시스템 보안을 무력화 시키는 전산관리자의 시스템 침해 행위 연구

류경하* · 박대우**

*호서대학교 벤처전문대학원

To Neutralize the Security Systems, Infringement Actions by the Administrator on the Computer Networks

kyong-ha Roo* · Dea-Woo Park**

*Hoseo Graduate School of Venture

E-mail : freejeus@gmail.com · prof1@paran.com

요 약

본 논문은 이 세상에 존재하는 어떤 종류의 보안시스템도 시스템 접근권한을 가진 전산 담당자의 시스템 침해 행위를 막아내기란 어려운 일이라는 점을 되새기고 전산 담당자의 침해 행위 사례와 그로인한 피해의 정도 등 심각성을 재조명하고 나아가 기술적 보안조치의 한계선상에 있는 전산 담당자의 권한 관리와 기술적 조치를 넘어 인적관리를 통한 침해예방 방안에 대해 나름의 대안을 찾아 보고자 한다.

ABSTRACT

In this paper, to remind ourselves that exist in the world what kind of security system is also difficult to defend a system with computerized access system representative of infringement that, Computerized personnel act of infringement cases, and thus the extent of the damage and the severity Revisited, Furthermore, technical measures beyond the limits of the technical security measures in line computerized rights management representative and for infringement prevention measures in Human Resource Management through its own alternative to find.

키워드

system trespassing, database, confidential business information, information network system, access right

Ⅰ. 서 론

해킹 피해 건수는 그림 1과 같이 매년 지속적이면서도 무시할 수 없는 수준을 유지해 오고 있따. 해킹에 따른 피해 역시 규모를 가늠할 수 없을 정도로 심각한 수준으로 국내는 물론 전 세계적으로도 해킹에 따른 피해와 구제 및 방지대책에 부심하고 있는 실정이다.

DDoS(Distributed Denial of Service) 공격, 바이러스 감염, 백도어 설치 등 각종 유형의 전산망 침해사고가 빈발하고 있다.

그러나 첨단 네트워크 및 컴퓨터 보안 시스템

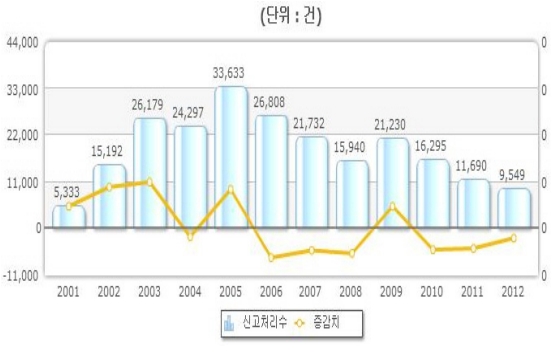

그림 1. 해킹신고 접수현황(출처:KISA 2012)

을 갖추었다 하더라도 최종적으로는 사람의 관리를 배제할 수 없는 것이고, 그렇다면 무엇보다 시스템 관리자에 의한 보안 침해의 예방 시스템 구축과 교육이 절실하다 아니할 수 없을 것이다. 특히 정보통신과 보안망을 취급하는 전산 담당자에 의한 시스템 침입 데이터 베이스 위변조와 유출, 영업비밀 침해 등의 관리적 보안으로 인한 사고가 계속하여 발생하고 있다.

따라서 본 논문에서는 보안망을 무력화 시킬 수 있는 관리적 보안 요소에 의한 전산담당자로 인한 피해요소를 분석하고, 해킹 피해 현황에 대해 개괄적으로 살펴볼 것이며, DB접근권한 보유자에 의한 침해사고 유형을 사례를 통해 연구하고, 시스템 관리자의 침해 행위와 2차 피해와 정통망법·개인정보보호법에 따른 시스템 관리자의 동종수법 침해 행위 연구를 통해 전산담당자에 대한 보안 분석 및 대책을 연구한다.

