정보보호 수준 자가 측정

환상 기업의 정보보호 수준을 측정하라

정보보호 부서 이동 후 새로운 업무를 이해하는 것만으로 한 달을 소비한 김 대리. 그렇다고 성과가 전혀 없던 것은 아니었다. 어떤 웹 사이트가 유용한 정보를 제공하고 있는지 알게 됐고, 악성코드나 바이러스처럼 간혹 언론매체를 통해 접했던 정보보호 관련 용어가 더 이상 낯설지 않게 됐다. 무엇보다 '환상' 기업의 보안관으로서 어떤 활동을 해야 할 것인지를 이해했다는 점에서 김 대리에게 지난 한 달은 의미있는 시간이었다. 하지만 이제 막 한숨을 돌린 김 대리는 또 다른 난관에 봉착했다. 경영진으로부터 환상기업의 정보보호 수준을 수치화해 보고하라는 지시가 내려온 것이다.

정보보호뉴스 취재팀

경영진으로부터 'Mission'을 전달받은 김 대리는 기업 정보보호 수준측정은 중요하지만 한편으로, 쉽지 않은 문제라고 생각했다. 왜냐하면 정보보호 수준은 해킹, 악성코드, 바이러스 등에 대비해 여러 개의 보안 시스템을 도입한다고 높아지는 것이 아닐 뿐만 아니라, 경영진을 비롯한 내부 직원들의 보안의식은 수치화될 수 없다는 생각이 들었기 때문이다. 특히 많은 보안사고의 원인이 직원들의 작은 실수와 무관심에서 비롯된다는 점은 정보보호 수준을 수치화해야 하는 김 대리에게 가장 큰 어려움이 아닐 수 없었다.

정보보호 컨설팅, 비용이 문제가 안 된다면

고민을 거듭하던 김 대리는 기업 정보자산의 규모가 크고, 또 기업의 운명을 결정짓는 산업기밀을 보유한 기업들은 공통적으로 정보보호 컨설팅을 받는다는 사실을 알게 됐다. 경영 컨설팅, 재무 컨설팅 등과 같은 단어는 들어봤지만 정보보호 컨설팅이라는 말이 낯설게만 느껴진 김 대리, 내침 김에 정보보호 컨설팅에 대해 좀 더 알아보기로 결심했다.

정보보호 컨설팅은

정보보호 컨설팅은 전산 시스템과 네트워크, PC 등 모든 IT 자산 및 데이터화된 정보자산의 운영 및 관리에 있어 발생 가능한 위험을 분석하고 대책을 수립, 이를 기업이 실현할 수 있도록 하는 자문 서비스로, 일반 기업들이 자사의 정보보호 수준을 평가하는 것은 물론, 정보보호 강화를 위한 사전 단계로 이용하고 있다. 국내에서는 정보통신과 관련된 주요 기반시설을 보유한 기관이 전자적 침해행위 즉, 침해사고 등으로부터 효과적으로 대응할 수 있도록 지난 2001년부터 '정보보호컨설팅전문업체' 제도를 운영하고 있으며, 2008년 4월을 기준으로 7개의 업체가 전문업체로 지정돼 있다. 이들 정보보호컨설팅전문업체는 국가가 지정한 주요기반시설에 대한 정보보호 컨설팅을 수행할 수 있는 자격을 갖게 되는 반면, 컨설팅 인력, 업무수행요건, 설비, 자본금 등에서 일정 이상의 요건을 갖춰야 하며, 3년마다 재심사를 거쳐 전문업체의 자격을 유지하게 된다. 다만, 정보보호컨설팅전문업체만이 정보보호 컨설팅을 할 수 있다는 의미는 아니며, 국가가 지정한 주요기반시설이 아닌 경우에는 다른 컨설팅 업체로부터 정보보호 컨설팅을 받을 수 있다. 최근에는 정보보호 업체뿐만이 아니라, 감사와 관련된 전문 경영 컨설팅 기업에서도 정보보호 컨설팅을 실시하고 있으며, 그에 따라 컨설팅 기법도 다양해지고 있다. 정보보호 컨설팅을 받은 후에는 기업의 정보보호 수준뿐만 아니라, 기업의 정보보호 정책방향 설정이나 보안 규정집이 제작되는 등 객관적인 산출물까지 얻을 수 있게 된다.

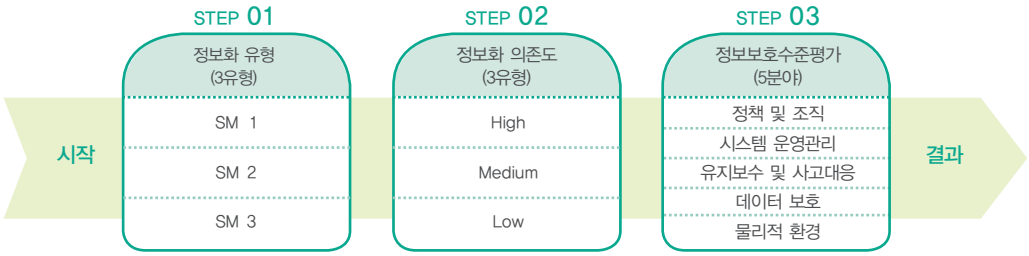
물론 정보보호 컨설팅이 이뤄지기 위해서는 기업 정보보호 담당자를 비롯해, 직원들 모두가 적극적으로 동참해야 한다는 전제가 있지만, 정보보호 컨설팅 하나만으로 지금까지의 고민이 해결될 것이라고 생각한 김 대리. 하지만 그가 간과한 것이 하나 있었다. 바로 정보보호 컨설팅을 받기 위한 비용이었다. 그렇지 않아도 정보보호를 위해서 투자를 하지 않는 경영진에게 정보보호 컨설팅 비용을 결제 받을 용기가 김 대리에게는 없었던 것이다.

