[정보보호] 중소기업 정보보호 활동의 활성화 방안

정보통계 조사에 따르면 중소기업은 민간부분 전체 기업의 99.96%를 차지하고 있으며, 사이버범죄의 주요 대상이 되고 있다. IT기술의 급속한 발전은 경제 활동에 있어 중소기업이 영향력을 확장할 수 있는 기반을 제공하고 있으며, 중소기업이 보유하고 있는 정보 자산의 가치 증가는 사이버범죄의 타겟이 되는 또 다른 이유이다. 최근 많은 보안 사고들이 중소기업들에서 발생하고 있는 것은 중소기업이 보안 활동의 사각지대에 노출되고 있음을 보여준다. 중소기업을 대상으로 하는 사이버범죄가 지속적으로 발생하고 있음에도 불구하고 대기업과 중소기업 간의 보안 준비 수준의 격차는 커지고 있다. 중소기업의 보안 수준은 더이상 한 기업만의 문제가 아니며 국가 안보 수준에까지 영향을 미칠 수 있음을 인지하여 한다. 우리는 중소기업의 보안 수준을 개선하기 위한 노력을 하여야 한다. 그러나 중소기업은 제한된 인력과 예산의 부족으로 인해 수준 높은 정보보호 활동을 이행하는 것이 어렵다는 현실적 문제를 가지고 있다. 중소기업이 스스로 정보보호 활동에 참여할 수 있도록 유도할 수 있는 활동이 필요하며, 중소기업을 위한 정보보호 관리체계의 국제 표준 개발과 제공은 중소기업이 정보 보호 활동에 적극적으로 참여할 수 있는 동기를 부여할 수 있을 것으로 기대된다.

❍ 국내 중소기업 정보보호 활동

한국인터넷진흥원(KISA)에서는 국내의 정보보호 관리체계(이하 K-ISMS)를 통하여 국내 기업이 스스로 정보보호 환경을 구축·운영하는데 활용할 수 있도록 관리체계 모델을 개발하여 제공하고 있다. 2003년 1.25 인터넷 대란 이후 기업이 최소한의 보안조치를 하도록 의무화하여 시행하던 종전의 정보보호 안전진단 제도가 실효성 문제 등으로 폐지되고 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 개정을 통하여 보다 높은 수준의 K-ISMS 인증 제도로 일원화 하였다. 그러나 강화된 K-ISMS의 인증 기준은 제도의 원활한 보급 등을 위하여 공공기관과 대기업 등 일정 규모 이상의 기관을 중심으로 활용이 되고 있다. 이에 기존의 진입장벽이 높은 인증 제도가 아닌 누구나 진입이 가능한 정보보호 제도가 사회적으로 요구되면서, 2014년 8월 정보보호 자율규제 문화 정착 및 기업의 자발적 보안 역량 강화 유도를 위한 민간 자율의

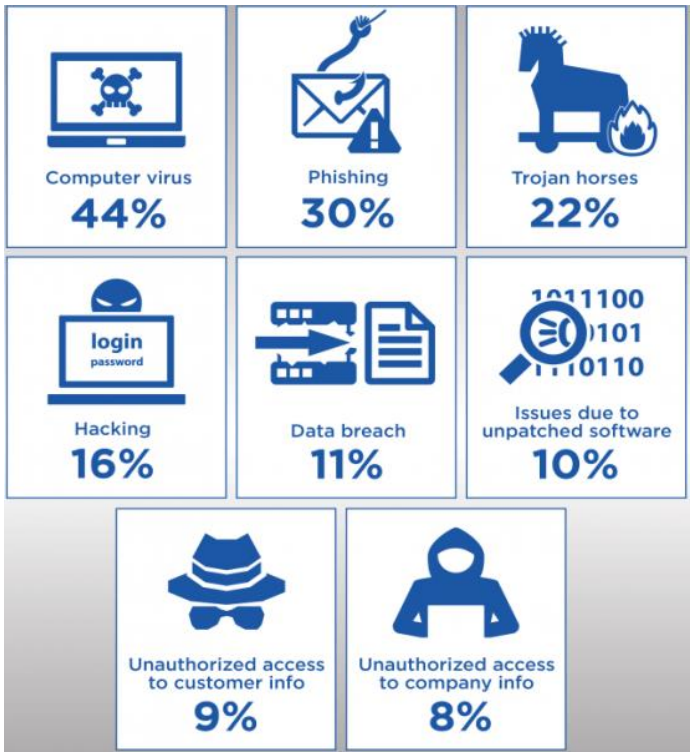
「정보보호 준비도 평가」제도에 대한 도입이 발표되었다. 「정보보호 준비도 평가」의 등급모델 및 평가기준 방법 등 초기 제도 설계는 국가에서 지원하되 도입과 시행은 기술 이전을 통해 민간 자율에 의해 운영한다는 전략으로 보안의 사각지대를 최소화하고, 중소기업을 포함한 정보보호 활동이 필요한 모든 대상에 대해 보안투자 비율 및 인력, 조직 확충, 개인정보보호, 법규 준수 등 기업의 보안역량 강화를 도모하고 촉진하고 하고있다.

