인터넷침해사고대응지원센터 대응지원팀

정보 네트워크의 중심에 서다

정보보호에 있어 다양한 정보수집과 공유는 가장 기본적이고 필수적인 요소다. 정보공유와 협력은 사이버 공간의 안전을 책임지는 KISA에게 가장 중요한 부분이며, 실제로 KISA에서는 광범위한 정보 수집을 위해 많은 기업 · 기관들과 끊임없이 정보를 교류하고 있다. 대응지원팀은 KISA가 침해사고 예방과 신속한 대응을 위한 정보교류, 즉 정보 네트워크의 중심에 서 있을 수 있도록 활약하는 팀이다.

글 · 사진 정보보호뉴스 취재팀

지난 2003년 1 · 25 인터넷 침해사고가 발생한 뒤 국내 네트워크와 시스템의 안전에 대한 근본적인 대책을 수립하기 위해 KISA 내 인터넷침해사고대응지원센터(이하 KISC)가 본격적으로 가동되기 시작했다. 국내 ISP, IDC 등 민간 정보통신사업자들과의 공조를 통해 다양한 정보를 수집 · 분석함으로써 침해사고에 대한 예방과 신속한 대응이 그 목적이었다. 그런데 이 정보공유라는 것이 침해사고에 대비하기 위한 가장 효과적인 방법이지만 반대로, 쉽지 않은 문제이기도 하다. KISC 설립 초기, 일부 전문가들이 민간 사업자들의 정보제공에 대해 회의적인 시각을 보였던 것도 KISC와 일

반 기업 간의 정보공유가 쉽지 않을 것이라는 예상이 있었기 때문이다. 그런데 이런 우려가 기우에 불과했다는 사실을 알기까지는 그리 많은 시간이 필요하지 않았다. KISC와 민간사업자와의 정보가 원활히 공유되기 시작했고, 정보공유를 통한 협조 수준도 더욱 깊어졌기 때문이다. 그리고 그 중심에는 여러 관계 기관 및 기업들과 KISC를 맺게 해 준 대응지원팀이 있다.

정보 공유 통해 더욱 신속한 대응 가능해져

"침해사고에 대응을 위해 가장 필요하고, 또 중요한 것이 정보공유라고 봐요. 침해사고에 대한 공동대응을 위해서는 국내외 기업 및 기관들과의 지속적인 정보 네트워크를 유지하는 것이 필수적이죠." 인터넷침해사고대응지원센터 대응지원팀 허창열 팀장의 얘기다. 정보통신망법에 근거해 KISC와 법적으로 정보가 공유되는 기관은 약 110여개. 여기에는 유·무선 ISP를 비롯해, IDC 업체, SO 사업자 등 인터넷 이상징후 판단을 위해 정보제공이 꼭 필요한 국내 주요 통신사업자들이 모두 포함되어 있고 특히, 최근에는 주요 포털 및 온라인 게임업체 등 침해사고 발생 시 피해규모가 클 수밖에 없는 민간 사업자들로 대상을 확대해 이상 징후 발생 시에 신속히 대응할 수 있는 체계를 구축했다.

물론 민간 기업들과의 공조가 초기부터 원활했던 것은 아니었다. "정보를 공유하는 기업 및 기관들 의식이 초기와는 많이 달라졌어요. 처음에는 정보를 제공한다는 사실 자체에도 거부감이 있었죠. 하지만 최근에는 KISC가 각종 정보를 수집하고 분석한 후 유용한 정보로 가공한 후 제공해 주고 있다는 인식이 높아지면서 협조가 더욱 원활하고 대응 또한 신속하게 이뤄지고 있어요"라는 허 팀장은 지속적인 협력 관계를 통해 신뢰를 쌓는 것이 무엇보다 중요하다고 강조한다. 복잡하게 얽힌 네트워크처럼 다양한 기관과 기업들의 협조체계를 구축함으로써 사고예방과 대응이 빨라진 배경에는 대응지원팀의 정보 네트워크 구축이 큰 몫을 담당해 온 셈이다.

국제공조, 미래 위한 투자

자사의 네트워크와 시스템을 보호하는 것만으로 외부 공격에 대한 충분한 대비가 될 수 없는 것처럼 국내 민간 사업자와 유관기관과의 협조체계 구축만으로는 침해사고 대응에 한계가 있을 수밖에 없다. 때문에 대응지원팀은 해외로의 정보 네트워크 구축 사업에도 적극적이다. 국제침해사고대응팀협의회(FIRST) 활동을 비롯해, APCERT 등 해외 침해사고 대응기구에서 대응지원팀은 KISA를 대표해 활동함으로써 보다 다양한 정보 네트워크를 구축하고 있다. "아시아·태평양 지역 14개국이 모인 APCERT에서는 회원국 간의 국제 침해사고 모의훈련이 진행되고 있을 만큼 긴밀한 협력이 이뤄지고 있죠. 물론 일부 국가를 제외하고는 KISC 수준의 기술과 정보를 가진 기관은 찾기 어려워요. 덕분에 KISA가 대부분의 활동을 주도하고 있는 상황이죠"라는 허 팀장은 KISC가 매년 다른 아시아 국가기관의 벤치마킹 대상이 되고, 또 기술 노하우를 전달하고 있다고 덧붙인다.

그런데 KISA가 타 아시아 국가들에게 기술을 전수하고, 교육하는 가장 큰 이유는 무엇일까. "미래를 위한 투자라고 봐요. 네트워크로 연결된 세계에서 국경은 의미가 없어요. 정보보호에 취약한 국가들은 우리의 네트워크를 위협하는 위협요소가 될 수 있고, 또 이들과의 공조를 통해 수집되는 정보 역시 유용하기기 때문이죠"라는 허 팀장은 그렇다고 투자만 이뤄지는 것은 아니란다. 지난해부터 중국과 악성 봇 C&C 서버 정보 교환을 비롯해, 이들이 계획하는 국가 간 정보교류가 서서히 빛을 볼 예정이라고 설명한다. 이제 이들이 닦아놓은 공조와 협력체제가 어떤 모습으로 펼쳐지게 될지 지켜보는 일만 남았다. S

"초기에는 우려도 있었지만 지금은 정보를 공유하는 기업 및 기관들의 생각이 달라졌어요. KISC가 수집하는 정보가 침해사고를 예방하고 신속하게 대응하기 위해 필수적이라는 사실이 알려지면서 자발적인 공조가 이뤄지고 있는 것이죠." 인터넷침해사고대응지원센터 대응지원팀 허창열 팀장은 국내 협력체계 뿐만 아니라, 해외 여러 국가와 기관들과의 협력체계를 통해 다양한 정보 네트워크를 구축하고 있다고 강조한다.