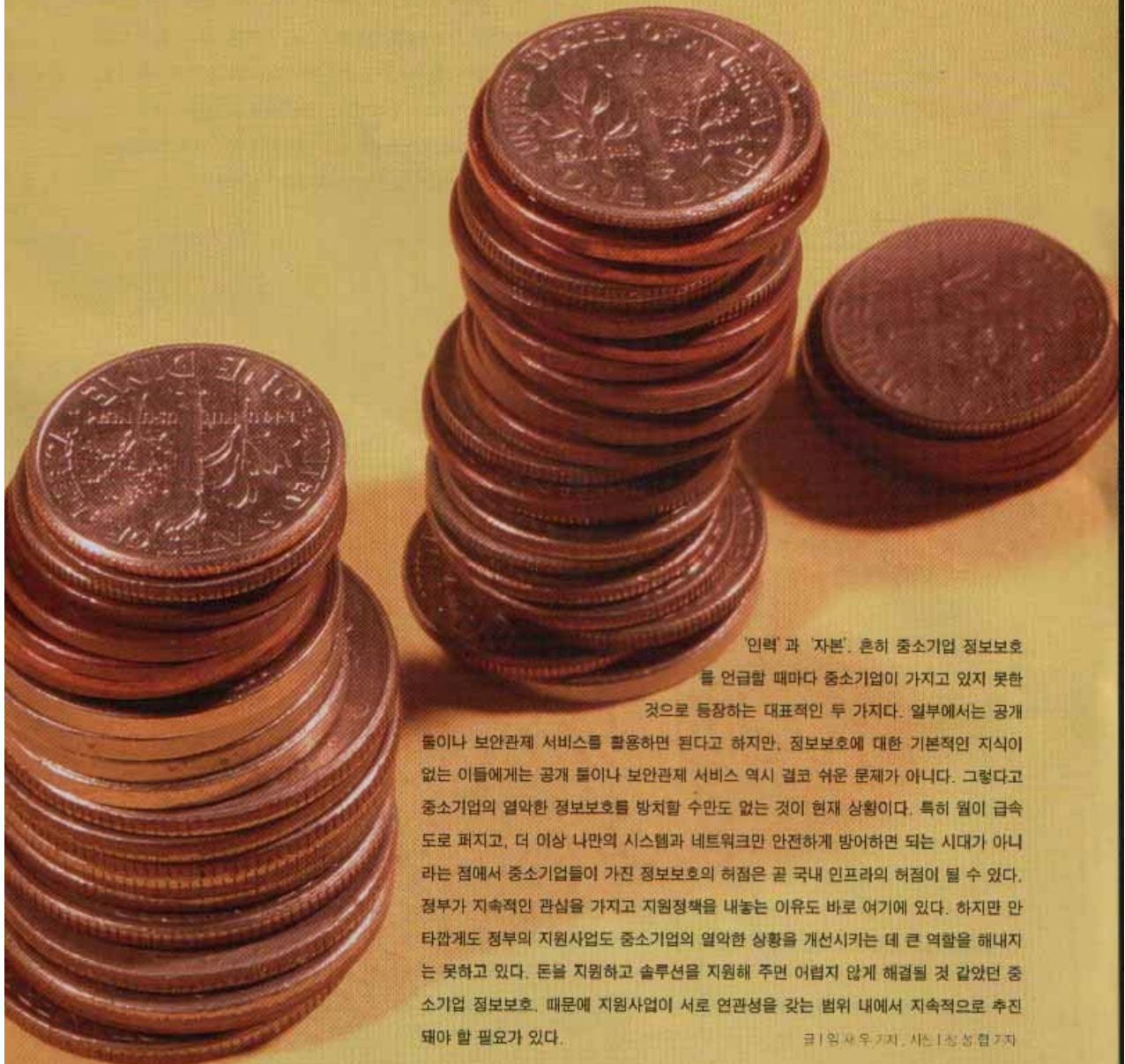


Special Report

잡힐 듯 안 잡히는

중소기업 정보보호를 잡아라



'인력'과 '자본'은 중소기업 정보보호를 언급할 때마다 중소기업이 가지고 있지 못한 것으로 등장하는 대표적인 두 가지다. 일부에서는 공개 데이터나 보안관제 서비스를 활용하면 된다고 하지만, 정보보호에 대한 기본적인 지식이 없는 이들에게는 공개 데이터나 보안관제 서비스 역시 결코 쉬운 문제가 아니다. 그렇다고 중소기업의 열악한 정보보호를 방치할 수만도 없는 것이 현재 상황이다. 특히 월이 급속도로 퍼지고, 더 이상 나만의 시스템과 네트워크만 안전하게 방어하면 되는 시대가 아니라라는 점에서 중소기업들이 가진 정보보호의 허점은 곧 국내 인프라의 허점이 될 수 있다. 정부가 지속적인 관심을 가지고 지원정책을 내놓는 이유도 바로 여기에 있다. 하지만 안타깝게도 정부의 지원사업도 중소기업의 열악한 상황을 개선시키는 데 큰 역할을 해내지는 못하고 있다. 돈을 지원하고 솔루션을 지원해 주면 어렵지 않게 해결될 것 같았던 중소기업 정보보호, 때문에 지원사업이 서로 연관성을 갖는 범위 내에서 지속적으로 추진돼야 할 필요가 있다.

글 | 임재우 기자, 시은 | 장성철 기자

정보보호의 블랙홀, 중소기업을 보호하라

일관성과 지속성 갖춘 지원사업이 필요하다

PC의 보급과 다양한 기업 정보화를 위한 소프트웨어가 제공되면서 중소기업의 정보화 수준도 상당히 높아지고 있다. 지난 3월 기업정보화지원센터가 국내 604개(중소기업 477개사) 기업을 대상으로 2003년 정보화 수준을 측정한 보고서에 따르면, 이들 기업들은 경기침체 등으로 양적인 성장은 소폭 감소된 반면, IT 분야를 활용하는 척도인 정보화 활용계획 등 질적 지표는 상대적으로 높은 수준으로 발전하고 있는 것으로 나타났다. 정보보호가 IT 산업의 발전과 함께 나아간다는 점에서 이제 중소기업의 정보보호는 과거보다도 더 높아진 수준이 요구되고 있는 것이다. 하지만 여전히 국내 중소기업의 정보보호 수준은 기초적인 보안 시스템 도입에 머무르고 있거나, 이마저도 여의치 않다는 것이 전문가들의 한결같은 주장이다.

