화학, 내부 사이버범죄 대책 허술

CSI, 2002년 미국 정보유출 손실 7000만달러 … 내부공격이 주류

사이버 테러 발생수 및 심각성은 기업의 종류와 규모, 보유 고객에 따라 차이가 있는 것으로 조사됐다.

미국의 사이버 범죄 수사기관인 CSI(Computer Security Institute)에 따르면, 제조기업의 사이버 테러 발생은 전력, 에너지, 비영리 및 금융 서비스보다 빈도나 심각성 면에서 훨씬 낮았고 직원수가 많은 대기업들은 소기업보다 사이버테러 빈도가 더 많고 심각했던 것으로 나타났다. 미국은 사이버테러의 빈도가 가장 높아 전체 사이버테러의 35.4%를 차지했다.

여러 메이저 화학기업들은 사이버보안 수준이 사이트와 물리적 보안과 동등한 수준으로 향상됐으며 대부분 최신 보안기술을 구축했고 보안의 허점을 항상 주시해왔다.

CSI 조사 응답자들도 비슷한 의견을 나타냈으며 Antivirus Software, 방화벽 및 침입 탐지 시스템(Intrusion Detection System) 등을 사용해왔다.

화학기업들은 사유정보 보호가 우선시돼야 하며 정보유출로 인한 손실액은 수치화하기가 힘들다고 주장하고 있다. CSI 조사에서 응답자 가운데 251명이 2002년 정보유출로 인해 7000만달러의 손해를 본 것으로 응답했다.

8년의 조사기간 동안 사이버범죄 중에서 정보유출로 인한 손실액이 가장 컸고, 바이러스 다음으로 많은 사이버 범죄는 서비스거부 공격(Denial-Service Attacks)으로 웹사이트에 가짜 이메일을 유포시키고 이를 처리 불가능하게 만든다.

그러나 응답자들은 가장 일반적인 형태의 공격은 네트워크 접속시 발생하는 바이러스와 내부공격이며 공격 주체는 개인 해커들이라고 지적했다.

CSI와 몇몇 다른 사이버 보안기관들은 기업들에게 사이버 범죄가 발생하면 FBI와 같은 법 집행기관에 보고할 것을 권고하고 있다. CSI 조사의 목적 가운데 하나는 법 집행기관과 사설기관의 협력 증진을 도모해 사이버범죄에 대한 실질적인 대비책을 마련하는 것이다.

그러나 376명의 응답자 중 30%만이 사이버 범죄를 보고한 것으로 나타났다. 보고율이 낮은 이유는 사이버 보안 전문가조차 사이버 범죄를 보고할 수 있다는 사실을 인지하지 못하고 있기 때문이다. 누군가 고객정보를 빼돌렸을 때 누구에게 책임을 물을 지도 명확하지 않다. CSI는 기업들에게 사이버 범죄 발생사실을 FBI에 보고하기를 충고하고 있다.

또 대부분의 사람들은 어떤 법 집행기관에 보고하고 어떤 방법으로 법이 집행되는지 모르고 있다. 해커를 추적해내는 것이 힘들기 때문에 몇몇 기업들은 사이버 범죄를 보고함으로써 기업이미지에 부정적인 영향을 미치지 않을까 우려하고 있다.

메이저 화학기업 대부분은 중대한 사이버범죄행위가 발생하면 보고하고 있지만 다른 기업들은 보고하지 않을 것이라고 믿고 있다. 또 일부 기업들은 사이버범죄 보고로 인해 고객들을 놓칠까 우려하고 있다.

Symantec은 기업들의 Peer-to-Peer 적용 뿐만 아니라 새롭게 떠오르고 있는 통제 불가능한 인스턴트 메시지와 같이 앞으로 예상되는 몇 가지 주요 사이버 범죄 리스트를 작성하고 있으며 사이버 공격에 대한 기업들의 취약성이 더 심화될 것으로 전망하고 있다.

<화학저널 2004/07/30>