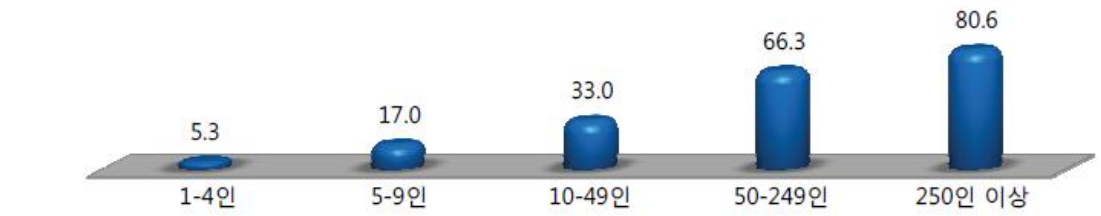
[정보보호] 중소기업 정보보호 관리체계 표준을 통한 정보보호 수준의 균형화

지능형 지속공격(APT) 등 사이버 위협이 확산되고 보안의 위협이 기업뿐만 아니라 국가 전반의 이슈로 확대됨에 따라 정부뿐만 아니라 범국가적인 차원에서 보안 활동에 대한 수준 제고의 필요성이 요구되고 있다. 사이버 공격의 과정에서는 상대적으로 보안이 취약한 수 많은 중소기업의 인프라가 공격의 주요 거점으로 이용되고 있다. 이는 현재의 정보보호 정책이 공격자들의 활동을 효과적으로 억제하고 있지 못하고 있음을 보여주는 하나의 예이다.

현재 우리나라는 정보보호 관리체계(ISMS)와 개인정보보호 관리체계(PIMS)를 중심으로 국가 주도의 정보보호 관리 수준 향상을 도모하는 활동을 전개하고 있다. 그러나 위 제도들은 대기업 또는 「정보통신망이용촉진 및 정보보호 등에 관한 법률」의 기준에 따른 일정 규모 이상의 기업에 대해서만 그 대상을 두고 있기에 국가 전반에 걸친 정보보호 수준의 균형적인 성장을 이끌기에는 어려움이 있다.

국내 정보보호 관리체계 제도의 경우 약 400여개의 기업만이 따르고 있으며, 이나마도 법률(「정보통신망법」 제 47조 제 2항)에서 정한 의무대상자(ISP, IDC, 정보통신서비스 매출액 100억 또는 이용자 수 100만 명 이상인 사업자)들이 주로 이행하고 있다고 할 수 있다. 다행히 2016년 5월 개정된 정보통신망법 시행령의 개정에 따라 연간 매출액 또는 세입이 1,500억 이상인 상급종합병원과 학교가 의무 대상자에 포함되기는 하였으나 여전히 정보보호 활동의 사각지대에 놓인 중소규모의 기업과 조직에 대해서는 자율에 맡기고 있어 비용과 인력의 한계로 인해 높은 수준의 정보보호 활동 기준을 준수하기에는 어려운 것이 현재의 실정이다.



[그림] 규모별 정보보호 정책의 수립 현황

(출처: 2014 정보보호실태조사,한국인터넷진흥원)

한국정보화진흥원의 “2014년 정보화통계조사” 결과에 따르면 우리나라에는 약 150만개의 사업장이 컴퓨터를 보유하거나 네트워크를 구축하고 있다. 컴퓨터와 네트워크를 이용하는 기업의 경우 정보를 전산화 하여 처리하고 있음을 의미하며 이는 곧 정보보호의 활동이 필요하다는 것을 의미한다. 이중 약 67%는 소상공인이며 약 30%가 소기업으로 전체의 97%를 차지하고 있다. 지금까지 우리의 정보보호 활동은 전체의 0.1%도 되지 않는 대기업을 중심으로만 이루어져 왔기에 이제는 정보보호 활동의 사각지대에 놓인 중소기업과 소상공인의 정보보호 활동을 지원하기 위한 적극적인 노력이 필요한 시점이다..

이러한 중소기업의 정보보호 관리에 대한 필요성이 제기됨에 따라 2014년 영세/중소기업 및 비 ICT 분야 등 정보보호 사각지대를 최소화하고 모든 정보보호 대상 기업에 대해 보안투자 비율 및 인력, 조직 확충, 개인정보보호, 법규 준수 등 기업의 보안역량 강화를 촉진하고 도모하고자 민간 자율의 「정보보호 준비도 평가」제도가 출범되었으나 아직 제도 초기인 만큼 국내 중소기업의 정보보호 활동을 적극적으로 지원하기 위한 노력의 지속이 필요하다고 하겠다.