Ⅱ. 관련연구

2.1 정보통신망이용촉진및정보보호등에관한법률

정보통신망이용촉진및정보보호등에관한법률(법률 제110485호, 시행 2012. 9. 16)에서는 제48조 (정보통신망침해행위 등의 금지)와 제49조 (비밀 등의 보호) 조문을 통해 정당한 접근권한 없는자와 접근권한을 초과한 정보통신망 침해(단순 침입, 데이터 또는 프로그램 등을 훼손, 멸실, 변경, 위조, 바이러스, 도용 등) 행위를 규제하고 있으며,

법정형은

- 제71조 제11호(제49조, 제48조 제2,3항):5년 이하 징역, 5천만원 이하 벌금
- 제72조 제1항 제1호(제48조 제1항, 제49조의2 제1항):3년 이하 징역, 3천만원 이하 벌금에 처하도록 규정하고 있다.

2.2 개인정보보호법

개인정보보호법(법률 제10465호, 시행 2012. 3. 30)에서는 제59조 (금지행위)와 제60조 (비밀유지 등) 조문을 통해 업무상 알게 된 개인정보의 누설과 권한 없이 다른 사람이 이용하도록 제공하는 행위, 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조, 유출한 행위의 규제와 비밀유지 의무를 규정하고 있으며,

법정형은

- 제71조(제59조 제2,3호):5년 이하 징역, 5천만원 이하 벌금
- 제72조(제59조 제1호, 제60조):3년 이하 징역, 3천만원 이하 벌금에 처하도록 규정하고 있다.

2.3 관련 동향 연구(DB 침해사고)

해킹 사건 유형 중 DB 침해 관련 사고로는 네이트온 회원정보 유출, 옥션 회원정보 유출, 농협 등등의 사례가 이미 사회적 이슈가 되었었고 그에 따른 피해는 아직도 현재 진행형으로 근본적인 피해 구제의 방법이 없는 실정으로 알려지지 않은 DB 침해 사고가 알려진 것에 비해 결코 작지 않을 것으로 추정된다.

그림 2. 전문 해커 조직 적발 방송(출처:2003, 11. 19 YTN)

그림 2는 2003년 11월 본 논문 작성자가 직접 수사하였던 사례로 '국세청' 등 공공기관과 병원, 인터넷 쇼핑몰 등 90곳의 인터넷 사이트를 해킹한 전문 해커그룹 검거 관련 YTN 기사이며, 그림 3에서 보는 바와 같이 지금도 누군가가 다수의 고객정보를 저장, 관리하고 있는 공공기관 및 공기업, 사기업을 불문하고 해킹 공격을 통한 개인정보 침해 행위를 꾸준하게 시도하고 있어 지속적인 보안강화 노력이 요구된다.

구분	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월
단순침입시도	202	184	159	106	206	394	-	-	-	-	-	-
기타해킹	233	307	415	515	488	796	-	-	-	-	-	-
스캠릴레이	429	395	474	621	693	598	-	-	-	-	-	-
피싱경유지	36	37	38	39	37	34	-	-	-	-	-	-
홈페이지변조	610	287	616	138	110	352	-	-	-	-	-	-
합계	1,510	1,210	1,702	1,419	1,534	2,174	-	-	-	-	-	-

그림 3. 2012년 월별(1~6월) 해킹신고 처리 구분(출처:KISA 2012)

Ⅲ. DB 접근권한 보유자의 침해(사례)

3.1 사건개요

○○생명보험 전산데이터 관리 및 시스템개발 담당자인 C씨는 보험대리점을 운영하던 자신의 배우자 TM(텔레마케팅) 영업에 사용할 목적으로 자신이 관리하던 ○○생명보험 DB시스템에 접근하여 TM고객 정보 141만건(약 35억원 상당)을 유출, 정보통신망 침해 및 영업비밀(개인정보) 유출

로 구속되었다.