그러나 중소기업의 많은 참여를 기대했던 「정보보호 준비도 평가」제도가 시작된 지도 3년이 다 되어가고 있으나 현재까지도 적극적으로 활성화 되고 있지는 못한 상황이며, 제도의 활성화를 위해서는 중소기업이 정보보호 활동을 체계적으로 이행할 수 있는 실효적인 가이드라인이 제공되어야 한다는 요구가 커지고 있다.

❍ 해외 중소기업 정보보호 활동

중소기업에 대한 보안을 강화해야 한다는 주장은 글로벌 국가들에서도 당면과제로 부상하고 있다.

[그림] 미국 중소기업의 사이버위협



※ 출처 : The 2015 Small Business Owner Study commissioned by nationwide and conducted by Harrris Poll Online.

2015년 11월 네이션와이드 (Nationwide)에서 300인 이하의 중소기업을 대상으로 한 사이버 범죄에 대한 준비도 조사 결과 발표에서는, 63%의 중소기업들이 1년에 한번 이상의 보안위협을 받았다고 조사되었음에도 불구하고 79%의 중소기업들은 사이버위협으로부터의 대응 계획을 여전히 가지고 있지 않은 것으로 조사되어 미국도 중소기업에 대한 정보보호 수준이 위험한 수준임을 확인할 수 있다.

미국 정부는 2016년 2월 사이버 국가행동계획 발표에서 140만 중소기업 및 소규모 비즈니스 이해관계자들에게 사이버 보안교육을 제공하는 계획을 포함하고 미국의 안보를 위한 주요 과제 중이 하나로 선정하여 발표하였으며, 미연방통신위원회(Federal Communications Commission)와 미중소기업청(The Small Business Administration)에서는 중소기업을 위한 사이버보안에 대한 가이드를 제공하고 있다.

미국에서의 중소기업을 위한 정보보호 가이드에서는 중앙집중식의 정보보호 관리가 어렵다는 현실을 반영하는 등 사용자 중심으로 일상생활에 밀접한 내용으로 가이드를 제공하고 있다.

❍ 중소기업 정보보호 관리체계의 개발과 보급

조직의 규모와 보안 역량의 수준은 통계적으로 유의미한 것으로 알려져 있으며, 인적 자원이 부족한 중소기업이 정보보호의 사각지대에 놓이고 있는 것은 당연한 결과이다. 정보보호의 수준은 정보보호 관리체계의 지속적인 운영과 성숙도에 따라 달라진다. 그러나, 현재 보급되고 있는 정보보호 활동의 가이드라인인 ISO27001과 K-ISMS는 중소기업의 역량에 대한 고려를 반영하고 있지 않으며, 일반적인 기준으로 적절한 정보보호 수준을 유지하기 위해 필요로 하는 관점에서 개발되었다. 대기업에 대하여 상대적으로 부족한 경험, 예산, 인적 자원은 중소기업들 스스로 정보보호 활동에 대한 참여하는 것을 어렵게 만들고 있다. 그 결과, 중소기업은 보안의 위협에 점점 더 많이 노출되고 있는 상황이 된 것이다.

중소기업의 정보보호 수준이 균형 있게 성장할 수 있도록 지원하기 위한 방안으로 중소기업을 위한 정보보호 관리체계의 개발이 진행되고 있다. 현재 ITU-T SG17에서는 가칭 X.sgsm이라는 중소조직을 위한 정보보호가이드라인이 개발이 되고 있다. 중소조직 관점에서의 정보보호 활동에 대한 기준으로 개발되고 있는 X.sgsm은 현재 한국과 일본이 공동으로 개발을 진행하고 있으며,

정보보호 관리체계의 국제 표준인 ISO27002의 오브젝트(Object)와 컨트롤(Control)을 유지하되 중소조직에서 정보보호 활동을 실행 할 때 도움이 될 수 있는 운영가이드를 제공하는 것을 목표로 진행되고 있다. 약 8년간의 연구 개발 기간을 거친 결과는 2017년 9월 회의에서 최종 승인될 것으로 기대되고 있으며, 중소조직을 위한 정보보호 관리체계가 국제표준으로 발표될 경우 중소기업의 자발적인 정보보호 활동에 대한 참여를 유도할 수 있을 것으로 기대된다. 중소기업에 대한 배려를 통한 공동의 정보보호 활동의 지원은, 우리 모두가 안심하고 활동할 수 있는 미래를 제공할 것이다.

김창오(주식회사 쿠팡 팀장, ispiadviser@gmail.com)