컴퓨터 범죄와 그 대비책

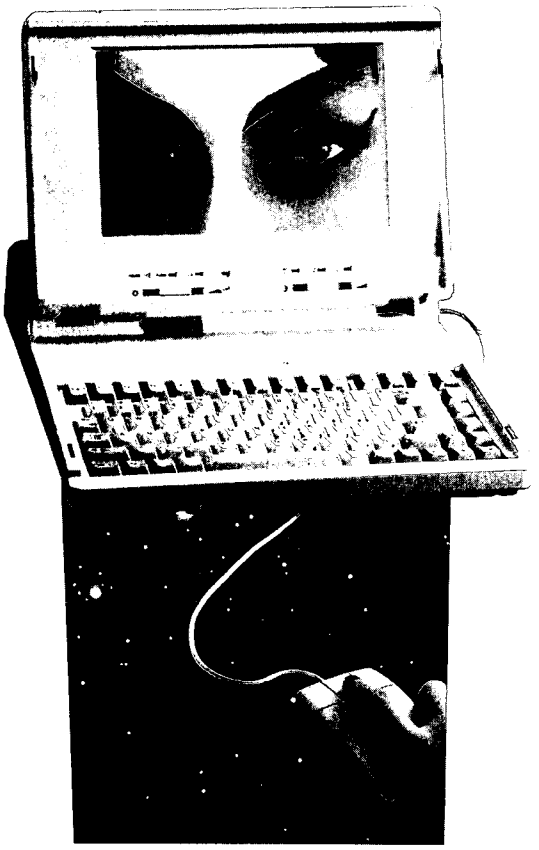
How to Block the computer's Crime?

1. 서 론

정보화의 물결은 가속도가 붙어 더욱 도도히 흐르고 있어 시대의 변혁기를 겪고 있는 오늘의 세대에게는 오히려 혼돈마저 가져다 주고 있다. 컴퓨터 문맹이라는 말이 이를 잘 나타내주고 있다. 정보기기를 비롯한 가전제품에 이르기까지 그 조작방법을 더욱 단순하면서도 간단하게 하여 자유자재로 이용할 수 있도록 개선되어가고 있다.

이는 정보화사회를 살아가는 우리들에게 보다 그 편리성을 손쉽게 누릴 수 있게 함일 것이다.

정보화사회의 최종골은 아직 그 누구도 예측을 불허하는 무한함을 향해 무섭게달려만 가고 있는 것이다. 그러나 항상 양지가 있으면 음지가 있게 마련이니 정보화의 사회에도 여러 가지 역기능과 부작용들이 따르고 있어 오늘날의 또 하나의 문제점으로 대두되고 있는 것이다. 이미 알려진 것으로 전자기기들을 사용할 때 발생되는 전자파의 피해나 장시간 키보드를 두드림으로써 일어나는 관절염, 텔레비전이나 컴퓨터 화면을 장시간 봄으로 인한 시력의 약화 등 물리적인 역기능과 컴퓨터 단말기나 비디오게임과같은 것만 상대함으로서 타인과 협조를 모르고 이기심만 조성되며 인간미가 없어지는 등 정신적인 역기능이 있고, 조작상의 실수로 그릇된 자료를 입력하거나 프로그램의 에러로 잘못 처리된 자료 때문에 일어나는 혼란과 컴퓨터 관련인들이 고의로 범하는 컴퓨터 범죄등이 있다. 그 중에서도 가장 심각한



것이 컴퓨터 범죄라고 생각한다. 직접 또는 간접적으로 입는 피해가 큼에도 이를 예방하기가 어렵다는데 문제가 있는 것이다. 다른 역기능들은 예측이 가능하여 그 피해를 제거하거나 줄일 수 있는 방법의 연구가 가능하지만 컴퓨터범죄만은 그것이 어렵거나 거의 불가능 하기 때문이다. 그러므로 여기서 컴퓨터범죄의 유형과 특징, 그리고 최근 달라진 컴퓨터범죄 분류기준과 그간에 우리나라에서 발생한 컴퓨터범죄의 현황을 살펴보고 제한적이나마 그 방지대책을 찾아보고자 한다.

2. 컴퓨터범죄의 유형과 특징

가. 컴퓨터범죄의 개념

컴퓨터범죄의 개념에 대하여 여러 학자들이 많은 연구를 해왔으나 아직까지 통설은 성립되지 않고 있다. 그간 주장된 학설을 보면

(1) 부정설

컴퓨터라는 것은 인류의 생활향상을 위하여 나온 것이며 범죄와 관련 있는 범죄의 개념이 아니므로 컴퓨터범죄라는 용어 자체를 사용하는 것이 부적절하다는 학설이다.

(2) 광의설

컴퓨터와 관련하여 일어나는 모든 범죄를 전부 컴퓨터범죄라고 한다. 즉, 직접적이든 간접적이든 불문한다. 이 학설은 너무 광범위하며 일반범죄와의 한계가 불분명하며 높은 기술력을 요구하는 컴퓨터범죄의 핵심을 흐리게 할 우려가 있다는 비평을 받는다.

(3) 협의설

컴퓨터를 이용하여 자기 또는 제삼자의 경제적인 이익을 취하게 하는 모든 행위라고 정의하고 있다. 이는 경제성을 강조하여 경제성이 없는 핵커들의 범죄를 빠지게 하는 경우를 범했다는 평을 받고 있다.

나. 컴퓨터범죄의 유형

컴퓨터범죄에 대하여 여러 학자들이 이를 유형별로 분류해보고자 노력해온바 그중 "돈 파커" 박사가 분류한 다음 여섯 가지 분류가 그간 주종을 이루어 왔다.