중소기업 정보보호의 수준은 얼마나

그렇다면 현재 중소기업의 정보보호 수준은 과거에 비해

어제 오늘의 문제는 아니지만, 다시금 중소기업 정보보호에 대한 문제가 제기되고 있다. 이 같은 배경에는 지난해부터 중소기업 정보보호 지원사업이 산업자원부와 정보통신부를 중심으로 의욕적으로 진행되고, 이를 뒷받침하듯 정보보호 업계들도 중소기업을 대상으로 한 제품들을 출시하고 있는 것도 하나의 배경이라고 볼 수 있다. 하지만 지원사업을 추진하고 있는 정부나, 중소기업용 보안 솔루션을 출시한 업계가 아직까지 이렇다 할 성과를 내놓지는 못하고 있다. 많은 전문가들은 그 이유에 대해 중소기업에 대한 명확한 실효성과 없이 단지 중소기업이라는 이름만으로 접근했기 때문이라고 지적하고 있다.

얼마나 나아졌을까, 중소기업 정보보호에 대한 현황 파악이 아직 미흡한 수준에 머물러 있고, 또 이에 대한 축적된 자료를 찾기 어렵다는 한계로, 현 상황에서 중소기업의 정보보호 수준이 어떻게 변화하고 있는지 파악하기는 어려운 문제다. 다만, 지난 2002년 10월 본지에서 중소기업진흥공단과 함께 100개 중소기업을 대상으로 실시했던 '중소기업 정보보호 실태조사'와 지난 2003년 중소기업정보화경영원이 실시한 '중소기업 정보화역기능 실태조사'를 비교해 본다면 국내 중소기업의 정보보호가 어떤 방향으로 흘러가고 있는지 간접적으로 느낄 수 있다.

표 1, 2는 본지와 중소기업정보화경영원이 각각 중소기업을 대상으로 실시했던 설문 중 정보보호 지침 보유현황에 대한 설문조사 결과로, 1년간 그 실태가 크게 변화되지 않았음을 알 수 있다. 특히, 정보보호 지침이 실제로 시행되고 있는 비율은 2년 전이나 지난해나 20% 내외에 머물고 있으며, IT 자산에 대한 보안지침 역시 큰 변화를 느낄 수 없다. 물론 1,261명을 표본으로 삼은 경영원의 설문조사와 100명

표 1. 정보보호21c 설문조사 결과(2002년 10월)

	있다	없다	준비 중
전산 시스템 및 네트워크에 대한 보안관리규정 보유여부	22%	38%	40%
해킹을 비롯한 침해사고가 발생했을 경우, 제지 불가능할 수 있는 규정의 보유여부	10%	62%	28%

표 2. 중소기업정보보호경영원 설문조사 결과(2003년 10월)

	수립해 시행 중	현재 수립 중	1~2년 내 수립 예정	이직 수립할 계획 없음
정보보호 지침 수립현황	16%	17%	24%	43%

표 3. 2003년 기업별 정보보호 시스템 운영현황(출처: 기업정보화지원센터)

	조사기업 수	침입차단 시스템	침입탐지 시스템	VPN	안티 바이러스	없음
중소기업	477개	41.9%	12.6%	18.2%	55.8%	21.8%
대기업	127개	88.2%	48%	75.5%	80.3%	4%

을 대상으로 했던 본지의 설문조사는 절대수치상에서 큰 차이를 보여 직접적인 비교에는 한계가 있지만, 중소기업 정보보호에 대한 단편적인 흐름을 반영하고 있다고 볼 수 있다. 이 같은 흐름은 2003년 중소기업 정보보호 솔루션 도입사례에서도 나타나고 있다. 표 3은 지난 3월 기업정보화지원센터가 중소기업과 대기업을 포함해 약 604개사를 대상으로 실시한 기업정보화수준평가 보고서에서 집계한 것으로, 이 보고서에 따르면 정보보호를 위한 어떤 보안 솔루션도 도입하지 않은 중소기업이 무려 20%가 넘게 나타나고 있으며, 정보보호에 가장 기본이라고 불리는 안티 바이러스의 도입도 50%를 간신히 넘기는 수준을 보이고 있어, 정보보호에 대해 기초적인 수준을 크게 벗어나고 있지 않음을 알 수 있다.

정부 지원사업은 계속 되는데...

물론 정부가 이처럼 나후된 중소기업 정보보호 상황을 방관만 하고 있는 것은 아니다. 한국정보보호진흥원이나 중소기업청 등이 실시하는 무료 취약점 분석 서비스나, 정보보호 컨설팅 지원사업 등 중소기업만을 위한 지원사업이 전개되고 있다.

하지만 이런 정부 지원사업도 높은 성과를 거두지는 못하고 있다. 중소기업 정보보호가 인력과 자금 면에서 상당히 어려운 상황이라는 점을 감안해 보면, 이 같은 정부의 지원사업이 성과를 거두지 못한다는 사실은 상당히 납득하기 어려운 부분이기도 하다. 이에 대해 정보보호 업체와 한 관계자는 "중소기업

에 대한 지원사업이 이뤄지고 있지만 정작 중소기업의 실태를 파악할 수 없는 상황이며, 실태파악이 어렵기 때문에 지원사업이 어떻게 진행되어야 하는지 방향을 잡기가 어려울 것"이라는 분석을 내놓았다. 즉, 구체적인 대상을 미처 파악하지 못한 상황에서 지원사업에 대한 생각이 앞섰다는 것이다. 중소기업 솔루션을 전문적으로 출시하고 있는 한 업체 관계자도 "정보부나 산자부가 이런 상황을 제대로 인식하지 못하고 있어, 이벤트 중심의 사업보다는 향후에 발생될 중소기업 지원사업 방향에 도움이 될 수 있는 사업을 준비해야 한다"고 강조했다.