정보보호 자가수준 측정 서비스를 찾다

다시 원점으로 돌아온 김 대리는 평소 즐겨찾던 한국정보보호진흥원의 웹 사이트를 검색하던 중 마침내 해결책을 찾았다. '기업 정보보호 자가수준 측정 서비스'가 바로 그 해답이었다. 정보보호 자가수준 측정 서비스는 환상기업처럼 정보보호에 투자하기 어려운 작은 규모의 중소기업이 스스로 자사의 정보보호 관리활동 및 정보자산의 보호조치 상태 등을 진단하고, 정보보호 조치가 필요한 부분과 그에 대한 가이드라인을 제시받을 수 있는 서비스로, 약 30분 정도의 시간만 투자하면 정보보호 수준을 측정할 수 있게 된다. 물론 소요되는 비용 없이 문제점과 결과, 그리고 대비책이 제시되기 때문에 김 대리에게는 더할 나위 없이 편리한 도구인 셈이다.

정보보호 자가수준 측정 서비스

'정보화 규모', '정보화 의존도', '정보보호 수준 측정' 등 3단계로 구성된 정보보호 자가수준 측정 서비스는 설문조사 형태로 진행되며, 약 30분 동안의 조사 후 해당 기업에게 필요한 정보보호 요소는 무엇이고, 또 해결방안은 무엇인지를 알려주게 된다.



▲ 정보보호 자가수준 측정 서비스 절차

정보화 유형

정보화 유형에서는 기업의 IT 환경에 따라 SM(Small & Medium) 1~3까지 구분하며, SM 3으로 이동할수록 보호해야 할 정보자산의 규모가 커짐을 의미하며, 그에 따라 요구되는 정보보호 수준도 높아지게 된다.

정보화 의존

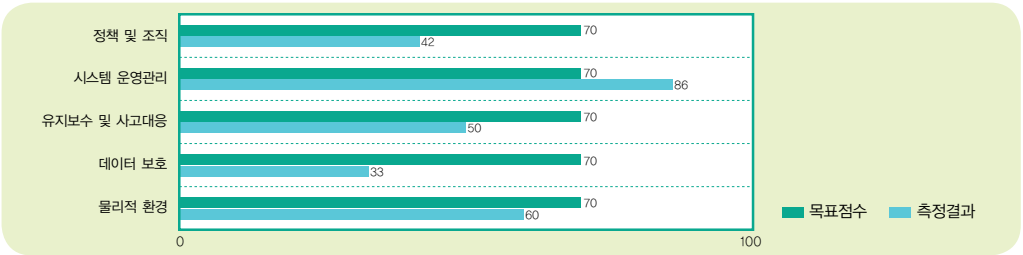
정보화 자산의 민감성, 침해사고 발생 시 기업에 미치는 영향 등에 따라 High, Medium, Low로 구분된다. 정보화 유형이 SM 1일지라도, 정보화 의존도가 높은 기업에게는 자연스럽게 높은 정보보호 수준이 요구된다.

정보보호 수준평가

이 단계에서는 기업이 보유한 보안 정책 및 조직, 시스템 운영관리, 유지보수 및 사고대응, 데이터 보호, 물리적 환경, 아웃소싱 관리, 교육 및 훈련 등과 관련해 보안수준을 측정하고 있다.

총 평

모든 측정이 이뤄진 후에는 분야별 보안현황에 대한 총평과 KISA가 발행한 중소기업 정보보호 가이드라인을 토대로 한 정보보호 강화방안이 함께 제시된다. 특히, 대책 부분에서는 목표점수와 측정결과를 비교해 보여줌으로써 해당 기업이 어떤 문제가 있으며, 이를 해결하기 위해서 어떤 활동이 필요한지를 이용자가 알 수 있다.



▲ 보안목표 수준과 현재의 보안 수준 비교 막대그래프 예시

정보보호 수준측정 도구를 통해 '환상' 기업의 정보화 수준이 어디까지 왔는지, 왜 그리고 어떤 부분에서 정보보호가 필요한지를 알게 된 김 대리. 비록, 측정 시작단계에서 기대했던 성적표를 받지는 못했지만, 앞으로 해야 할 일이 그만큼 중요하고 필요하다는 사실을 새삼 확인하는 계기가 됐다. 이제 김 대리에게는 남은 일은 목표점수보다 떨어진 '환상'기업의 정보보호 수준을 어떻게 올릴 것이냐 하는 것이다.