봇넷 확산, 2008년 사이버 범죄의 최대 화두될 것


Mirko Manske(BKA)

지난해 등장한 정보보호 관련 사건의 특징 중 하나는 금전적 이익을 목적으로 한 사이버 범죄가 본격적으로 등장했다는 점이다. 이런 유형의 범죄는 비단 국내뿐만이 아니라, 미국, 유럽 등 전 세계적인 관심사로 떠올랐다. 이런 의미에서 지난 10월 경찰청 주최로 개최된 '국제 사이버테러 대응 공동심포지움' 참석차 한국을 방문한 독일 BKA 소속 Mirko Manske로부터 독일 및 EU 지역의 사이버 범죄 현황에 대한 의견을 들어봤다. Mirko Manske는 독일 연방 범죄 경찰국(Bundeskr-iminalant, BKA) 소속으로 지난 2006년부터 국내 경찰청 사이버테러대응센터에 해당하는 BKA 내 National High Tech Crime Unit(NHTCU)의 정보분석 및 수집 전문가로 활동하고 있다.

정보보호뉴스 취재팀

한국에는 침해사고 및 사이버 범죄에 대응하기 위해 KISA, NCSC, CTRC 등과 같은 전문 기관이 있다. 독일의 사이버 공격 및 범죄에 대한 대응 기관 및 시스템은 어떻게 구축되어 있나.

독일은 기본적으로 자치권을 갖고 있는 16개주로 구성된 연방 법제 시스템을 갖추고 있으며, 각각의 주는 수백 개의 지역 경찰당국으로 구성된 경찰병력을 갖고 있다. 일반적으로 지역 경찰당국은 어떤 형태의 범죄에도 대응해야할 책임이 있고, 첨단 기술범죄 또한 이에 해당된다. 여기에 연방정부 내 연방경찰국(BKA)이 있는데, 주 경찰국과 BKA에 긴밀하게 협동하며, 첨단기술 범죄를 비롯한 다양한 범죄사례를 조사하고 있다.
아울러, 독일의 주요 시설들(Critical Infrastructures)을 보호하고 발생 가능한 공격에 대응하기 위한 전문 기관인 연방사무국(BSI)이 있으며, 이들은 정보보호를 위한 전문화된 기관이라고 생각하면 된다.

2006년과 2007년 독일에서 발생한 사이버 범죄 사건과 그 피해 규모를 말해 달라.

NHTCU(National High Tech Crime Unit)가 파악한 바에 따르면, 지난 2006년에는 온라인뱅킹 정보 및 신용카드 개인정보에 대한 피싱 범죄가 주요 사이버 범죄 형태로 파악됐다. 독일 내 사이버 범죄의 90% 이상이 이 같은 피싱과 관련이 있었고, 2006년 한 해 동안 약 3,500건이 발생해, 사건당 평균 2,000~3,000 유로의 피해를 안겼다. 2007년 유형과 피해규모에 대해서는 정확한 통계가 발표되지는 않았지만, 이보다 높은 수치를 보일 것으로 예상된다.

사이버 범죄 및 침해사고 대응에 있어 큰 문제점 중 하나는 웜이나 바이러스를 만들고 악의적으로 이를 배포하는 범죄자에 대한 체포 비율이 낮다는 것이다. 범죄자들을 잡을 수 있는 가장 좋은 방법이 무엇이라 생각하나.

지난 2년 동안 독일 NHTCU 단독으로 첨단기술 범죄 관련 용의자 16명을 체포했지만 범인체포는 여전히 어려운 문제이라고 생각한다. 사이버 범죄자들이 매우 독창적이고 지능적인 것은 분명한 사실이지만 이에 대응하는 우리 경찰들 역시 이들을 잡기 위해 끊임없는 노력이 필요하다고 본다.

