

컴퓨터망 해커에 의한 산업 기밀 유출 방지 대책 시급

황의창(특허청 상표심사2과장)

80년대 이후 미국, 유럽 등에서 신종 범죄로 등장하기 시작한 컴퓨터 해커 범죄는 컴퓨터에 뛰어난 실력을 가진 해커들이 중요 컴퓨터망에 침입하여 정보를 탐지해가는 신종 첨단기술 범죄이다.

그동안 제한적으로만 활용되어 왔던 국제통신전산망 인터넷 가입이 올해부터 자유화됨으로서 컴퓨터 해킹의 발생 가능성이 그 어느 해 보다도 높아가고 있는 가운데 최근 국내 통신 이용자에 의한 유럽 암 연구센터 침입이나 영국의 16세세의 컴퓨터 해커가 2차례나 미공군 컴퓨터망에 침입하여 한국원자력연구소와 미국 항공우주국 등에 수록되어 있는 과학기술 및 군사정보를 복사한 후 미국 뉴욕에 위치한 롬 항공개발센터의 컴퓨터에 옮겨 놓은 사건이라든가 스위스 해커가 유럽 암센터를 경유, 우리나라의 콘트롤 데이터 코리아 전산시스템에 24차례나 침입한 사실 등 외국통신 이용자에 의한 컴퓨터 침입사실이 밝혀지고 있어(워싱턴타임지 3일자) 우리의 허술한 정보관리에 일대 경종이 되어 인터넷 등 국제전산망 가입 업체들이 바짝 긴장하는 등 컴퓨터 통신망의 보안관리에 초

비상이 걸려 국제적인 해커들에 대한 대책마련이 시급한 실정이다.

그러나 국내연구소의 전산관리자 중에는 아직 해커를 막을 만한 능력있는 전문가가 거의 없는 실정이고 고작 해커가 주로 이용하고 있는 유닉스 시스템에 중요한 자료를 올려 놓지 않는 정도이다.

그나마 대형컴퓨터들은 암호화나만 알아내면 얼마든지 접속할 수 있는 데 이 정도는 대학에서 전산학을 전공한 사람이면 누구나 풀어낼 수 있는 직업이라고 이분야 전문가는 말하고 있다.

이에 반해 고속정보화의 진행에 따라 세계 최대의 컴퓨터 통신망인 인터넷 등 국제적인 통신망과의 연결은 날로 늘어나 이제는 연구소나 대학 뿐만 아니라 일반인, 기업, 공공기관 할 것 없이 빠른 속도로 통신망에 접속하여 해커들의 활동 공간은 계속 넓어져 가고 있다.

이와 같은 컴퓨터 통신망에 의한 원격조작 방법에 의해 컴퓨터 시설에 침입하여 정보를 빼내거나 파괴하는 것은 비록 어제 오늘의 일만은 아니고 이미 10여년전부터 유럽, 미국 등지에서 성행해 온 신종범죄로 최근 인터넷 등 세계를 하나로

묶는 통신망이 발전하면서 더욱 늘어나고 있는 추세이다.

서독청년 다섯명이 미국의 육·해군의 데이터베이스에서 군사정보를 빼내어 구소련 KGB에 팔아 넘긴 사건은 컴퓨터 해커에 의한 대표적인 범죄로 알려지고 있다.

'89년에 일어난 웜(worm)사건은 전자우편 프로그램의 허점을 이용하여 사람이 아닌 「웜」이라는 프로그램이 통신망을 돌아다니면서 컴퓨터 시스템의 성능을 급격히 떨어뜨린 전형적인 「해킹」사건이며 '90년에는 호주의 해커가 국제통신망을 통해 하버드대학 연구소 컴퓨터에 침입하여 컴퓨터를 조작하다가 체포되었던 사건도 있었다.

