현대정보기술 ITO 센터 ITO 기술팀

CERT라는 이름의 그대, 어떤 업무를 하나요

기업이나 기관의 네트워크, 시스템에 침해사고 발생 시 신속한 대응과 예방활동을 펼치는 조직을 CERT(Computer Emergency Response Team)라고 한다. 국내 기업들 가운데 정보보호의 중요성을 깨닫고, IT 자산 보호의 일환으로 적지 않은 기업이 정보보호팀을 운영하고 있지만, 정작 CERT라는 이름을 내걸고 보안활동을 펼치는 기업은 그리 많지 않다. 그런 의미에서 지난해 개최된 정보보호大賞에서 우수상을 차지한 현대정보기술은 국내에서 CERT라는 이름을 가진 몇 안 되는 기업 중 하나다.

글·사진 정보보호뉴스 취재팀

기업 이름의 이니셜을 딴 HIT(Hyundai Information Technology) CERT는 지난 2001년부터 현대정보기술 내에 들어선 각종 시스템과 네트워크 장비에 대한 보안정책 수립과 운영을 맡고 있다. 대부분의 IDC가 그러하듯, IDC의 보안은 여러 기업의 이익과 밀접한 관계를 맺고 있어 보안의 강도는 그 어느 곳보다 강하고, 그 업무를 수행해야 하는 CERT의 중요도 역시 크다. 현대정보기술에서 그 중요한 CERT 업무를 주도하는 곳이 바로 ITO(Information Technology Outsourcing) 센터 ITO 기술팀이다.

부서를 아우르는 CERT

"ITO 기술팀이 주도하고 있지만 HIT CERT 활동에는 ITO 센터 내 여러 부서가 동참하고 있어요. 전담부서가 전사적 보안을 책임진다는 것이 장점보다는 단점이 더 많을 것이라고 판단했기 때문이죠." 현대정보기술 ITO 센터 ITO 기술팀 유우영 과장은 HIT CERT는 ITO 센터 내 서버, 네트워크, 메인프레임, 서비스 관리, 보안팀 등 5개 파트가 어우러진 조직이라고 말한다. "네트워크, 시스템이 밀집된 IDC 보안을 중심으로 활동하는 HIT CERT는 보안정책을 수립하고, 사고대응을 위해 필요한 기능을 담당하고 있어요"라는 유 과장은 HIT CERT는 부서의 개념이 아닌 Function 즉, 기능 중심의 조직이라고 설명한다. 때문에 현대정보기술의 정보보호는 침해사고 예방과 대응을 위한 전담부서 체계가 아닌, 각 부서별 예방과 대응지침을 통해 CERT 활동이 자연스럽게 귀결된다는 것이 유 과장의 얘기다. 물론 각 부서별 활동을 조율하는 것은 ITO 기술팀의 몫이 되겠지만, 각자의 업무수행이 곧 정보보호 강화라는 목표로 이뤄지게 된다. "보안이 기업의 비즈니스 요구를 충족시켜주기 위한 서비스 품질의 일환이라는 점에서 보안활동도 다양한 부서가 어우러진 총체적인 관점이 필요하다고 봐요. 여기에 기업 내 조직개편 시에도 CERT 본연의 업무와 영역은 존속될 수 있다는 장점도 있죠"라며 유 과장은 여러 부서가 어우러진 HIT CERT의 장점을 강조한다.

"침해사고 예방업무와 함께 최근에는 정보보호 성과관리에 대한 관심이 높아지고 있어요. CERT 혹은 정보보호팀의 가치를 스스로 개발해야 한다는 측면에서, 그리고 보안업무를 객관적이고 정량화된 수치로 표현해야 한다는 점에서 CERT 활동의 성과를 관리하는 것은 정보보호 담당자들에게는 매우 중요한 업무 중 하나라고 봐요." 현대정보기술 ITO 센터 ITO 기술팀 유우영 과장은 최근의 정보보호팀은 기술적인 측면뿐만 아니라, 자신들의 역할과 업무성과를 잘 표현할 수도 있어야 한다고 강조한다.