(1) 조작상의 부정

조작상의 부정은 컴퓨터를 움직이는데 필요한 모든 행위를 포함하는 광의의 조작을 의미한다. 즉, 단순기기조작에서 부터 프로그램작성에 이르기까지의 전체를 포함한다.

이 조작상의 부정은 다시 입력진의 부정과 콘솔상의 부정, 프로그램부정으로 세분된다. 입력상의 부정은 다시 원시서류의 부정과 키인상의 부정으로 나눌 수 있다.

(2) 컴퓨터파괴(사보타지)

컴퓨터파괴는 물리적으로 컴퓨터기기를 파괴하는 행위를 말한다. 컴퓨터기기는 주컴퓨터는 물론 주변기기나 컴퓨터를 운영하는데 필요한 부대장비 및 데이터 통신을 위한 통신장비도 포함된다. 또한 일부학자들은 시스템프로그램 및 컴퓨터를 움직이는데 필수적으로 소요되는 각종 유틸리티까지를 포함시키고 있다.

(3) 데이타의 부정입수

컴퓨터에 의해 처리되는 모든 데이터를 정당한 권한없이 불법으로 입수하는 행위를 말한다. 데이타의 형태는 컴퓨터내부에 있는 전자기록이든 서류상에 기록된 원시서류든 기록매체에 들어있는 것이든 불문하며 처리는 처리가 되어 나온 것이든 처리를 위해 준비중인 서류든 상관하지 않는다. 입수하는 방법 또한 직접 소지하여 반출하든 전선을 통하여 원격지에서 입수하든 관계되지 않는다.

(4) 컴퓨터의 부정사용컴퓨터의 부정사용은 정당한 권한없이 타인의 컴퓨터의 처리능력을 이용하는 것이다.

정당한 권리이라 함은 주어진 범위내를 말하는 것이니 조직의 전산 담당이라 하더라도 공무외에 사적인 일을 위해 사용할 경우 부정사용이 된다.

(5) 신용카드의 부정사용현금지급카드나 은행 신용카드 등 컴퓨터와 관련되어 움직이는 카드를 부정으로 사용하는 것을 말한다. 즉, 카인의 카드를 위조하거나 분실한 것을 습득 또는 절취하여 사용하는 모든 행위를 말한다.

다. 컴퓨터의 특징

컴퓨터범죄는 다른 범죄와 달리 여러 가지의 특징을 갖고 있다.

(1) 행위면에서의 특징

컴퓨터범죄는 그 행위에서 특징이 있다. 첫째 컴퓨터범죄는 한번 작용시켜 놓으면 영속적이고 자동적이다. 둘째, 한번의 행위로 커다란 위력을 발휘한다.

(2) 범행인의 특징

첫째, 대부분 연령이 젊은층이 많다. 둘째, 범죄에 대한 죄책감이 없다. 셋째, 경제적인 이익보다 모험심을 충족시키려는 범죄가 많다. 넷째, 빈곤보다는 향락을 추구하기 위한 경우가 많다. 다섯째, 외부보다 내부인이 많다. 여섯째, 지식인에 의한 화이트칼라범죄이다.

(3) 범죄적인 면의 특징

첫째, 발각이 어렵다. 둘째, 증거를 확보하기가 어렵다. 셋째, 피해액이 크다. 넷째, 업무전체가 마비되는 경우가 많다.

3. 우리 나라 컴퓨터범죄의 현황

가. 발생개황

1973년 소위 에이 아이 아파트 부정추첨사건이라는 컴퓨터범죄가 최초로 발생한 이후 많은 컴퓨터범죄가 발생하였으나 이에 대한 공식통계는 아직까지 산정되지 않고 있어 정확한 숫자의 파악은 불가능한 실정이다. 그나마 몇몇 관심 있는 전문가들이 개별적으로 자료를 수집하여 산출한 통계만 있으며, 각자 그 수집 방법과 기간등에 따라 다소 차이를 보이고 있는 실정이다. 다음은 그간 필자가 개인적으로 수집한 자료를 토대로 산출한 통계인바 1994년6월10일 현재 총 발생 건수는 72건으로 집계되고 있어 연평균 3.4건으로 크게 문제되지 않는 것으로 보이나 70년대에는 극히 소수에 지나지 않았고 80년대에 들어와 금융기관의 업무가 전산화가 이루어짐으로서 증가하였다.

'80년 이후로 보면 평균 5.6건으로 나타나고 있다. 그러나 여기에는 소프트웨어보호법이나 지적소유건에 관한 사건의 숫자는 대부분이 빠져 있는 것이다. 또한 컴퓨터범죄는 금융기관에서 많이 발생하고 있는데 이것이 노출될 경우 신용도의 문제가 야기됨으로 피해액이 적은 경우는 이를 자체 수습하고 발표하지 않음으로 실제사건은 훨씬 더 많을 것으로 추정되고 있다. 미국 스탠포드대학부설 연구소의 컴퓨터범죄 전문가인 "돈 파커"박사는 노출되는 컴퓨터범죄는 불과 3%를 넘지 못할 것이라고 말하고 있는 것을 보면 우리도 여기에서 크게 벗어나지 못할 것으로 생각된다.

나. 발생 기관별 현황

현재까지 발생한 총건수는 72건을 발생 기관별로 분류해보면 다음과 같다.