국내에서도 '92년 7월 서울대 교육전산망에 해커가 침입하여 성적자료, 학술자료, 학사일정 등이 수록된 정보를 모조리 파괴하여 전산망 가동이 10여 시간이나 마비되었던 사건이 있었는가 하면 '93년 2월에는 한 재수생이 정권 인수팀을 사칭하여 컴퓨터로 금융기관의 온라인망 구조를 탐지하여 휴면계좌의 예금을 인출하려던 사건 등이 잇따라 일어나고 있다.

이러한 해커의 침입을 방지하기

위하여 다음과 같은 컴퓨터 통신망 보안관리 대책을 마련하여 시행하는 일이 필요하다.

첫째, 컴퓨터 통신망 시설의 이용은 반드시 암호를 사용하되 여러 가지 암호를 두고 수시로 바꿔 사용하며 사용자에 대한 별도의 로깅과 일(사용자일지)을 남겨 수시로 검사하고 대형컴퓨터의 시스템에 접속한 사용자명(ID)과 사용기간, 어떤 작업을 했는지 작업명과 작업내용을 구체적으로 기록해 두는 등 사용자명과 사용내용 및 비밀번호의 보안을 철저히 한다.

둘째, 교환장치를 이용한 보안이

나 선진국의 첨단 보안장치를 사용하는 등의 시스템 보안장치에 각별한 주의를 기울인다.

셋째, 자료의 성격에 따라 일반 정보와 비밀정보를 분류하여 이에 따른 시스템 접근을 제한하는 관리 체계를 마련한다.

넷째, 컴퓨터 보안에 대한 중요성을 인식하고 이에 대처해 나갈 수 있는 전문인력을 양성한다.

이상과 같은 정보통신망에 수록된 정보자료에 관한 업계의 보안대책 뿐만 아니라 정부에서도 산업기밀 유출방지를 위한 기반구축을 위해 컴퓨터 보안장치의 의무화와 해

커범죄를 처벌할 수 있는 법률의 제정, 현재 GNP의 2%정도에 머물고 있는 기술투자 규모의 확대 및 기업이 필요로 한 기술을 언제든지 어디서나 손쉽게 들여와 사용할 수 있도록 하는 등의 법적, 제도적 장치의 마련이 함께 이루어져야 할 것이다.

이와 같이 컴퓨터 해킹 방지는 어느 특정 개인이나 기업, 정부만의 일이 아니라 개인, 기업, 정부가 다 함께 총력전 체제로 대응해 나아갈 때 비로소 소기의 성과를 거둘 수 있을 것이다.

용어해설

Projector

디스플레이 하고자 하는 내용을 기기 자체적(TV 튜너 내장) 또는 외부기기(VTR, LDP, 캠코더, 컴퓨터 등)와 연결하여 내부의 소형(3~10인치) CRT나 LCD를 이용하여 대형화면(20~200인치)으로 볼 수 있게 투자하는 영상기기.

MNP(Microcom Networking Protocol)

MNP는 모뎀 제작회사인 마이크로콤(Microcom)사에서 제창한 하드웨어 지향의 프로토콜로써, 보통 모뎀의 펌웨어(firmware)에 기억시킨다.

MNP탑재 모뎀과 PC사이에서는 보통의 비동기식(RS-232C) 통신이 이루어지는 반면에 오류검출과 재전송처리, 데이터압축 등을 모뎀이 자동적으로 수행해 준다.

CTS

기존의 활판을 이용한 제작 방식에서 벗어난 신문 정보의 가공 및 제작방법을 전산 처리화한 것이 CTS(Computerized Typesetting System)라고 할 수 있다.

이에는 기사 입력시스템, 면편집시스템, 화상처리시스템(사진, 지문제목, 컷 등), 종합관리 시스템 및 데이터 베이스 등으로 구성된다.

Multimedia

컴퓨터와 인간 혹은 인간과 인간 사이에 메시지(텍스트, 그래픽, 영상, 오디오, 비디오)를 효율적으로 전달하고 가장 적당한 수준의 적합한 매체를 선택하는 기술.