보안업무의 가치, 스스로 입증해야 할 때

흔히 사고가 발생하지 않는다면 CERT는 불필요한 조직이라고 오해하기 쉽다. 그러나 CERT의 업무 영역 중 사고대응 부문보다 더 중요한 업무가 있다. 바로 예방활동이다. 물론 HIT CERT 역시 다르지 않다. 그리고 그 예방활동 중에서 가장 먼저 등장하는 것이 감사활동이다. "매년 초

가 되면 연간 감사계획을 수립하고 정기적인 감사와, 비정기적인 감사활동을 실시하고 있어요. 매월 발견된 지적항목과 개선 계획을 구체적으로 명시해 지속적인 피드백이 있게 되죠"라는 유 과장은 두꺼운 서류철을 꺼내 보이며, 지금까지 HIT CERT가 수행해 왔던 다양한 감사활동의 증적을 보여준다. 보안품질 향상의 일환으로 진행되고 있는 감사활동은 사고를 미연에 방지하기 위한 CERT 활동 및 성과를 보여주는 가장 기초적이고 중요한 자료라고 한다.

"감사활동 뿐만이 아니라, 보안활동 전체가 성과관리 측면에서 다뤄져야 한다고 봐요. 중요한 보안활동은 무엇인지, 왜 필요한지를 알려줘야 할 필요가 있기 때문이죠. 정보보호 분야에서는 쉽지 않겠지만 다른 부서처럼 CERT 혹은 정보보호팀의 가치 역시 부서 스스로 개발해야 하겠죠." 유 과장은 그런 의미에서 CERT 활동에 대한 성과를 관리하는 방안을 도출해 지속적으로 실시하고 있다고 한다. "보안 업무를 수행하면서 이에 대한 객관적이고 정량화된 수치가 필요하다는 것을 알게 됐어요. 그런데 일반적으로 정보보호 관련 업무 성과를 측정하기 위한 항목들이 제대로 정형화된 곳은 없어요. 가령, 계정관리를 위한 보안활동을 점검하는데 필요한 보안항목은 매우 많지만, 그것 모두를 해당 기업의 특성에 맞게 정리해 놓은 자료는 어디에도 없다고 봐요. 부서 스스로 만들어 가야죠"라는 유 과장의 말 속에서 보안활동과 성과관리에 대한 HIT CERT만의 노하우가 있음을 짐작할 수 있다.

자발적인 동참 위한 보안 교육 최우선 과제

침해사고 예방과 대응체계 구축, 그리고 성과관리를 통한 체계화된 보안활동이 이뤄지고 있는 HIT CERT가 2008년 한해 중점적으로 계획하고 있는 정보보호활동은 무엇일까. "정보보호를 기업 문화 차원으로 이끌어내려고 해요. 정보보호가 언제나 새로운 기술만을 다뤄야 하는 것은 아니라고 봐요. 새로운 것에 대한 대비와 함께 성숙한 보안문화를 기업 문화화시키는 것. 이것의 2008년의 가장 큰 목표에요." 이 같은 유 과장의 설명은 사내 구성원들에게 '통제로서의 보안'이 아닌 '자발적인 의지에 의한 정보보호'가 정착될 수 있도록 유도하겠다는 의지가 담겨있다. "이를 위해 사내 구성원들을 위한 보안교육을 강화해 각 개개인이 보안 수칙을 잘 지키도록 할 예정이에요. 쉽진 않겠지만, 어떻게 하느냐 따라 그 결과는 정말 많은 차이가 있을 것 같아요"라는 유 과장은 기술적 측면과 관리적 측면 그리고 교육에 이르기까지 다양한 역할을 수행할 것이라고 강조한다.

많은 정보보호 담당자들 역시 익히 알고 있는 사실이기도 하지만 기업 정보보호는 기술적인 측면이 강조되는 것만으로는 수준 높은 보안체계를 갖출 수 없다. 때문에 최근의 기업 정보보호팀 역시 빠르게 그 역할과 업무영역을 확장하고 또 재정립하고 있다. 2001년 기술적 측면에서 보안을 강화하기 위해 조직된 HIT CERT. 하지만 시대적 변화에 따라 어떤 역할이 CERT나 정보보호팀에게 요구되는지를 보여주고 있다. S