'가 가장 중요한 요인으로 판단하였다. 'LV3 패키지'를 선호하는 사업체의 경우 '위험 외부IP 접속 여부(47.1%)', '위험IP 접속의 근거 및 내용(41.2%)'등 순으로 중요한 요인을 응답하였다.

· 악성코드 분석 서비스 제공 시 중요한 부분

악성코드 분석 서비스 제공 시 중요한 부분으로는 '신속한 악성코드 탐지(53.8%)'가 가장 많은 응답을 얻었다. 그 다음으로 '포괄적인 악성코드탐지(25.0%)', '분석 보고서의 충실도(21.2%)' 도 중요한 요인으로 평가 되었다. 선호 패키지별로 살펴보면 'LV2 패키지'를 선호하는 사업체의 경우 '신속한 악성코드 탐지(57.7%)', '포괄적인 악성코드 탐지(26.9%)', '분석 보고서의 충실도(15.4%)'등 순으로 중요도를 평가 하였다. 'LV3 패키지'를 선호하는 사업체의 경우 '신속한 악성코드 탐지(50.0%)', '분석 보고서의 충실도(26.9%)', '포괄적인 악성 코드탐지(23.1%)' 순으로 응답하였다. 방화벽 보유 경험이 있는 사업체를 대상으로 분석한 결과 '신속한 악성코드 탐지(52.9%)'가 가장 중요한 것으로 조사되었다. 따라서 악성코드 분석 서비스 제공시 중요한 부분은 대부분의 사업체에서 공통적으로 악성코드 탐지의 신속성이 가장 중요한 것으로 판단하고 있다.

· 네트워크 통신이상 분석 서비스 제공 시 중요한 부분

네트워크 통신이상 분석 서비스 제공 시 중요한 부분으로는 '신속한 APT 탐지(50.0%)'가 가장 많은 응답을 얻었으며 다음으로는 '분석 보고서의 충실도 (26.9%)', '포괄적인 APT 탐지(23.1%)'등 순으로 나타났다. 아울러, 방화벽 보유 경험이 있는 사업체에서도 '신속한 APT 탐지(41.2%)'가 가장 중요하다고 응답하였으며, '포괄적인 APT 탐지(29.4%)', '분석 보고서의 충실도(29.4%)' 는 동일한 중요도를 보였다.

· 악성 행위 감시를 위한 보안장비 설치 허용 여부

기업에 침해사고를 유발하는 악성 행위를 감시할 수 있는 보안 장비 설치 허용 여부는 '예(66.2%)', '아니오(33.8%)'로 보안 장비 설치에 대해 긍정적인 의견이 더 많이 나타났다. 또한 방화벽 보유 경험이 있는 사업체의 경우 '예(69.2%)', '아니오 (30.8%)'로 조사되어 방화벽 보유 경험이 있는 사업체의 경우 보안 장비 설치에 대해 더 긍정적으로 평가 하고 있는 것으로 조사 되었다.

· 선호하는 보안장비 방식

보안장비 설치 시 중소 사업체에서 선호하는 방식은 '기업 유휴 PC 또는 서버에 S/W설치 방식(58.2%)'이 가장 높게 나타났으며 '상관없음(21.5%)', '전용 H/W 설치(20.3%)' 순으로 나타났다. 반면 방화벽을 보유한 경험이 있는 사업체를 대상으로 결과를 분석 하였을 때 사업체에서 선호하는 보안 장비 설치 방식은 '기업 유휴 PC 또는 서버에 S/W 설치 방식(54.9%)'가 가장 높은

응답률을 보였으며, 그 다음으로는 '전용 H/W 설치 방식(25.5%)', '상관없음(19.6%)' 순으로 나타났다.

