말뫼의 눈물 - 이제는 시장이다

사이버 공간에서의 보안은 공격자와 방어자가 서로의 행동에 연속적으로 반응하는 일종의 군비확장 경쟁(Arms Race)에 비유된다. 정보기술과 사이버 공간이 현재와 같은 속도로 진화하는 동안에는 이런 경쟁이 계속될 가능성이 높다. 따라서 방어자의 입장에서 사이버 보안에 대한 접근은 보호하고자 하는 정보자산의 가치에 따라 예방적(Preventive)이고 선제적(Preemptive)인 대책을 구사할 필요가 있다. 그렇지 않으면 일이 터지고 그때서야 대책 마련에 부지런을 떠는 '소 잃고 외양간 고치는' 식의 대응적(Responsive) 수준에 머무를 수 밖에 없다. 상황에 따라 대응적 수준의 보안대책이 최선인 경우도 있으나, 정보기술 환경 또는 사이버 공간의 안전·신뢰성을 적극적으로 확보하기 위해서는 예방적이고 선제적인 보안 수단을 다양한 조직과 시스템에 광범위하게 적용할 필요가 있다.

김홍근 개인정보보호지원센터 연구위원(hgkim@kisa.or.kr)

정보보호 시장(또는 산업)은 사이버 공간의 대응적 또는 선제적 보안 수단을 제공하는 원천이다. 그런데, 대응적이든 선제적이든 시장이 충분한 보안수단을 공급하지 못한다면, 사이버 보안은 공격자에 비해 열세에 놓일 수밖에 없다. 사이버 보안에 필요한 수단을 개발 보급하는 주역이 정보보호 시장이기 때문에, 정보보호 시장이 강해야 우리나라의 전체 사이버 보안이 강화될 수 있다. 정보보호 시장을 강화시키기 위해서는 무엇보다도 산업이 들어설 수 있는 수요 창출이 핵심이다. 또한, 미국이나 이스라엘 등의 정보보호 강국과 경쟁할 실력을 기르기 위해서도 우리의 정보보호 시장 규모는 좀 더 커져야 한다.

정보보호 시장확대, 누가 주도해야 하나

정보보호 시장의 성장을 위해서는 첫 번째, 정보보호 서비스에 대한 공공분야의 시장을 확대해야 한다. 사이버 보안수단의 구현에는 비용이 소요돼 경제적으로 민감하다. 만일 사이버 보안의 개선으로 충분한 경제적 인센티브가 발생한다면, 기존의 이행과 같은 규제가 없어도 투자가 이루어질 수 있다. 그러나 사이버 보안에 대한 투자 대비 효과를 측정하기는 쉽지 않아, 민간 분야에서의 사이버 보안에 대한 투자는 대부분의 경우 후순위로 밀려난다. 따라서 사이버 보안에서의 시장은 공공 분야가 선도하고, 민간 분야는 이를 따라가는 형국이 될 수밖에 없다. 한편 진화하는 사이버 위협을 적극적으로 반영하는 보안기능은 소프트웨어로 구현되며, 소프트웨어가 서비스로 자리잡는 추세에 따라 정보보호 산업도 많은 부분 서비스 시장으로 형성되고 있다. 안티-악성코드 제품이 지속적인 탐지 패턴 갱신 서비스를 받지 않는다면 무용지물이며, 네트워크 방화벽, 침입탐지, 컨텐츠 필터링 등의 제품이 사용되는 소위 '보안 관제(Managed Security Service)'로 불리는 실시간 침입관리(Intrusion Management)는 대표적인 정보보호 서비스이다. 정보보호 자체가 일회성 보안 제품의 설치로 이루어지는 것이 아니라, 연속적인 보안 관리 프로세스임을 감안할 때, 앞으로도 정보보호 시장은 정보보호 서비스를 중심으로 성장할 것이다. 정보보호 강국인 미국에서 IT 보안을 위한 제품이나 서비스의 공공분야 조달도 스스로 개발 조달하는 GOTS(Government Off The Shelf)에서 벗어나 시장에서 조달하는 COTS(Commercial Off The Shelf)을 채택하고 있다. IT 자산에 대한 보안 관리의 핵심 프로세스인 위험 분석이나 실시간 침입관리 서비스를 포함해 다양한 정보보호 서비스를 민간에 아웃소싱해, 정보보호 시장의 성장을 견인하려는 공공 분야의 발상의 전환이 요구된다.

ISP 차원의 개인 사용자 보호 이뤄져야

정보보호 시장 성장을 위한 두 번째 요소는 국가주요 인프라의 분야별 정보공유분석센터 ISAC(Information Sharing & Analysis Center)[1]를 설립해 운영하는 것이다. 미국에서는 1999년 금융 분야를 시작으로 통신, 전기, 수자원, 운송, 도로, 에너지 등 14개의 주요 인프라별 정보공유

분석센터를 설립해 운영하고 있다. 우리나라도 정보통신 기반보호법에 의거해, 금융 ISAC을 설립, 실시간 경보 · 분석 체계를 운영하고 있다. 통신 분야를 포함해 일부 ISAC이 설립돼 있으나, 아직까지 조직이나 예산 규모 측면에서 미미한 실정이다. 국가사회 주요 인프라의 IT 자산에 대한 지속적이고 일관된 보안 관리 프로세스를 위한 정보공유분석센터의 역할은 미국의 사례에서와 같이 매우 중요한 의미를 갖는다. 때문에, 금융분야 외에도 공공부문의 분야별 정보공유분석센터의 설립을 확산시켜야 한다. 침해 모니터링 및 실시간 경보 · 대응체계 운영, 취약점 및 침해요인과 이에 대한 대응방안에 대한 각종 정보제공, 정보기술 환경에 대한 취약점 분석 평가 및 보호대책 수립 등 정보공유분석센터의 업무는 정보보호 시장 규모의 증가로 이어질 것이다.