- ○ 은행 : 49건 전체의 68.5%
- ○ 보험 및 증권 : 3건 4.1%(*금융기관 전체 52건 72%)
- ○ 국가기관 : 5건 6.9%
- ○ 컴퓨터회사 : 4건 5.5%
- ○ 일반회사 : 6건 8.3%

－위에서 보는 바와 같이 현금을 직접 다루는 은행에서의 범법율이 가장 높으면 일반회사는 그 숫자에 비해 범죄율이 낮은 것으로 생각된다.

다. 범죄유형별 현황

총발생 사건을 컴퓨터범죄의 5대 유형으로 분류해 보면 다음과 같다.

- ○ 조작상의 부정 : 57건 79%
  (이중 입력상의 부정조작이 45건(79%),
  프로그램 조작이 12건(21%))
- ○ 데이터 부정 입수 : 9건 12.5%
- ○ 카드 부정 사용 : 6건 10.5%
- ○ 컴퓨터파괴 및 컴퓨터 부정사용은 아직 한 건도 나타난 것이 없다.
  - —이중 컴퓨터 파괴는 실재로 발생되지 않았을 가능성이 높으나 컴퓨터의 부정사용은 발생하였다 하더라도 발각되지 않았거나 발각됐다고 하더라도 이를 문제 삼지 않았을 것으로 생각된다. 또한 법률적인 면에서도 컴퓨터의 부정사용은 아직까지 처벌할 수 있는 법적 근거가 미약하다고 법률전문가들은 말하고 있다.

라. 피해액 현황

컴퓨터범죄는 그 피해액을 숫자로 산출할 수 있는 것과 숫자로의 산출은 불가능하나 실질적인 피해는 막대한 것으로 보인다. 즉, 직접적으로 나타낼 수 있는 것을 학자들은 제1차 피해, 그 범죄로 인하여 연속적으로 일어나는 피해를 제2차 피해, 또한 이로 인하여 야기되는 현상 때문에 발생한 피해를 제3차 피해라고 말하고 있다. 따라서 피해액을 산출하려면 이 세가지를 전부 계산하는 것이 바람직하나 자료수집의 어려움 때문에 아래 내용은 직접적인 피해금액만을 계산한 것이다. 이 직접적인 피해 금액에 대하여도 자료의 불충분으로 일정금액 단위로 분석할 수 없으나 이를 평균해 보면

- ○ 1991년까지 발생한 사건 건당 평균 약 1억원 정도
- ○ 1993년 6월까지 발생한 사건 건당 130억원
- ○ 1994년 6월 현재 발생한 사건 건당 1억 5천만원 위의 자료를 보면
  - —1991년 이전은 은행의 대리급이하의 행원들이 자기자신들의 신분지위에 맞는 금액을 주 범죄대상으로 하였다는 것을 알 수 있으며,
  - —1992년에서 '93년 6월까지는 주로 능력이 있다고 자타가 인정하던 대리급의 중견간부들이 부정에 개입함으로써 그 액수가 백배 이상으로 급등하였으며,
  - —1993년 6월이 후로는 다시 정상적인 수준의 금액으로 돌아온 것을 볼 수 있다.

마. 연령별 현황

- —연령별 현황 역시 1993년 6월 이전까지는 정확한 분석을 할 수 있는 자료가 없어 20대 젊은층이라는 정도의 분석밖에 나올 수가 없었다.
- —1993년 6월 이후 발생한 사건 11건에 관련된 인원 35명을 분석한 결과는 다음과 같다.
- ○ 10대 : 1명 2.9%
- ○ 20대 : 2명 5.7%
- ○ 30대 : 23명 65.7%
- ○ 40대 : 6명 17.1%
- ○ 50대이상 : 3명 8.6%

위의 표에 나타난 것과 같이 30대가 가장 많은 결과를 보여주고 있는데 이는 외국에서는 젊은층 하면 10대와 20대를 말하고 있는데 이 기준에서 본다면 젊은층이라고 보기는 어렵다. 우리는 의외로 30대가 60%이상을 차지하고 있어 그 주류를 이루고 있다. 이와 같은 현상은 조직내에 들어온 보통 5년에서 10년정도 되어 업무처리방법을 충분히 알고 있으며 조직의 분위기 등을 손쉽게 파악할 수 있는점 등을 고려해 볼 때 그 정도의 경력이 필요한 것이 아닌가하는 추측도 가능하게 된다.

－또한 남녀별로 분석도 보면 현재까지 알려진 여성 범죄는 총 6건 정도로서 무시할 수 없는 비율을 점하고 있으며, 최근 1년간의 통계도 11건중 2건에 2명의 여성이 관련되어 있고, 건수 비율로도 18.2%나 차지하고 있어 결코 무시할 수 없는 비율이다.

－또한 여성범법자의 연령을 보면 20대의 초반 보다는 후반이나 30대 중반에 가까운 층이라는 점이다. 이는 어느 정도 업무에 익숙해 있어 직무의 처리절차를 잘 알고 있는 사람이 가능하다는 점과 둘째로 단독으로 범의를 가지기 보다는 외부의 남자가 관련되는 경우가 많다는 점이다.

바. 범죄발생 추세

컴퓨터범죄의 발생추세를 보면 여러 가지의 재미있는 현상을 발견할 수 있다.

(1) 2～3년을 주기로 발생

－1973년 최초 범죄가 발생한 후로 75년까지 3년간은 범죄가 발생하지 않은 것으로 나타났으며, 그후 외환은행등 은행업무의 전산화가 시작된 1976년부터 발생하기 시작하였으나 극소수에 불과했다.