· 선호하는 보안장비 설치 위치

중소 사업체의 선호하는 보안장비 설치 위치는 '인터넷 구간에만(45.6%)'을 가장 선호 되는 것으로 나타났으며, 이어 '내부망(34.2%)', '상관없음(20.3%)' 순으로 조사 되었다.방화벽 보유 경험이 있는 사업체만을 대상으로 결과를 분석 하였을 때 보안장비 설치 위치는 '인터넷 구간에만(47.1%)'을 가장 선호되는 것으로 나타났으며 '내부망 (37.3%)', '상관없음(15.7%)' 순으로 나타났다. 선호하는 패키지별로 살펴보면 'LV1 패키지', 'LV2 패키지' 그리고 'LV3 패키지' 모두 '인터넷구간에만' 보안장비를 설치하는 것을 선호하였다.

· 선호하는 보안침해사고 징후 탐지 주기

선호하는 보안침해사고 징후 탐지주기는 '상시(75.9%)'가 가장 높게 나타났으며 그 다음으로는 '주간(15.2%)', '일간(5.1%)', '월간(3.8%)' 순으로 조사되었다. 또한 방화벽을 보유한 경험이 있는 사업체 역시 '상시(82.4%)'를 보안침해사고 징후 탐지 주기로 가장 선호 하는 것으로 나타났다.

· 보안침해사고 징후 포착 시 선호하는 알람 제공 방식

보안침해사고 징후 포착 시 선호하는 알람 제공 방식은 '모니터 화면 내 알림창 제공(50.6%)', '문자 메시지(25.3%)', '이메일(24.1%)' 순으로 조사 되었다. 방화벽 보유 경험이 있는 사업체 역시 '모니터 화면 내 알림창 제공(43.1%)'를 가장 선호하는 것으로 나타났으며, 그 다음으로 '이메일(33.3%)', '문자 메시지(23.5%)' 순으로 나타났다.

· 공익차원에서 장비가 수집하는 정보의 공유 허용 여부

보안장비를 이용 시 공익차원에서 장비가 수집하는 정보의 공유 허용 여부는 '예(37.6%)', '아니오(62.4%)'로 조사 되어 장비가 수집하는 정보의 공유 허용 여부는 부정적인 의견이 더 많은 것으로 나타났다.

4. 결과분석

본 조사를 바탕으로 분석해 본 결과 일반적으로 중소기업들은 정보보호(보안) 정책 및 운영에 적은 자원과 인력을 투입하고 있는 것으로 나타난다. 특히 조사 대상 사업체 중 정보보호전담 조직을 설치, 운영하고 있는 사업체는 절반 이하로 나타났으며, 전담조직을 보유하고 있더라고 평균 3.6명의 매우 적은 인원으로 운영 되고 있다. 또한 중소기업의 보안 시스템의 대다수는 전산 담당자 혹은 내부 직원에 의해서 운영되고 있으며 정보보호 방침 및 지침이 수립된 사업체도 절반 이하에 그쳐 정보보호 (보안)과 관련된 체계성을 기대하기는 어려운 실정이다. 더불어 정보보호(보안) 장비 및 솔루션을 보유하고 있더라도 기초적인 정보보호(장비) 및 솔루션을 이용에 그치고 있는 것으로 조사됐다.

이러한 문제를 해결하기 위해 우리는 본 조사의 몇 가지 결과에 집중해 볼 필요가 있다. 첫 번째로, 고비용의 문제이다. 현재 정보보호(보안) 관련 서비스를 받지 않고 있는 사업체를 대상으로 보안관련 서비스를 받지 않는 이유를 물어 보았을 때 50%이상의 사업체가 투입 되는 비용이 높아 보안관련 서비스를 받지 않는 다고 응답 하였으며 자체 해결이라 응답한 사업체 역시 비용

상의 문제로 인하여 정보보호(보안) 관련 서비스를 받지 못하고 있는 것으로 추정 된다. 또한 현재 정보보호(보안) 관련 서비스를 이용하고 있는 업체들 역시도 현재 받고 있는 서비스의 가장 큰 문제점으로 고비용을 지적하며 비용문제로 인하여 중소기업의 정보보호(보안) 운영이 어렵다는 것을 확인 하였다.