2004년 시행될 중소기업 정보보호 지원사업

- 중소기업 정보보호 봉사단 : 한국정보보호진흥원과 대한상공회의소가 MOU를 맺고 중소기업 정보보호에 대한 무료점검과 실무자 대상 정보보호 교육을 실시하게 된다. 특히, 이번 사업은 지난 2003년까지 KISA가 정보보호 동아리 지원사업'을 통해 지원했던 전국의 동아리를 활용해 직접 중소기업을 방문, 실태 조사를 경험 것으로 알려져 있어 관심을 끌고 있다.
- 정보보호 지원사업 : 중소기업정보보호경영원이 실시하는 정보보호지원사업은 기업의 전산 시스템을 물리적·관리적 차원에서 진단하고 발견된 취약점에 대해 긴급조치나 대처법, 정보보호 가이드라인 등을 제시해 주는 사업으로, 한 기업당 지원금액은 컨설팅 비용의 80%, 최대 275만원까지 지원하고 있으며, 올해에는 약 50여개 기업을 지원할 계획인 것으로 알려져 있다.

업계도 갈광질광

상황이 이렇다보니, 정작 중소기업을 대상으로 활발한 솔루션 판매에 열을 올려야 할 정보보호 업체들도 갈피를 못 잡기는 마찬가지다. 최근 업계가 활발하게 중소기업용 정보보호 솔루션을 내놓고 있기는 하지만 제품만 출시하고 있을 뿐, 아직 구체적인 마케팅 전략도 잡지 못하고 있는 기업도 많다는 얘기가 들리는 것도 이와 무관하지 않다. 특히, 이런 분위기는 올해 초까지만 해도 침체된 정보보호 시장에서 새로운 시장으로 중소기업 시장이 떠오를 것으로 예상했던 업계의 고무적인 분위기와는 사뭇 상반된 상황이다.

"도대체 어떤 중소기업이 보안 솔루션을 도입한 것인지, 또 이들이 원하는 솔루션이 무엇인지 모르겠다"고 밝힌 한 보안업체 관계자는 "이제는 과연 중소기업들에게도 정보보호 솔루션이 필요할까라는 의문까지 든다"고 중소기업 시장에 대해 회의

중소기업과 채널 마케팅

최근 국내외 보안업체가 중소기업용 보안 솔루션에 집중하고 있는 가운데, 중소기업 시장에서도 외국 벤더와 국내 업체들 간의 치열한 경쟁이 시작될 것으로 보인다. 그렇다면 현재 국내 중소기업 시장에서 우세를 보이는 쪽은 어디일까. 대부분의 관계자들은 외산 벤더가 조금 더 낫다고 한다. 그 이유는 다양한 채널 마케팅을 통해 중소기업 시장을 공략하고 있기 때문. 비록 국내 업체가 대형 프로젝트 사업에서는 비교적 좋은 성과를 거두고 있기는 하지만, 국내 업체라는 점으로 인해 오히려 채널 마케팅이 상대적으로 미흡하다는 얘기가.

적인 목소리를 내기도 했다. 어차피 정보보호를 위해서 솔루션 도입이 기본 바탕이 되어야 한다는 사실을 감안하면, 업계의 이같은 분위기는 중소기업의 정보보호가 얼마나 심각한지를 반증하는 셈이다.

연속성 가지고 꾸준히

정부도 업계도 이처럼 진전을 보이지 못하고 있는 상황이지만, 정보보호의 사각지대로 남겨놓을 수도 또, 더 늦출 수만도 없는 것이 중소기업 정보보호다. 그렇다면 무엇인가 반전을 노릴 만한 정부지원이나, 업계의 시장확대가 필요한 시기라고 볼 수 있다. 그러나 앞서 살펴봐왔듯, 중소기업 정보보호는 단편적인 이벤트가 아닌 지속적인 지원과 관심, 그리고 정부가 추진하는 다양한 지원사업이 서로 연속성을 가져야 한다. 중소기업청의 중소기업역기능방식센터 운영이나 정보통신부가 추진했던 중소기업 정보보호 지원사업들이 모두 본래의 의도와 달리 뚜렷한 성과를 거두지 못한 것도 했던 것도, 사업의 연속성이나 일관성을 가지지 못했기 때문이라고 볼 수 있다. "올 초 의욕적으로 정보보호 서비스 프로젝트를 기획했지만, 담당 공무원의 자리이동으로 유야무야 되고 있다"며 아쉬움을 토로한 한 보안업체 관계자의 주장도 어쩌면 이런 배경에서 등장한 것 이라고 볼 수 있다.

이런 의미에서 지난해 급진전을 보이다 한동안 논의대상에서 제외됐던 기업 정보보호 지원센터에 대한 재논의를 생각해 볼 수도 있다. 물론 중소기업 정보보호만을 위한 기관을 별도로 설립한다는 자체가 쉬운 일은 아니지만, 이런 기관을 통해 지원사업을 단일화하고 연속성을 가져야 한다는 주장도 의미 있다고 볼 수 있다.

대부분의 전문가들은 우리나라가 추진해 왔던 IT 산업 중 가

IT렌탈산업협회

지난 2004년 3월 창립총회를 갖고 본격 출범한 IT렌탈산업협회 (<http://www.kitria.or.kr>)는 IT 자산을 단순히 구매 소유하는 개념이 아닌 임대방식을 활용함으로써, 기업 사용자들에게는 최신의, 그리고 필수 장비를 저렴한 가격으로 제공한다는 목적에서 등장했다. 비용부담으로 인해 시스템 도입을 꺼리는 중소기업을 대상으로 IT 전반에 대한 모든 장비임대가능 것으로 보이며, 특히, 고가의 정보보호 솔루션에 대해서도 렌탈서비스가 이뤄질 것으로 보인다. 다만 아직까지는 협회가 제 모습을 찾아가는 단계로, 구체적인 렌탈 사업계획의 등장은 빨리도 율 허받기가 되어야 할 것으로 보인다.