－그후 1973년대 말부터 80년대까지는 거의 주기적이라고 할만큼 2～3년간의 간격을 두고 발생했다. 이는 컴퓨터범죄가 발생하면 언론등에서 거론함으로 인하여 경영자 및 관리자들이 이에 대한 대책을 세우고 관리를 철저히 해서이기 보다는 범죄를 저지르려는 범의가 언론의 영향으로 위축되었기 때문이라고 보는 것이 관련자들의 견해이다. 왜냐하면 사건이 발생하면 어떤 대책이나 제도를 보완하는 것이 아니고 주의를 환기시키는 훈시나 하는 정도에 그치고 있기 때문이다. 이것은 은행 관리자들의 면담에서도 잘 나타나 있다.

(2) 유능한 자의 대담한 범죄

－1991년 이전의 범죄는 대부분 하부나 초급간부들이 소규모로 범행을 해왔으나 1992년부터는 조직내에서 유능하다고 인정받는 중견들이 거액을 사취하는 범죄가 연이어 발생한 것이다. (예 : 국민은행 압구정동지점 사건 250억원 사취사건, 상업은행 명동지점 사건등)

(3) 공무원범죄의 급격증가

국가기관의 전산화는 일찍이 1967년부터 시작되었으나 대부분이 내부의 업무를 처리하는 것으로, 범죄발생이 가능한 요인이 많지 않았음으로 문제가 없었다. 그러나 1980년대에 들어서면서 컴퓨터가 대민 업무에 사용되기 시작하자 범죄발생이 급격히 늘어났다. 이는 현금을 취급하는 우체국이나 철도청업무 등을 비롯하여 토지대장, 주민등록 등을 처리하는 일선 시, 구, 군청, 여권을 발급하는 외무부, 각종 정보를 보유하는 수사기관, 세금을 담당하는 국세청 등 각처에서 여러 가지 형태로 나타나기 시작한 것이다.

(4) 기술수법의 향상

대부분의 사건이 단순조작을 요하는 것들이었으나 최근에 들어서서는 위조된 신용카드를 사용한다던가(범인이 검거되지 않아 본인의 직접위조 여부는 불명하나 위조가능성도 있음)타인의 패스포드를 찾아내려고 노력한 것이나라든가, 아르바이트 학생이 콘트롤 코멘드를 조작하여 타인의 예금을 빼내어 자기의 계좌로 옮긴 것 등 종래에 보기 어려웠던 기법들이 서서히 등장하고 있어 불원간 전문적인 수법의 범죄가 발생할 가능성을 높여주고 있다.

4. 우리 나라 컴퓨터범죄의 특징

가. 기술적인 특징

－현재 노출된 범죄의 현상에서 살펴보면 아

직까지 기술적인 면에서는 주로 단순조작으로 가능한 조작상의 부정수준을 넘지 않고 있다.

-그러나 표면으로 드러나고 있지는 않지만 현실적으로 발생하고 있는 핵커들은 상당수가 잠재하고 있는 것으로 판단되고 있다. 이는 학술연구망에 연결된 각 대학이나 연구소 컴퓨터를 사용하고 있는 사용자들의 입을 통하여 자주 들려오고 있기 때문이다. 그러므로 그 전문가들이 언제든 마음만 먹으면 보다 고도의 기술의 범죄가 발생할 가능성은 충분히 예상할 수 있다.

나. 문화적인 특징

-우리 나라 컴퓨터범죄는 외국처럼 어떤 룰이 잘 지켜지는데서 발생하는 것이 아니고 룰은 있으되 이를 그대로 지키지 않고 인간적인 면으로 대처하는데서 많이 발생한다는데 특징이 있다.

-구미계열의 민족들은 역사적으로 이동하며 생활하던 유목민족의 문화를 가졌으므로 모든 것을 계약이나 규칙에 의해 모든 일을 처리하는데 익숙해져 있으나 처음부터 정착해서 농경생활을 해온 우리 민족은 계약이나 규칙문화에 익숙지 못하고 그보다 인간관계에 더욱 익숙해온 것이다. 따라서 규칙이나 계약보다 인정이 먼저 앞서는 것이다. 이러한 문화적 배경에서 철두철미하게 움직이는 컴퓨터와는 우선 그 정서부터가 맞지 않는다는데 그 원인이 있다고 보겠다. 예를 들면 컴퓨터보안규정에 등에 간부들이 해야할 일들이 규정되어 있으나 이를 자신들이 하지 않고 이를 담당자들에게 전부 위임하는 사례가 허다하다는 것이다.

다. 최고 경영자의 동참

-컴퓨터범죄뿐만 아니지만 범죄행위를 최고경영자가 동참한다는데 특징이 있다. 이는 앞항의 문화적인 면과도 관련이 있으나 그보다도 국민의 윤리의식이 확립되어 있지 못하다는 점을 보여주고 있는 것이다.

-이 경우는 최고 경영자도 그 조직의 이익을 위해서는 어떤 불법도 용인된다는 생각을 가지고 있으며 사회적인 정의를 뒤로하는 윤리의식의 결핍이라고 하겠다. (각 대학의 부정입시조작 및 외환은행 입찰조작, 동아투

금 실명제조작 등)

- 다음으로 문제가 되는 것은 대기업을 비롯한 많은 기업들이 탈세를 위한 이중 경리처리와 뇌물 등에 사용할 부정적인 비자금의 관리 등을 위하여 종래에 사용하던 비밀장부 대신에 개인용 컴퓨터를 사용한다는 점이다. 그 이용 자체는 컴퓨터범죄라고 보기에는 어려우나 컴퓨터를 부정행위의 수단으로 이용한다는 문제점이 있다.