정보보호 시장의 성장을 위한 세 번째는 인터넷 서비스를 제공하는 ISP의 사용자 보호 역할을 강화하는 것이다. 사이버 보안은 일반적인 인터넷 사용자들에게 부담을 주기에 충분한 기술적 지식과 숙련을 요구한다. 또한 기술과 위협의 동반 진화에 따른 교육과 훈련이 이를 따라잡지 못하는 것이 현실이다. 따라서 지금까지의 가정용 컴퓨터 사용자를 교육시켜 스스로 컴퓨터 보안을 관리케 하는 방식은 성공하지 못하고 있다. 반면, 감염된 사용자 컴퓨터로부터의 비정상 IP 트래픽을 탐지하는 기술의 발전에 따라, ISP가 가입자 컴퓨터에서 출발하는 비정상 패킷을 탐지 · 제거하는 것이 가능해졌다. 따라서 좀비 컴퓨터로부터의 스팸 메일을 차단시키는 시스템이나, 악성코드에 감염된 가입자 컴퓨터들을 자동적으로 식별하고 격리시켜, 추가적인 악성 소프트웨어의 전파를 차단하는 시스템을 ISP가 운영할 필요가 있다. ISP 입장에서는 악성코드에 의해 트래픽이 증가하거나, 악성코드에 의해 오작동하는 컴퓨터에 대한 가입자의 불만으로 발생하는 가입자 이탈율(Churn Rate)을 억제시키는 효과[2]도 있다. 가정용 컴퓨터는 대부분 초고속 인터넷에 접속되어 있기 때문에 가정용 컴퓨터의 보안 관리를 ISP의 서비스로 일정 부분 대체하면 이는 시장의 서비스를 필요로 하는 보안 관리 대상의 상당한 증가를 의미한다. ISP는 대형 통신업체와 지역 케이블 사업자 등 가입자 규모와 매출액 등의 측면에서 다양하며, 또한 가입자 컴퓨터에 대한 보안관리 역량도 들쭉날쭉이다. 이들 사업자의 가입자 컴퓨터에 대한 보안관리 역량을 일정 수준 이상으로 균등화하는 것도 정보보호 시장의 수요를 유발할 수 있다.

세계 최대 정보보호 기업의 출현을 바라며

'말뫼(Malmö)의 눈물'이라는 말이 있다. 우리나라 조선(造船) 신화를 이야기할 때 곧잘 회자되는 말이다. 울산시 방어동에 위치한 현대중공업의 1,500톤 골리앗 크레인은 조선공업에서 한 때 세계 최강이었던 스웨덴 말뫼의 한 조선소에 있던 크레인을 현대중공업이 단돈 "1달러"에 인수해온 초대형 크레인이다. 당시 이 크레인이 울산으로 떠나자 스웨덴 언론들이 '말뫼가 울었다'는 제목으로 안타까움을 보도해 이후 '말뫼의 눈물'이란 별명이 붙었다. 특히 이 크레인은 유럽 조선업체의 번영기를 상징하던 것으로, 이 크레인이 유럽에서 옮겨졌다는 것은 세계 조선업계의 패권이 유럽에서 한국으로 이동했다는 것으로 해석되기도 한다. 피터 드러커는 저서 '넥스트 소사이어티'에서 기업가 정신 1등 국가로 한국을 꼽으면서 그 이유를 이렇게 밝혔다. "약 40년 전만 해도 한국에는 기업이 전혀 없었다. 한국을 몇 십 년 동안 지배한 일본이 기업과 고등교육을 허용하지 않았다. 한국전쟁이 끝날 무렵 남한은 완전히 파괴됐다. 오늘날 한국은 24개 가량의 산업에서 세계 일류 수준이고 조선과 몇몇 분야에서는 세계 선두주자다."[3] 우리의 정보보호 산업도 세계 일류가 될 수 있다. 그러기 위해서는 정보보호 시장의 규모를 키우고, 우수한 인재들을 끌어들여야 한다. 마침 새로운 정부의 정책도 시장 친화적으로 한층 업그레이드될 것으로 기대되고 있다. 우리 모두 팔을 걷어붙이고 세계 최대 정보보호 기업 시만텍을 능가하는 일류 기업이 나올 수 있도록 해보자. 그러기 위해서는 가장 먼저 시장이 커져야 한다. S

1 필자는 '정보공유 및 분석'이라는 단어적 의미 이상으로 해당 분야의 정보보호 전담기관의 의미로 해석한다.

2 영국의 인터넷 보안회사 StreamShield 社는 봇 또는 좀비 감염 PC에 의한 트래픽 증가와 가입자 이탈율 증가로 인해, 브로드밴드 또는 케이블 인터넷 서비스 사업자가 입는 손실이 연간 5억 달러에 이른다고 주장. http://www.streamshield.com

3 황호택, 지금 영웅들은 기업에 있다, 동아일보, 2007년 10월 12일 http://www.donga.com/fbin/moeum?n=column$i_58&a=v&l=10&id=200710120476