해외 중소기업 정보보호 지원

- 영국 : 무역산업국을 통해 지난 1991년부터 2년마다 보안침해사고에 대한 조사를 실시하고 있다. 직원 수에 따라 소기업(50인 미만), 중기업(50~249), 대기업(250 이상)으로 구분해, 각 기업에 적합한 가이드라인을 홈페이지를 통해 제공하고 있다.
- 독일 : 중소기업을 위한 CERT 'BITKOM-CERT'를 중심으로 중소기업에 새로운 위협과 대응방법 등 IT 보안에 대한 최신정보를 제공하는 한편, 비상시 지원 서비스를 시행하고 있으며, 자체예산을 확보해 독립적으로 운영하고 있다.
- 미국 : NIST(National Institute of Standards and Technology)와 소기업청, 그리고 미국 국토안보국이 함께 중소기업 정보보호를 지원하고 있다. 이들 각 기관은 보안진단 프로그램을 제공하거나, 온라인 정보보호 교육, 중소기업 정보보호 전략수립 등의 역할을 분담해 중소기업의 정보보호를 강화하고 있다.

장 성공적인 사례로 휴대폰과 초고속 인터넷 보급을 주저 없이 꼽는다. 보조금제도를 만들어 휴대폰의 대중화에 기여했고, 곳곳에 인터넷 망을 연결해 유저들의 관심을 불러일으켰다. 물론 다른 성격의 문제일 수 있지만 어차피 이들 사업을 추진할 초기에도 많은 사람들은 휴대폰이 무엇인지, 그리고 초고속이 인터넷 망이 무엇인지 잘 몰랐을 것이다. 또한 이렇게 빠르게, 또 이렇게 많은 사람들이 사용하게 될지는 디디욱 예상하지 못했을 것이다. 그렇다면 이런 성공적인 사업배경에는 무엇이 있었는지를 한번쯤 되돌아 볼 필요가 있지 않을까.

제품을 구매해볼까, 서비스를 받아볼까

중소기업을 이해하는 보안 솔루션 & 서비스

중소기업이 정보보호를 실시하기 어려운 배경에는 여러 가지 문제점들이 있을 수 있다. 그러나 이런 문제들을 겁안한다고 해도 중소기업 역시 정보보호의 예외지역이 될 수 없다는 사실은 분명하다. 때문에 중소기업이 가진 무수히 많은 문제점들을 이해(?)해 줄 수 있는 중소기업만을 위한 정보보호 서비스나 제품이 필요한 것이다. 하지만 본격적으로 중소기업을 겨냥한 제품들이 출시되고 있는 최근에도, 이들 서비스나 제품을 구매할 당사자인 중소기업들은 이들 제품이나 서비스를 생소하게 생각하는 것이 현실이다.

지난해, 그리고 올해 초부터 정부가 중소기업 정보보호에 대한 관심에 눈을 돌리면서 다양한 사업을 전개할 움직임을 보이자, 정보보호 업계 역시 기존 하이엔드 중심의 보안 솔루션에서 탈피, 중소기업용 겨냥한 보안 솔루션을 출시하고 있다. 이런 움직임은 정보보호 업계뿐만 아니라, 대형 침해사고를 몇 차례 경험했던 ISP도 마찬가지다. 비록 국내에서는 보안 관제 서비스라는 정보보호 서비스가 엄연히 존재하지만, 이마저 비용문제로 고민하는 중소기업들을 겨냥해, 대형 ISP들이 월 몇 만원 규모의 보안 서비스를 실시하고 있다.

이렇게 서비스와 제품들이 중소기업용 타깃으로 출시되고 있지만, 정작 이들 중소기업용 제품이나 서비스가 어떤 기준에서 중소기업용 제품과 서비스라고 불리고 있는지, 어떤 기능들을 가지고 있는지, 또 각 제품의 차이는 무엇인지에 대해서는 명확한 설명이 부족한 상황이다. 그런 의미에서 중소기업용 제품의 특징은 무엇이고 또 어떤 기능을 필수적으로 제공해야 하는지 살펴볼 필요가 있다.

'통합', '가격', 그리고 '편리성'

중소기업용 보안 솔루션의 최근 추세는 하이엔드 제품과 동일한 통합형 모델이다. 다만 하이엔드의 통합화는 기본적으로 관리의 편의성에서 출발한 것인 반면, 중소기업용 통합제품은 침입차단 시스템, VPN, 침입탐지 시스템, IPS 그리고 백신 등 다양한 단위 보안 솔루션을 모두 구매할 수 없는 중소기업의 한계를 보완하기 위한 것이라고 볼 수 있다. 또한 여기에 이들 솔루션을 관리할 수 있는 관리자가 부재한 점을 고려해 간결한 인터페이스를 유지하기 위해서도 통합화는 반드시 필요한 요소라고 볼 수 있다.

한편, 중소기업용 제품이라고 불리기 위해서는 가격이 가장 큰 문제로 작용하게 된다. 현재 중소기업용이라고 명명된 제품들은 대부분 1,000만원 이하의 가격대를 보이고 있다. 일반적으로 중소기업용 보안 솔루션이 하이엔드 제품과 비교해 볼 때 기능상의 차이는 크지 않지만 가격은 월등히 낮아지는데, 이는 성능이 낮기 때문이라고 볼 수 있다. 대형

제품에서부터 중소기업 제품을 모두 갖춘 한 업체 관계자는 "중소기업용 보안 솔루션을 규정짓는다고 해도, 이들 솔루션이 기능적인 측면에서 하이엔드 제품과 달라지는 것이 아니라 유지 수 등을 고려한 성능적인 요소와 그에 따른 가격"이라며, 중소기업용 통합보안 솔루션의 특징을 설명한다.