5. 컴퓨터범죄의 변천

가. 개 설

앞에서 살펴본 바와 같이 우리 나라의 컴퓨터범죄도 20여년간 여러 가지 형태로 그 상황이 변천되어 온 것을 단편적이나마 볼 수 있다. 불행하게도 공식적으로 자료를 수집하고 이를 분석할 수 있는 제도가 마련되지 못하여 충분한 분석을 할 수 없다는 것은 안타까운 일이다. 그러나 우리보다 먼저 컴퓨터를 사용한 선진국도 역시 사용하는 측면만을 추구한 나머지 컴퓨터범죄에 대하여는 충분히 대처해 왔다고는 보기에는 부족한 감을 느끼게 하고 있다. 그러나 미국을 비롯한 선진국에서는 일부학자 차원이기는 하나 일찍이 1970년대 초부터 자료를 수집하고 연구에 착수하여 많은 많은 업적을 남겼으며 특히 1990년대에 들어와서는 괄목할만한 성과를 거두고 있다. 즉, 1991년부터 1993년 말까지 3여년에 걸쳐 미국 스탠포드대학 부설 연구소를 주축으로 산·학·관 합동 연구진을 구성하고 그간 발생한 4, 000여건의 사건관계자들을 일일이 찾아가 인터뷰하여 동기에서부터 기술적인 범죄수법에 이르기까지 다양한 자료를 수집 분석하는 성과를 거둔 것이다. 뿐만 아니라 1991년부터 범위를 넓혀 대부분의 선진국들이 참여하는 국제기구인 I-4(International Integrate Informaton Institute)를 창설하여 활동의 폭을 넓히고 있다. 이와 같이 연구가 활발한 것은 이제 컴퓨터범죄가 어느 일개 국가나 기관의 힘만 가지고는 그 예방이 어렵다는데 공감하고 있기 때문이다. 즉, 컴퓨터는 이제 통신과 결합하여 전세계를 하나의 장으로 묶어 놓았으므로 어느 국가의 특정 장소라는 개념이 없어지고 있기 때문이다. 범죄수법도 나라마다 그 나라 문화 등 현실에 따라 다양하게 나타나고 있고 또한 이것을 다른 나라에서 그대로 모방하는 범죄가 계속 늘어가고 있다.

나. 발생범죄 유형의 변천

컴퓨터범죄를 연구하는 학자들은 범죄의 유형분류를 여러 가지로 시도하여 왔는데 그 중에서도 가장 긍정적으로 인정되어 왔던 분류는 스탠포드대학 부설 연구소의 돈파커박사가 분류한 5대 유형 즉, 조작상의 부정, 테이타의 부정입수, 컴퓨터의 파괴, 컴퓨터의 부정사용, 크레디트카드의 부정사용 등으로, 이는 컴퓨터를 활용하는 측면에 기준을 두는 것이다. 1991년 2월 포럼에서 이 범죄행위의 기법을 기준으로 분류하는 쪽으로 바꾸어 발표하게 되었고 세계의 모든 I-4 멤버들에게 그 카피를 송부하기에 이르렀다. 그 분류내용을 보면 크게 7개 그룹으로 대 분류하고 각각 그 밑에 3~4개씩 다시 세분류를 하여 총 26개의 소분류로 나누고 있다.

(1) 외부적인 악용(External Abuses)
  (개) 스파이행위(Visual Spying)
  (내) 오전(Misrepresentation)
  (대) 물리적 쓰레기 줍기(Physical Scavenging)
(2) 하드웨어 악용(Hardware Abuses)
  (개) 도청(Eavesdropping)
  (내) 전파방해(Interference)
  (대) 장비에 물리적 공격이나 모디파이(Pysical Attack on or Modification of Equipment)

(라) 장비의 이동(Pysical Removal of Equipment)

(3) 가장(Masquerading)

(가) 분쟁(Impersonation)

(나) 등에 업고 공격하기(Piggybacking Attack)

(다) 되돌려 공격하기(Playback Attack)

(4) 유해프로그램넣기(Pest Programs)

(가) 트로이목마식공격(Trojan Horse Attack)

(나) 논리폭탄(Logic Bomb)

(다) 악성기생충공격(Malevolent Worm Attack)

(라) 바이러스공격(Virus Attack)

(5) 검분자와 권한자 비켜가기(Bypassing Authentication/Authority)

(가) 들창 만들기 공격(Trapdoor Attack)

(나) 패스워드공격(Password Attack)

(6) 액티브한 리소스 악용(Active Resource Abuses)

(가) 오소리티의 일반적인 악용(General Misuse of Authority)

(나) 자료조작 및 틀린자료입력(Data Manipulation and Fale Data Entry)

(다) 점증적 공격(Incremental Attack)

(라) 서비스의 거부(Denial of Service)

(7) 리소스의 수동적 악용(Passive Resource Abuses)

(가) 공표와 서칭(Browing and Searching)

(나) 추정과 취합(Inference and Aggregation)

(다) 자료의 누출(Data Leakage)

(라) 인액숀을 통한 악용(Misuse Through Inaction)

(마) 차후 악용을 위해 간접적인 사용(Use as an Indirect Aid for Subsequent Abuse)

다. 수법의 변천

컴퓨터범죄의 수법도 컴퓨터의 발전과 비례하여 급속도로 변천되어 왔다. 1960년대말 70년대 초까지에는 컴퓨터자체가 주로 특정목적을 위하여 어느 조직내에서만 사용되었으므로 범죄의 숫자도 극소수였으며 수법 또한 단순한 자료의 누출이나 변경 정도의 단순한 것들이었다. 1970년대 중반에 들어서면서 컴퓨터와 통신이 결합하여 데이터 통신망이 구성되고 은행을 비롯한 금융기관이 온라인제도를 도입하게 되자 이의 약점을 찾아 현금편취를 노리는 각종 범죄가 증가하기 시작하였으니 대표적인 것인 단말기의 부정조작이며 다음이 프로그램 부정조작의 형태로 나타났다. 그후 1980년대 후반부터 보다 많은 업무들이 소위 공중전송망을 사용하게 됨에 따라 이를 이용하는 범죄가 늘어나기 시작하였다. 여기에는 현금을 불법취득하는 단순목적외에 국가간의 비밀이나 회사간의 산업기술에 대한 비밀을 빼 내가는 다양한 목적의 범죄로 확산되기 시작하였다.