중소기업의 정보보호 활동을 지원하기 위한 연구는 2010년부터 한국인터넷진흥원(KISA)를 중심으로 진행되어 왔으며, 기업의 규모와 상황을 고려한 정보보호 활동 가이드의 필요성이

제기됨에 따라 현재는 한국정보통신기술협회(TTA)를 중심으로 2015년부터 중소기업을 위한 정보보호 관리체계에 대한 국제 표준을 추진하고 있다.

ITU-T(International Telecommunication Union Telecommunication Standardization Sector) SG(Study Group)17에는 통신 조직을 대상으로 정보보호와 관련한 표준활동들이 주도적으로 진행되어 왔으며, 정보보호 활동에 대한 기준이 되는 관리체계에 대한 표준을 수립하기 위한 활동도 지속되어 왔다. 글로벌 하게는 ISO27001을 정보보호 관리체계에 대한 표준으로 활용되고 있으며 우리나라에서는 이를 기준으로 한국형 정보보호 관리체계(K-ISMS)를 수립하여 모든 정보통신 산업이 활용하고 있는 실정이다. 그러한 이러한 표준은 현재의 표준은 조직의 규모와 상황에 관계 없이 획일적으로 단일 표준 가이드를 제공하고 있어 중소규모의 조직에서는 표준 정보보호 관리체계를 따르는 것이 인력 및 비용의 투자 등에 있어 어려움과 한계가 있는 것이 현실이다. 따라서, 이러한 현실적 문제를 극복하고 중소기업들이 최소한의 정보보호 관리체계를 수립할 수 있는 공인된 표준이 필요하다고 하겠다.

제한적인 자원을 가진 중소기업이 정보보호 활동의 사각지대에 놓이지 않고 균형 있는 정보보호 수준의 향상을 도모하기 위해서는, 중소기업들에게 실직적으로 도움이 될 수 있는 중소 조직의 환경을 고려한 공인된 정보보호 관리 활동의 표준 수립이 필요한 것이다.
중소기업 정보보호 관리 활동의 표준화 방향은 기존 대기업 중심의 정보보호 활동 기준이 아닌 인력과 비용의 투자에 제약을 가진 중소기업이 실효적이며 실제 이행이 가능한 현실적인 활동 기준을 표준화되어야 하며 중소기업의 정보보호 관리체계 활동에 대한 동기를 부여할 수 있는 새로운 기준 지표를 제공하는 것이 목표 이다.

중소기업을 위한 정보보호관리 체계의 필요성에 대해서는 우리나라 뿐만 아니라 일본에서도 매우 많은 관심을 가지고 있으며 현재 ITU-T SG17에서 한국과 일본의 주도로 중소기업의 정보보호 표준활동 가이드에 대한 국제표준화를 준비되고 있으며, 2017년 발표를 목표로 진행되고 있는 X.sgsm으로 불리는 중소기업 정보보호 관리체계 표준가이드(Information security management guidelines for small and medium telecommunication organizations)는 국내뿐만

아니라 국제적으로 중소기업들의 정보보호활동에 활력을 불어 넣을 수 있는 새로운 기준을 제시할 수 있을 것으로 기대된다.

따라서 국내 중소기업에 대한 현실을 국제표준에 반영하기 위한 지속적인 연구와 노력과 함께 중소기업의 정보보호 활동에 대한 자발적이고 적극적인 참여를 유도할 수 있는 다양한 제도의 활성화는 국가 전체의 균형 있는 정보보호수준 향상의 기반이 될 수 있을 것으로 기대된다.

기초가 약하여 오래가지 못하는 것을 뜻하는 사상누각(沙上樓閣)이라는 고사성어가 있다. 이는 건축에서뿐 아니라 사상이나 정책에서도 그 기반이 튼튼해야 한다는 의미를 시사하고 있다. 따라서, 중소기업의 현실을 고려한 최소한의 정보보호 관리체계의 수립을 통해 산업 전반의 정보보호 수준에 대한 균형적인 발전을 지원할 필요가 있다고 하겠다. 우리나라의 정보보호 수준이 개선되기 위해서는 산업의 기반이 되고 있는 중소기업에 대한 정보보호 수준이 튼튼해져야 국가 전반의 안정적이고 균형적인 정보보호 수준의 성장을 기대할 수 있을 것이다.

김창오(포워드벤처스 팀장, ispiadvisor@gmail.com)