“△△기능 왜 필요하죠?”

하지만 통합과 가격, 그리고 관리의 편의성을 중소기업용 보안 솔루션의 특징으로 규정해 본다. 통합의 구체적인 기능에 대한 기준도 논란의 대상이 될 수 있다. 물론, 기본적으로 대기업이든 중소기업이든 동일한 위협요소에 직면하고 있고, 또 정보보호 솔루션을 통해 보안을 수행하는 절차가 크게 달라질 수는 없다. 그럼에도 불구하고 중소기업용 보안 솔루션의 기능을 규정지어야 하는 이유는 투자비용이 제한적인 중소기업의 상황을 감안해 볼 때, 필요이상의 기능은 비용의 부담으로 이어질 수 있고, 또 사용의 편의성을 해칠 수 있기 때문이다. 이런 의미에서 전문가들은 침입차단 시스템과 VPN, 그리고 침입차단 시스템의 문제를 보완해 줄 수 있는 IPS나 콘텐츠 필터링, 안티 바이러스 등의 기능은 반드시 탑재되어야 할 기능이라고 입을 모은다. 과거 중소기업용 정보보호 솔루션에 대한 시장조사를 실시한 적이 있었다고 밝힌 한국정보보호진흥원 취약점 분석팀 허창렬 팀장은 "당시에도 업체마다 다양한 기능을 가지고 있어, 중소기업에 꼭 필요한 기능을 일반화시키는데 어려움을 겪었다"며, "현재의 공격유형과 특징을 고려해 볼 때, 다양한 기능 중에서도 내부 네트워크의 대문 역할을 하는 침입차단 시스템과 통신보안을 위한 VPN이 필요하며, 여기에 IPS나 콘텐츠 필터링, 안티 바이러스처럼 침입차단 시스템이 미처 차단해 주지 못하는 유해 트래픽을 차단하고 치료해주는 기능이 포함되어야 할 것"이라고 밝혔다.

침입차단 시스템

침입차단 시스템의 올바른 적용만으로 모든 공격을 막을 수 있다고 주장하는 것처럼, 침입차단 시스템은 정보보호의 기본적인 요소라고 볼 수 있다. 가정의 대문 역할을 하는 침입차단 시스템은 기업 내부 네트워크로 들어오는 불필요한 트래픽이나 침입시도를 기본적으로 차단할 수 있으며, 정보보호 뿐만 아니라 효율적인 네트워크 사용을 위해서도 반드시 필요한 솔루션이라고 볼 수 있다.

VPN

최근 대부분의 침입차단 시스템과 통합돼 등장하는 VPN은

작은 규모의 기업들에게는 상대적으로 필요성이 반감될 수 있지만, 중소기업 직원들의 규모가 급변할 수 있고 또 지사와의 통신을 위해서 반드시 필요한 기능으로 분류할 수 있다. 특히, 최근에는 단지 사무실에 앉아서만 업무를 보는 것이 아니라, 외부에서 혹은 각 가정에서 기업의 네트워크를 접속하는 상황이 빈번하게 발생함에 따라 안전한 접속을 보장하는 VPN을 제외시킬 수는 없을 것으로 보인다.

안티 바이러스 혹은 IPS 기능

침입차단 시스템이나 VPN의 경우, 정보보호를 위한 가장 기본적인 보안 솔루션들이라고 볼 수 있지만, 여기에 안티 바이러스나 IPS 혹은 콘텐츠 필터링 기능은 최근의 등장하는 워딩의 특징으로 인해 필요해진 기능이다. 특히, 침입차단 시스템이 가질 수 있는 문제가 열려 있는 포트로 유입되는 웜이나 바이러스에 대해서는 한계를 드러내고 있기 때문에, 이를 보완할 수 있는 기능의 솔루션들이 필요하다는 것이다. 일부 중소기업용 통합보안 솔루션들 중에는 웜이 스팸메일을 통해 유입된다는 점에 착안, 스팸메일 차단기능으로 이들 기능을 대신하는 경우도 있다.

보안기능 및 사용자 증감에 따른 장비 업데이트

필수기능이라고 보기에 모호하지만, 보안기능의 업데이트와 사용자 증감에 따른 장비의 업데이트는 적시이러야 보충한 중소기업용 보안 솔루션에 있어서는 상당히 중요한 문제라고 볼 수 있다. 특히, 보안을 전담하거나 정보보호에 대해 잘 알고 있는 담당자가 없다는 점에서, 보안업체가 제공하는 지속적인 업데이트는 필수적이다. 또한 정기적인 점검 서비스라든지, 중소기업이 차라이동이 빈번하다는 점을 고려해 사용자 수의 증감에 따라 신속한 장비의 업그레이드도 반드시 뒤따라야 한다.

정보보호 서비스도 있다

중소기업이 정보보호를 하는데 있어 제품구매만이 유일한 방법은 아니다. 보다 효율적이고 전문적인 정보보호를 위해 정보보호 관제 서비스를 받듯, 이들 중소기업도 정보보호 서비스를 고려해 볼 수 있다. 현재 저가의 정보보호 서비스는 데이콤과 KT를 중심으로 제공되고 있으며, 그 서비스 방법은 저가의 통합보안 솔루션을 임대해 이 솔루션을 관리해 주는 방식을 취하고 있다. 한편, 회선 사용자들을 대상으로 제공되는 정보보호 서비스도 등장하고 있는데, 데이콤 CADNET(Cyber Attack Defense Network) 서비스가 이 경우에 해당된다.

이들 정보보호 서비스는 월별로 일정한 금액만을 지불하면

비교적 높은 수준의 보안을 유지할 수 있을 뿐만 아니라, 별도의 장비관리나 담당자가 필요하지 않아, 중소기업들에게는 오래전부터 유용하게 적용된 모델로 간주돼 왔다. 하지만 이들 서비스가 아직 초기단계라는 점 때문에 판단하기에는 이른 감이 있지만, 보안 서비스가 중소기업들에게 보다 각광받기 위해서는 현재처럼 단순히 유저 수에 의한 서비스 구분보다는 정보 보호 서비스 항목을 보다 세분화하고 상품화할 필요가 있다고 전문가들은 지적하고 있다.