최근에는 그 기술적 수법들이 상상을 초월할 정도로 전문화되고 있으니 1993년 가을 미국에서 발생한 은행 현금지급기의 현금인출사건은 그 대표적인 것이라 하겠다. 그 수법은 극히 얇은 플라스틱조각과 같은 IC소자로 만든 전파수신기를 현금지급기 카드 넣는 곳에 투입시켜두고 고객이 현금을 인출할 때 카드를 읽어들이는 기기의 전파와 키보드를 누르면서 발생 전파를 전부 원격지에서 수신하여 고객에 관한 모든 정보를 취득한 후 그 중에서 가장 예금고가 많은 사람의 카드와 동일한 카드를 만들어 이를 이용하여 거액을 인출한 사건이다. 이와 같이 최근에는 전자기기에서 발생하는 각종 전자파를 수신하여 이를 재생 분석하면 완전한 정보를 얻는 기법들이 발전하고 있다고 한다.

6. 방지대책

가. 개 설

컴퓨터범죄는 범법자와 이를 방지하려는 자간의 두뇌전쟁이라고 돈파커는 입버릇처럼 말하고 있다. 따라서 완전한 방지라는 것은 거의 불가능하며 얼마만큼 줄일 수 있느냐에 목표를 두고 있다고 말한다. 이는 컴퓨터범죄는 항상 새로운 기법의 범죄가 발생한 후에나 그런 수법도 가능하겠구나 하고 느끼는 경우가 많다고 한다. 그러므로 방지대책은 대부분 현재까지 발생한 사건을 기준으로 세워질 수밖에 없다고 한다. 그런데 우리 나라에서는 아직까지 여러 면에서 초보단계를 벗어나지 못하고 있는 실정이다. 따라서 우리가 당장 하여야할 대책들을 정리해본다.

나. 사법 행정적인 대책

(1) 법령의 정비

무엇보다도 먼저 컴퓨터범죄가 발생하였을 때 명확하게 처벌할 수 있는 형사법의 정비가 선행되어야 할 것 같다. 87년부터 추진되어온 형법개정은 이유야 어떻든 아직까지 이루어지지 않고 있는 실정이다. 또한 전산업무의 범죄를 방지할 수 있는 각종 규칙과 이를 감시할 수 있는 인적 자원을 키워낼 수 있는 법적 근거 등이 신속히 만들어져야 하겠다.

(2) 보안에 대한 전문기술확보

컴퓨터 시큐리티에 대하여 선진국에서는 그 필요성을 일찍이 실감하고 연구에 전념하고 있고, 많은 제도와 제품들이 나오고 있다. 그러나 우리는 아직까지 극히 일부 대기업에서나 이제 관심을 갖는 정도이다. 그러나 그 대부분이 외국의 제도나 제품을 그대로 들여다가 사용하려하나 우리의 환경과 잘맞지 않아 그 실효성을 얻기는 매우 어려운 실정이다. 그러므로 우리 나라의 모든 제도에 적합한 보안시설 즉, 하드웨어나 소프트웨어가 하루 속히 연구되어야 할 것이다.

(3) 전문 수사요원 및 연구기관의 확보

전항에서 살펴본바와 같이 컴퓨터범죄의 수법은 기술적으로 급변하는 있는 현상이며 이는 언제 우리 나라에도 발생할지 예측할 수 없는 것이다. 그러므로 이에 대한 전문수사요원의 양성 없이는 사건해결이나 공소를 유지할 수 있는 증거를 확보하기가 어려울 것이다. 또한 전문수사요원을 지원할 수 있는 연구기관이나 부서가 있어 국내에서 발생하는 모든 컴퓨터범죄의 자료를 수집 분석하고 이에 대한 예방대책도 제시하여야 할 것이다.

다. 사회문화적인 대책

(1) 컴퓨터에 대한 인식전환 운동

모든 기계문명이 그렇지만 그 대표적인 컴퓨터는 그 룰에 따라서만이 활용이 가능하고 예외는 인정되지 않는 것의 대표적인 기계이다. 따라서 컴퓨터안전과 보안에 대한 규정들은 그대로 철저히 지켜지지 않으면 범죄는 발생할 수 밖에 없는 것이다. 컴퓨터는 만능이 아니고 정해진 규칙대로 움직이는 기계라는 것을 재인식토록 하여야 할 것이다.

(2) 비밀번호 등 보안에 대한 인식제고

일본에서는 경찰이 신용카드나 은행통장의 비밀번호안에 대한 계몽팜플렛을 만들어 사회단체를 통하여 널리 계몽시키고 있다. 우리는 아직까지 은행비밀번호를 현금지급 신청서에 기재하고 있는 웃지 못할 현상이 지금도 계속 이어지고 있다. 적을 때나 창구에 제출할 때 누구나 마음만 먹으면 언제든지 볼 수가 있다. 비밀번호의 누출은 바로 현금을 잃는 것이나 같다는 점을 우리는

바로 인식하여 할 것이다. 또한 비밀번호 제조방법이나 이를 관리하는 방법 등을 사회단체 등을 통하여 널리 계몽하는 것이 시급한 과제라고 하겠다.