두 번째로, 비록 중소기업이 정보보호(보안) 서비스를 이용하더라도 기대 대비 만족이 낮다는 점이다. 현재 보안 서비스를 받고 있는 사업체를 대상으로 문제점을 조사한 결과 '미비한 보안 개선효과', '취약점 관리능력 부재', '침해사고 분석 능력 부족', '사후조치 미비' 등 현재 보안 서비스의 효과 및 서비스 그 자체에 대해 불만족 하고 있는 실정이다. 이러한 중소기업의 정보보호(보안) 서비스에 대한 불만족 경험은 사업체들이 차후 정보보호(보안) 서비스를 이용하는데 있어 주저하게 만드는 하나의 요인이라 할 수 있다.

하지만, 빅데이터 기반의 사이버 위협 예측분석 서비스 패키지의 선호조사 결과에서 수요없음이 21.6%로 나타난 점을 고려하였을 때 75.0% 이상의 사업체는 정보보호(보안) 서비스에 대한 수요가 있는 것으로 판단되며 이러한 사업체의 수요는 LV1, 2, 3 패키지에 고르게 분포 되어 있어 금액적인 측면에서는 다양한 사업체의 요구를 충족시키고 있는 것으로 판단된다.

또한, 기존의 정보보호(보안) 서비스와는 달리 본 조사에서 파악된 사업체들이 빅데이터 기반의 사이버 위협 예측분석 서비스 패키지에 기대하는 신속한 악성코드 탐지 및 APT 공격 탐지, 보안침해사고 징후 상시 탐지와 같은 점들을 충족시켜 제공한다면 기대 이상의 수요를 중소기업으로부터 이끌어 낼 수 있을 것으로 판단된다. 다만, 보안장비가 수집하는 정보를 공유 하는 것에는 중소 사업체들이 거부감을 지니고 있으므로 사업체들의 반감을 불러 일으키지 않기 위해서 수집된 정보의 공유는 다소 신중하게 이루어질 필요가 있다.

5. 결 론

국내 중소기업의 현실은 정보 통신과 관련된 보안에 있어서 매우 열악한 환경에 처해 있다는 것을 본 조사를 통해 다시 한번 확인할 수 있었다. 기존의 중소기업의 인프라로는 현재 점차 증가되고 있는 사이버 위협에 적절한 대응이 어렵다는 점은 본 조사의 결과를 살펴 보았을 때 파악되는 사실이다. 하지만 합리적인 가격으로 제공되는 서비스패키지에 대해 긍정적인 관심을 보인다는 점, 빅데이터 기반의 사이버 위협 예측분석 서비스 패키지에 대해 구체적으로 바라는 부분들이 파악 되었다는 점들을 고려하였을 때, 빅데이터 기반의 사이버 위협 예측분석 서비스 패키지는 향후 중소 사업체의 충분한 수요를 이끌어 내고 해당 사업체들의 정보보호(보안) 측면에 있어 큰 도움을 줄 수 있을 것으로 기대된다.

저 자 약 력

전 덕 조

이메일 : dejeon@cqvista.com

- 1995년 5월 미국 뉴멕시코주립대(NMSU) 석사
- 1991년 1월~2002년 POSCOICT 기술연구소 팀장/정보보호추진반장
- 2003년 1월~2005년 (주)한매기술 보안사업부문장 / 이사
- 2005년 9월~현재 (주)씨큐비스타 대표이사
- ISO/IEC/JTC1/SC27 정보보안기술 전문 위원회 WG4 그룹장
- SANS Institute GIAC GSEC 한국지역 멘터(Mentor)
- 한국인정원(KAB) ISMS 인정심사원/자문위원
- 관심분야 : 네트워크 보안, 보안관리, 지능형 위협 대응

이 일 주

이메일 : ijlee@tw.ac.kr

- 1988년 2월 아주대학교 전자계산학과 공학사
- 1994년 8월 한양대학교 전자계산학과 공학석사
- 2006년 8월 아주대학교 컴퓨터공학과 공학박사
- 1989년 9월~1998년 1월 현대미디어시스템/현대정보기술 책임
- 2009년~2010년 미국 하와이주립대학교 연구교수
- 1998년 3월~현재 동원대학교 IT융합학부 교수
- 관심분야 : 정보검색, 모바일 프로그램