중소기업 통합보안 솔루션 및 서비스(가나다 순)

네트워크 박스 「SOHO-200」



<http://www.network-box.co.kr>

- 통합된 기능 : 침입차단 시스템, VPN, 인터 바이러스 게이트웨이, 인터스팸 게이트웨이, IPS, 콘텐츠 필터링
- 침입차단 시스템 최대 성능 : 190Mbps
- 보안기능 업데이트 : 전세계 네트워크 박스를 사용하는 모든 고객에게 하루 12번씩 동일 시간에 보안 시그니처 자동 업데이트
- 사용자 증감에 따른 업그레이드 : 유지보수기간 내 무상으로 기교체가 가능하며, 서비스와 기능의 추가 업그레이드는 실시간으로 가능
- 제품 유지보수 지원체계 및 제품 점검방법 : 네트워크 박스 한국 관제센터를 통해 관리기능을 제공하며, 서비스 상태에서부터 CPU 및 메모리 등 하드웨어 상태까지 일괄적인 관리 가능
- 주요 특징 : 중소기업들 중심으로 전세계 공급이 이뤄지고 있는 네트워크 박스 「SOHO-200」의 가장 큰 특징은 제품구매와 서비스가 동시에 이뤄져 일거양득의 효과가 있다는 점이다. 각국의 지사별로 별도의 관제센터를 운영해 고객에게 제품관리를 비롯해 보안기능 업데이트, 그리고 별도의 유지보수가 함께 제공된다.

또한, 1년에 한 차례씩 중소기업의 취약점 분석 및 컨설팅 서비스를 실시해 해당 중소기업이 지속적인 정보보호에 대한 지속적인 관심을 가질 수 있도록 유도하고 있다. 한편, 신선(?)한 보안성을 유지하기 위해 각종 시그니처 업데이트를 하루 12번씩 강제로 실시해 준다.

소닉월 「PRO 2040」



<http://www.sonicwall.co.kr>

- 통합된 기능 : 침입차단 시스템, VPN, 콘텐츠 필터링, IPS, 인터 바이러스
- 침입차단 시스템 최대 성능 : 200Mbps
- 보안기능 업데이트 : 자체 DB를 통해 자동 업데이트 가능
- 사용자 증감에 따른 업그레이드 : 일반적인 사용자 증가시 라이선스 노드 수에 맞게 업그레이드 가능
- 제품 유지보수 지원체계 및 제품 점검방법 : 1차적으로 웹 상의 원격접속을 통해 관리가 가능하며, 방문을 통해 하드웨어 상태 확인, 네트워크 구성 이상 유무확인 등을 실시한다.
- 주요 특징 : 현재까지 약 500,000개 이상의 장비가 설치돼, 안정성에서 높은 점수를 받고 있는 소닉월의 소호용 제품 「PRO 2040」은 별도의 보안 관리자가 없는 기업의 경우에도 관리 및 사용이 용이한 보안 솔루션으로 알려져 있다. 특히, 기본적인 통합기능 뿐만 아니라, 소닉월 OS를 통해 로드밸런싱, Fail-Over, VPN, 세컨드리 터널 및 Input/Output에 대한 QoS 등 강력한 네트워크 관리기능이 포함돼 있다는 점이 특징이다.

시큐어소프트 「수호신 Absolute 100」



<http://www.securesoft.com>

- 통합된 기능 : 침입차단 시스템, 침입탐지 시스템, VPN, 인터 바이러스, URL 필터링, PKI
- 침입차단 시스템 최대 성능 : 200Mbps
- 보안기능 업데이트 : 웹을 통한 패던 및 백신 자동 업데이트
- 사용자 증감에 따른 업그레이드 : 제품 라인업이 성능에 따라 구상돼 있으며, 사용자의 증가로 트래픽 용량이 증가될 경우, 그에

따른 상위제품 교체가 가능

• **제품 유지보수 지원체계 및 제품 점검방법** : 원격지 서비스를 통한 지속적인 점검은 물론 정기적인 방문점검을 통해 기술지원이 가능, 별도의 콜 센터 운영

• **주요 특징** : 중소기업용 솔루션으로는 비교적 오래전 출시됐던 시큐어소프트 「수호신 Absolute 100」은 최대 36,000개의 보안정책 적용이 가능하며, 침입탐지 시스템과의 연동을 통해 보안정책 클이 즉시 적용된다. 특히, 백신 전문업체와의 제휴를 통해 Http, SMTP, FTP 등 다양한 프로토콜을 검사해 이를 통해 유입되는 바이러스를 차단할 수 있다. 또한 로드밸런싱이 가능하며, 사내 시스템이나 네트워크 관리 시스템과의 연동이 가능하다. 이밖에도 직관적인 인터페이스를 통해 보안정책의 검색 및 조회시간이 짧다는 점도 장점이다.