(3) 전산종사자의 윤리관 제고

컴퓨터보안을 위한 어떠한 제도나 장치도 내부 전산 전문인에게는 부정을 하는데 아무런 장해가 되지 않는다. 마음만 먹으면 언제나 가공할 범죄를 일으킬 수 있다. 뿐만 아니라 완전에 가까운 증거도 없앨 수도 있다. 따라서 외부인에 의한 침해보다 내부인의 범죄가 더 많이 발생한 것이다. 따라서 이들에 대한 윤리관을 높이지 않는 한 범죄예방은 불가능한 것이다. 그러므로 전산종사자들을 위한 자율단체 등을 통하여 윤리관을 확립시키도록 하고 이에 대한 필요한 교육등을 실시할 수 있도록 정부의 지원이 뒤따라야 할 것이다.

(4) 경영자 및 관리자의 의식전환

많이 나아지기는 하였으나 컴퓨터하면 아직도 전문가의 전유물로 인식하는 관리자들이 많이 있다. 이제 누구나 쉽게 사용이 가능하도록 편리한 컴퓨터제품들이 많이 나오고 있어 이에 대한 인식을 바꾸어 직접 다뤄보는 자세를 가져야 한다는 점이다. 다음으로는 컴퓨터의 효능을 부정에 사용하려는 자세를 버리고 선진국처럼 이제 컴퓨터와 같이 모든 업무의 처리는 규정대로 하여야 한다는 윤리관을 견지하지 않으면 않될 것이다. 최고 경영자가 포함된 컴퓨터범죄는 우리 나라만의 현상으로 국가적 수치라고 아니할 수 없다.

(5) 전산관련인의 인간관계 개선

컴퓨터범죄는 결국 사람에 의해서 이루어지는 것이며 외부인보다 내부인에 의해 저질러지는 경우가 더 많다. 내부인이 범행할 경우 발각이 어려우며 발각되어도 그 증거를 확보하기가 무척 힘들다. 그러므로 컴퓨터범죄를 방치한다는 것은 결국 내부의 전산인을 어떻게 관리하느냐가 핵심이라고 할 수 있다. 내부직원을 관리하는 방법은 인사관리 전문가들의 많은 연구가 있겠지만, 전산인으로서 특이한 몇가지 특성이 있다는 점을 감안하여 행하여야 한다. 첫째, 전산인은 대부분이 정신노동을 하는 노동자이면서 무에서 유를 창조하는 예술인과도 같다. 따라서 정신적인 안정이 없이는 작업의 능률도 오르지 않을 뿐더러 자신이 하는 일에 비해 충분한 대우를 못 받는다고 느끼고 있다. 이는 특히 소프트웨어, 즉 프로그램을 작성하는 사람은 더욱 그렇다. 프로그램의 로직구성은 사무실내에서만 이루어지는 것이 아님으로 잠자는 시간을 제외한 전시간을 쏟아 붓기도 하기 때문이다. 또한 풀리지 않던 로직이 풀렸을 때 그 성취감이란 그들만이 알 수 있는 쾌감이며 자부심이다. 그러나 외부에서는 그것을 알아주지 못하고 다른 직원과 같이 생각함으로 불만을 느끼는 경우가 많다. 지금은 전문회사들이 설립되어 많이 개선되었다고는 하나 아직도 정부관서 등에서 제대로 대우를 받지 못하고 있다. 이들이 자신의 긍지와 보람을 갖고 일할 수 있는 인간관계를 최고 경영자나 고위관리자들은 만들어 주어야 한다.

라. 기술적인 대책

(1) 개설기술적인 대책은 기계실 건물설비에서부터 소소한 자료의 운반과정, 프로그램개발과정의 하자 등 그 범위가 넓어 상세한 언급은 어려우므로 일반에서 이미 많이 실시하고 있는 물리적인면의 시설들에 대하여는 생략하기로 하고 여기서는 가장 많이 발생하는 입력상의 부정과 프로그램상의 부정, 데이타의 부정입수 등에 대하여 주로 기술하고자 한다.

(2) 공통적인 대책조작상의 부정과 관련된 부정에 대한 공통적인 대비책은 다음과 같다.

(개) 사용자 로깅화일의 작성

시스템로깅화일은 제조업체에서 직접 공급하고 있으나 거기에는 구체적인 기록내용이 수록되지도 않을 뿐더러 수록된 내용을 분석하는데도 여러 가지 제약을 받고 있는 실정이다. 따라서 각 사용자가 자기자신의 업무에 적합한 사용자 고유의 로깅화일을 만들어 활용하고 이를 전 직원에게 널리 홍보하여야 한다.

(나) 모니터링 제도의 확립

모니터링제도란 여러 개의 단말기를 하나의 호스트에 연결시켜 사용하는 경우나 개인용 컴퓨터들을 랜(LAN)등 통신선으로 연결시켜 사용하는 경우에 어떤 특정 단말기에서 자기가 감독하는 직원의 단말기에서 하는 일을 모니터링 하여 볼 수 있게 하여 놓는 장치로서 이를 시행함으로서 감독자가 수시로 직원들의 하는 일을 확인할 수 있을 뿐 아니라 직원들에게는 감독자가 항상 자기가 처리하고 있는 일을 보고 있다는 것을 느낌으로서 부정행위를 할 마음을 갖지 못하게 하는 효과가 가져올 수 있는 것이다.