사이버 범죄와 사기사건은 국경을 뛰어 넘고 있으며, 비슷한 범죄사례가 세계 곳곳에서 일어나고 있다. 이는 각 대륙과 국가가 범죄에 공동으로 대응하기 위해 노력해야 한다는 것을 의미하지만 종종 국가 간의 협력이 제대로 이루어지지 않고 있는 것 또한 사실이다. 여기에는 어떠한 문제가 있다고 생각하는가.

우리의 경험상 협동과 공조가 수사 성공의 중요한 요소임을 알 수 있다. 특히 전 세계 국가 간에 강력한 상호 협력관계를 구축하기 위해서 Interpol, Europol 등과 같은 기관의 정보교환에 대한 '기준'을 마련하기 위해 노력하고 있다. 협력을 위해서는 사람, 기관, 두 가지 모두가 필수적이다. 이것이 우리가 2007년 10월 서울에서 열린 '사이버테러 대응 국제 심포지움'에 참가한 이유이기도 하다. 실제로 우리는 그 자리에서 실력있고 열성적인 사람들을 다수 만났으며 이런 만남이 차후에 유용하게 작용할 수 있을 것이라고 믿고 있다.

최근 한국에서는 사이버 공간에서의 범죄에 대응하고 개인정보를 보호하기 위한 법률을 정비하는 중이다. 새로운 사이버 법 체계를 구축하는데 필요한 조언을 해줄 수 있는가.

독일의 법제는 사이버 범죄를 예방하고 대처하는데 적합한 수단이기는 하지만 성문법이 아닌 추상적인 체계라는 점에서 조언은 부적절하다고 본다. 다만 기술로 인해 우리의 세계가 끊임없이 바뀌고 있고, 법률 역시 매순간 바뀔 필요가 있다는 점을 유념한다면 오히려 특별히 사이버 공간을 위한 법률은 필요하지 않다고 생각한다.

독일에서 일어난 사이버 범죄 중 기억에 남는 사건과 사건의 조사과정 및 결과를 간략하게 소개해주길 바란다.

지난 2007년 9월, 18개월 동안 BKA와 검찰의 합동수사 끝에 독일, 러시아, 우크라이나인 10여명으로 구성된 국제적인 피싱 조직을 검거한 적이 있다. 이들은 트로이안이 첨부된 메일을 Deusche Telekom AG, eBay Internation AG 등 유명 기업 및 기관의 메일인 것처럼 속여 발송했으며, 메일을 열어보는 순간 피해자의 PC를 바이러스에 감염시켰다. 이후 감염된 PC에서 빼낸 피해자의 은행정보 등을 통해 피해자들의 돈을 갈취해 Financial Agents라고 불리는 중개자들과 짜고 돈을 해외 계좌로 송금하는 방법을 이용했다. 물론 최종적으로 이 돈은 용의자들이 독일 내 ATM을 이용해 인출했다.
특히, 이 사건은 막대한 이익을 위해 인터넷을 사용하는 범죄가 급격히 증가하고 있다는 것을 다시 한번 보여준 것으로, 범죄 집단이 점차 전문화, 국제화돼 가고 있으며 사이버 범죄 관련 법집행 당국은 논리적, 재정적, 인적 노력을 강화해 지속적으로 대응해야 한다는 것을 알려준 사례이다. 단순히 사이버 범죄를 조사하는데 그쳐서는 안 되며, 사법부와 검찰의 긴밀한 협동, 그리고 기술발전을 통해 지속적으로 정보를 업데이트 하는 것이 필요하다.

2008년 가장 위협적인 사이버 범죄는 무엇이 될 것이라고 생각하나.

봇넷의 세계적인 확산과 그로 인한 범죄 활동이 왕성해질 것이라고 확신한다. 봇넷은 범죄집단의 기반이 될 가능성이 크며, 이미 많은 범죄자들이 봇넷을 기반으로 DDoSing, Spamming, Malware의 확산 등을 통해 막대한 이득을 취하고 있다. S