워치가드 테크놀러지스 「Firebox X」



<http://www.watchguard.co.kr>

• **통합된 기능** : 침입차단 시스템, VPN, 침입탐지 시스템, IPS, 스팸차단, 애플리케이션 공격, 유해 사이트 차단, 취약점 분석

• **침입차단 시스템 최대 성능** : 275Mbps

• **보안기능 업데이트** : 워치가드 테크놀러지스 Live Security Service 팀을 통해 실시간 업데이트가 가능하며, 바이러스 패턴, 침입탐지 시스템 패턴 자동 업데이트

• **사용자 증감에 따른 업그레이드** : 장비교체 없이 기존 하드웨어 플랫폼에 소프트웨어 라이선스 키만으로 최고 25배까지 성능 업그레이드 가능

• **제품 유지보수 지원체계 및 제품 점검방법** : 각 채널을 통한 지원과 웹을 통한 원격관리, 1년간 무상교체 및 업그레이드 가능

• **주요 특징** : 오래전부터 중소기업용 통합보안 솔루션을 출시해 온 워치가드 테크놀러지스의 「Firebox X」는 확장 가능한 하드웨어 플랫폼을 독자 개발, 라이선스 키만으로 모델의 성능, 기능, 서비스를 최대 25배까지 업그레이드 할 수 있다는 점이다. 때문에 중소기업의 다양한 직원 수 변화에도 유연한 대처가 가능하며, 지능형 계층보안(Intelligent Layered Security) 엔진

을 탑재해 새로운 위협에 대한 실시간 탐지율과 전송처리 성능을 보여주고 있다. 이밖에도 최적의 TCO 체계를 제공해 비용절감효과를 동시에 얻을 수 있다는 것도 빼놓을 수 없는 특징이다.

주니퍼 네트워크스 「NetScreen-5GT/5XT」



<http://www.kr.juniper.net>

• **통합된 기능** : 침입차단 시스템, VPN, IPS 기능, 백신

• **침입차단 시스템 최대 성능** : 75Mbps

• **보안기능 업데이트** : 온라인 업데이트 가능

• **사용자 증감에 따른 업그레이드** : 소프트웨어 라이선스 통한 업그레이드

• **제품 유지보수 지원체계 및 제품 점검방법** : 주니퍼의 TAC/SE와 국내 파트너사의 NASC(NetScreen Authorized Support Center)를 통해 24시간 365일 지원 가능

• **주요 특징** : 얼마 전 주니퍼 네트워크스로 합병된 넷스크린 「NetScreen-5GT/5XT」는 ADSL 서비스를 사용하는 지사 사무실에서 필요로 하는 다양한 기능을 하나의 편리한 플랫폼에서 제공한다는 점이 가장 큰 특징이다. ADSL 인터페이스 및 WAN 라우팅과 함께, 딥 인스펙션, IPSec VPN, DoS 방어, 안티 바이러스 등 다양한 보안기능을 통합 제공할 수 있다. 특히, 제품 설치시 외장형 ADSL 모듈이 필요하지 않아 분사와 떨어진 지사 사무실의 보안을 강화시킬 수 있다는 점이 눈에 띈다. 이밖에도 보안과 ADSL 모듈의 통합으로 하드웨어 비용이 절감될 수 있다는 것도 빼놓을 수 없는 장점이다.

포티넷 「Fortigate-60」



<http://www.fortinet.co.kr>

- **통합된 기능** : 침입차단 시스템, VPN, 안티 바이러스, 침입탐지 시스템, 스팸메일 차단, 유해 사이트 차단, QoS, 웹 필터링
- **침입차단 시스템 최대 성능** : 70Mbps
- **보안기능 업데이트** : 사용자 설정에 의한 자동 업데이트
- **사용자 증감에 따른 업그레이드** : 별도의 사용자를 제한하지 않고 있어 사용자 수에 관계없이 사용할 수 있으며, 필요에 따라 상위 제품으로 장비교체 가능
- **제품 유지보수 지원체계 및 제품 점검방법** : 24시간 원격에서 장비 모니터링이 가능해 장애발생시 서울 지역의 경우 4시간 이내 처리 가능
- **주요 특징** : ASIC 기반의 통합보안 기능을 제공하는 포티넷 'Fortigate-60'은 이미 KT나 테이콤의 정보보호 서비스에 이용될 만큼 속도와 안정성에서 검증된 점이 장점으로, 펌웨어 업그레이드만으로 새로운 기능을 추가할 수 있어 새로운 보안위협에 대해 유연한 대처가 가능하다. 또한 한 장비 내에서 백신, IPSec, 침입탐지, 침입차단 기능에 대한 ICSA 인증을 모두 획득했다는 점이 눈에 띈다. 10Mbps~10GB까지 다양한 네트워크 환경에 적용할 수 있는 제품 라인업을 갖춰 국내에서도 다양한 고객층을 확보하고 있는 것으로 알려져 있다.

퓨처시스템, 「이지락」



<http://www.future.co.kr>

- **통합된 기능** : 침입차단 시스템, 바이러스 및 스팸 차단, 유해 사이트 차단, 온라인 프로그램 제한, IP 공유
- **침입차단 시스템 최대 성능** : 100Mbps
- **보안기능 업데이트** : 바이러스 엔진 및 패턴 업데이트가 가능하며, 정보통신위원회 유해 사이트 DB 등을 활용해 웹을 이용한 업데이트가 가능하다.
- **사용자 증감에 따른 업그레이드** : 최대 50인 이하의 기업 내에서 사용이 가능하며, 추가적인 업그레이드가 필요할 경우 퓨처시스템 통합 게이트웨이 제품군과 교체 가능
- **제품 유지보수 지원체계 및 제품 점검방법** : 서비스 센터를 통해 모니터링할 수 있으며, 이지락에 걸린 메시지를 주기적으로 보

내 장애여부를 점검

- **주요 특징** : 퓨처시스템의 중소기업용 통합보안 제품 「이지락」은 여기에 소개된 통합장비들 중 가장 저렴한 가격대의 통합보안 솔루션이다. 50인 미만의 중소기업에 특화된 솔루션으로, 중소기업에 필요한 다양한 기능과 업데이트를 제공하며, 온라인을 통해 사용자 간편하게 장비설정을 제어할 수 있고, 별도의 통계 리포트를 살펴볼 수 있다. 또한 펌웨어를 통해 바이러스 패턴 등을 업데이트할 수 있으며, 데이터백업의 제휴를 통해 저렴한 정보 보호 서비스를 위한 임대장비로도 활용될 것으로 보인다.