(3) 직원의 보안교육 철저

전산에 종사하는 직원들에게 수시로 보안 교육을 실시하며 보안에 대한 인식을 항상 갖도록 하여야 한다. 여기에는 전산실 출입을 통제하는 수위나 각 사무실이나 컴퓨터기계실을 출입하면서 물품을 공급하거나 폐지를 반출하는 직원에 이르기까지 빠짐없이 실시하여야 한다. 교육내용은 이론보다는 구체적으로 실제 행동에 옮길 것을 주로 하여야 한다. 예를 들면 단말기를 다루는 직원은 자리를 뜰 경우 반드시 단말기를 로그-오프시켜야 한다던가, 출입구 경비원은 직원이나 간부의 이름을 대고 만나러 들어간다고 하여 그냥 통과시켜서는 안된다든가 하는 등과 같다.

(4) 입력상의 부정방지책

(개) 원시서류와 처리결과를 수시 대조 비교하여 모순점을 발견.

(나) 단말기 조작원은 이석할 경우 반드시 단말기의 전원을 끄도록 한다.

(다) 주요한 자료의 입력시는 상호 크로스체크하는 프로그램을 만들어 운용하여야 한다.

(라) 사용자 로깅화일상에 감사시 추적이 용이토록 포맷설계를 하여야 한다.

(마) 감독자는 수시로 모니터링을 실시 하여야 한다.

(5) 프로그램 부정에 대한 대책

(개) 중요한 프로그램은 자체개발 할 것

(나) 용역 개발시는 정확한 스펙을 작성하여 검수시 일일이 대조할 것

(다) 메이커나 프로그램 공급자 측이 매인터넌스할 때는 반드시 입회하고 작업내용을 확인할 것.

(라) 하드웨어 고장시, 컴퓨터의 병력을 기록한 카트리지 테이프나 디스켓을 반출할시는 그 내용을 확인하고 내보낼 것.

(마) 중요프로그램은 이에 상응하는 검사용 프로그램을 만들어 수시로 이를 돌려 프로그램의 부정 변경여부를 확인할 것.

(배) 프로그램 담당자들의 신상변동에 유의할 것.

(사) 전산감사를 철저히 실시할 것.

(6) 데이타 부정입수에 대한 대책

(가) 패스워드관리에 철저히 하여 패스워드는 가능하면 자리수를 많이 하는 것이 효과적이며, 자신의 신상주위의 번호, 추측이 가능하거나 추리를 하면 알 수 있는 번호를 피하여야 함.

(나) 중요한 화일은 패스워드를 중복으로 부여할 것.

(다) 중요한 화일은 암호화하여 보관할 것.

(라) 중요 자료를 다루는 기계실은 전파차단 장치를 할 것.

(마) 각종 통신선은 도청 가능성을 검토하고 보완할 것.

(바) 중요한 자료는 무선통신망이나 위성통신망으로 구성된 선로를 이용하지 말 것.

7. 결 론

컴퓨터범죄에 대하여는 현재까지 전산인 일부에서 하나의 흥미꺼리 대상으로만 생각해온 정도이며, 이에 심각성을 아직 느끼지 못하고 있는 것 같다. 그러나 급속히 몰아닥치고 있는 정보화의 물결속에 이미 우리는 원하지 않든 휩쓸려 들어간 것이다. 따라서 그 역기능인 컴퓨터범죄도 직접 우리 주변에 기생하고 있으며.결코 남의 일이 아닌 것을 인식하여야 한다. 우리는 근 반세기에 가까운 시간을 남북대치하에서 군사적인 영향을 많이 받고 살아왔다. 따라서 보안하면 비밀을 생각하게 되고 비밀하면 바로 1급비밀 2급비밀 하는 것들만 생각하게 된다. 그러나 정보화사회에서는 모아진 모든 데이타 화일은 전부 특급비밀이 될 수 있다는 점을 인식하여야 한다. 이는 모아진 정보를 가공하면 상상할 수 없는 정보들이 산출될 수 있기 때문이다. 우리는 아직까지 산업정보의 해외누출에 대한 걱정은 크게 하지 않았던 것이 사실이다. 이는 첫째로 우리의 산업정보가 외국에서 탐낼 만큼 가치 있는 것이 없기도 하였지만, 컴퓨터에 수록된 자료들은 대부분 회사나 그룹내부에서 전용통신망을 통하여 이용되었음으로 외부에 누출될 가능성이 거의 없었기 때문이다. 그러나 1990년대에 들어서면서 우리의 환경은 급변하고 있다. 즉, 우리의 기술력이 일부나마 선진국수준을 능가하는 수준을 나타내기 시작을 하자 외국에서 이를 눈독들이게 되었고, 전산 환경도 국내에서는 공공통신망을 공동으로 활용하게 되었으며 국제적으로도 위성통신망을 통한 국제네트워크에 가입되어 많은 데이타가 이미 교류되고 있다. 이러한 현상은 앞으로 급속도로 늘어갈 것이다. 따라서 그만큼 외국으로부터 핵커들에 의한 데이타의 침공은 더욱 늘어날 것으로 예상되고 있어 결코 안심하고 있을 때는 지난 것이다. DB

(이 글은 한국정보시스템감사인 협회에서 주최한 컴퓨터범죄와 프라이버시 보호에 대한 강연 및 토론회의 노연후 대검찰청 전산실장의 글을 옮긴 것이다.)