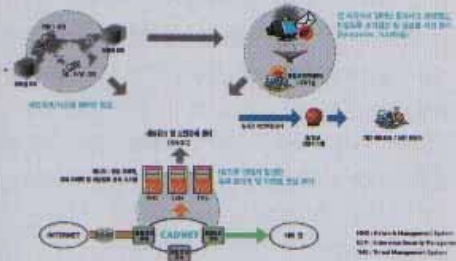
한인터넷 « HanWall-Pro(HWP-1000) »



<http://www.haninternet.co.kr>

- **통합된 기능** : 침입차단 시스템, 침입탐지 시스템, 스팸 필터, 바이러스 메일 필터, VPN, QoS
- **침입차단 시스템 최대 성능** : 105Mbps
- **보안기능 업데이트** : 다운로드 패치가 가능하며, 각 라이브러리는 실시간 온라인 업데이트 제공
- **사용자 증감에 따른 업그레이드** : 사용자가 밀집수준 이상의 증가를 원할 경우, 하드웨어 교체 가능
- **제품 유지보수 지원체계 및 제품 점검방법** : 보안문제 센터를 통해 모니터링 서비스와 실시간 라이브러리 업데이트가 가능하며, 라이브러리 업데이트는 모든 솔루션에 한해 1년간 무상 제공
- **주요 특징** : 침입차단 시스템 VPN, 스팸메일 및 바이러스 메일 필터를 하나의 어플라이언스로 통합한 한인터넷 « HanWall-Pro »은 개발 초기부터 중소기업시장을 겨냥했기 때문에 관리 및 제품구성이 간편한 것으로 알려져 있다. 특히, 메신저, 증권 등 무분별한 웹 사이트 및 서비스 이용을 관리자가 시간대별로 제어할 수 있는 Site QuickWall 기능과 원과 관련된 스팸과 바이러스 메일을 걸러내는 Mail QuickWall 기능이 눈에 띈다. 한편, 단말장치들에 적용될 보안대상을 중앙 서버로부터 다운로드 받아 적용하기 때문에 전문인력 없이도 손쉬운 보안설정이 가능하다.

데이콤, 「CADNET」



<http://www.dacom.net>

• 서비스 항목 : MPLS 기반의 VPN 및 인터넷 접속 서비스, 침입차단 및 유해 트래픽 차단, 침입탐지, 안티 바이러스 및 스펀, 패치관리, 취약점 정보제공

• 서비스 요금 : 보안 서비스 요금은 네트워크 회선료에 통합되어 있으며, 속도별로 기존 회선요금의 20~30% 추가

• 서비스 주요 특징 : 네트워크를 안전하게 유지하고 통신마비의 위험으로부터 기업 네트워크를 효과적으로 보호하기 위한 데이콤 네트워크 서비스 CADNET(Cyber Attack Defense Network)은 별도의 보안장비 및 관리 시스템을 도입하지 않고, 단순히 회선 서비스만 이용해도 보안 솔루션을 도입하는 것 이상의 효과를 낼 수 있다는 점에서 여타의 보안 서비스와도 구별된다. 또한 초기 구축비용이 필요하지 않으며 최신 공격기법에 대한 업데이트, 네트워크 대역의 확장, 장비 노후화 대체 투자가 큰 특징으로 손꼽힌다.

데이콤, 「시큐어박스」



<http://www.dacom.net>

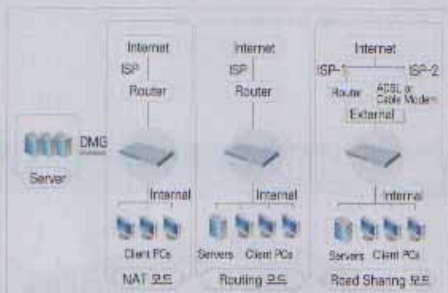
• 서비스 항목 : 침입차단 시스템, VPN, IPS, 바이러스 윌, 콘텐츠 필터링

• 서비스 이용료(변경설치비, 회당 30,000원, 단위 : 원)

	서비스 이용료				설치비	대상고객
	무이용	1년 약정	2년 약정	3년 약정		
Secure BOX 20	69,000	64,000	69,000	49,000	60,000	PC 10대규모
Secure BOX 50	79,000	74,000	69,000	59,000	60,000	PC 50대규모
Secure BOX 200	300,000	285,000	270,000	255,000	200,000	PC 200대규모
Secure BOX 300	700,000	665,000	630,000	595,000	600,000	PC 300대규모

• 주요특징 : 50인 이하, 소기업 100여 고객을 대상으로 한 설문조사를 바탕으로 필수 서비스만을 선별적으로 제공하는 「시큐어박스」 서비스는 임대장비를 통한 보안 서비스로, 데이콤 관제 센터를 통해 관제 및 24시간 장애 대응 서비스를 제공한다. 특히, 보안의 필요성에도 불구하고 소기업용 솔루션이 부재해 가격과 인력에 부담을 느끼는 고객들을 위한 최초의 통합보안 서비스로 유저 수에 따라 각 서비스 항목의 선택이 가능하다.

KT 비즈메카, 「Secure NET」



<http://www.bizmeka.com>

• 서비스 항목 : 침입차단·탐지 시스템, 백신, VPN, 콘텐츠 필터링

• 서비스 이용료(단위 : 원)

	서비스 이용료	설치비	미집비	대상고객
SecureNET 50	88,000	60,000	30,000	PC 50대 이하 규모
SecureNET 150	330,000	200,000	100,000	PC 150대 이하 규모
SecureNET 250	760,000	300,000	150,000	PC 250대 이하 규모

• 서비스의 특징 : 중소기업뿐만 아니라 의료기관, 소규모 금융기관들을 대상으로 서비스하고 있는 이 서비스 역시 제품을 임대한 후 이를 통해 웹, 바이러스, 해킹은 물론 스팸 및 유해 사이트 차단과 같은 보안 서비스를 제공한다. 임대장비로는 데이콤이 제공하고 있는 포트넷 「포티게이트」 시리즈를 제공하고 있다. 한편, 24시간 보안관제 서비스와 펌웨어 업데이트 등을 적용해 지속적인 보안강화를 이루고 있다.