3.2 판결 및 형량 분석

당사자 및 변호인은 피해 회사의 전산망에 정당한 접근권한이 있었고, 허용된 접근권한에 기하여 전산망에 접근하였다고 주장하였으나, 재판부는 '허용받은 접근권한을 초과한 전산망 침입'이라 판시하였다.,

정보통신망이용및정보보호등에관한법률위반과 부정경쟁방지및영업비밀보호에관한법률위반이 인정되었으나 초범이라는 점을 감안하여 징역1년, 집행유예 2년을 선고(2008고합4 가. 업무상배임, 나. 부정경쟁방지 및 영업비밀보호에 관한 법률위반으로 판시하였다. 정보통신망이용촉진및정보보호등에관한법률위반(정보통신망침해 등) - 2008. 3. 7. 서울중앙지방법원, 2008노743-2008. 7. 10. 서울고등법원 항소 기각)

3.3 집행유예 기간 경과

2010. 7. 9. 집행유예 기간 2년 경과되었다(확정일에 따라 차이가 있을 수 있음).

Ⅳ. 시스템 관리자의 침해 행위와2차 피해(집행유예 기간 경과 후)

4.1 사건개요

1차 침해 행위에 따른 법원의 집행유예 선고 기간이 경과된 이후 시점인 2011. 2월경 1차 침해 당시 확보하였던 ○○생명보험 TM고객 정보 141만건을 복사하여 별도로 보관해 두었던 것을 재활용하여 보험대리점을 운영하던 동업자와 함께 TM영업에 재사용하다가 적발되어 두 번째 구속되었다.

4.2 판결 및 형량 분석

동종 범죄사실로 집행유예를 받은 바 있음에도 자중하지 아니한 채 기존에 취득하였던 영업비밀(TM고객 정보)를 활용한 점으로 미루어 엄중한 처벌이 마땅하나 잘못을 깊이 뉘우치고 있으며, 피해자 회사가 선처를 바라고 있는 점을 참작하여 징역 10월 선고(2011고단812 부정경쟁방지 및 영업비밀보호에 관한 법률위반(영업비밀누설 등)으로 구속하였다. - 2012. 5. 1. 서울중앙지방법원, 2012노1588 -2012. 7. 27. 서울중앙지방법원 항소 기각)

Ⅴ. 정통망법·개인정보보호법에 따른 시스템 관리자의 동종수법 침해 행위 연구

5.1 시스템 관리자(전산 담당자) 정의

다중 사용자 컴퓨터 시스템과 통신 시스템의 사용에 대한 관리 책임을 지는 사람 사용자 계정과 암호의 할당, 기밀(보안) 접근 수준의 설정, 기억장치 공간 할당 등의 임무를 수행한다. 또한 무단 접근을 감시하고 바이러스나 트로이 목마 프로그램 등 시스템을 남용하거나 악용하는 프로그램이 시스템에 침입하지 못하도록 방지할 책임이 있다.

5.2 시스템 관리자(전산 담당자)의 역할과 범위

시스템 관리자의 역할은 전산망 이용에 애로사항이 없도록 유지, 보수, 관리하는 업무와 필요 데이터를 요구사항에 맞춰 발췌, 정리, 자료화 하는데 있을 것이고, 시스템 관리자 역할의 범위는 앞에서 열거한 사항과 관련하여 정상적인 업무 한계를 벗어나지 않는데 있다고 할 것이다.

5.3 정통망법·개인정보보호법에 따른 시스템 관리자 행위의 적법성과 위법성 분석

시스템 관리자라는 신분 때문에 금융감독원으로부터 침해 행위가 아니라는 유권해석이 있었고, 여러곳의 수사기관에서도 상담 결과 수사대상이 아니라는 답변이 있어 피해자 회사는 전전긍긍하였으나, 정상적인 접근권한이 부여된 시스템 관리자라고 하더라도 시스템 유지 보수, 관리 등의 허용된 접근권을 초과한 일련의 행위는 '전산망 침입'에 해당한다 할 것이므로 적법과 위법의 경계선을 명확히 구분하여야 할 것이다.

즉, 시스템 관리자 일지라도 허용된 범위내에서 정당한 업무와 관련한 전산망 접근만이 적법한 접근인 것이다.

특히 정보통신과 보안망을 취급하는 전산 담당자에 의한 시스템 침입, 데이터 베이스 위, 변조와 유출, 영업비밀 침해 등의 보안 침해사고는 향후로도 그 피해와 심각성은 우려하지 않을 수 없고, 따라서 후속 조치는 물론 선제적 보안에도 끊임없는 노력을 경주하여야 할 것이다.

Ⅵ. 결론

본 논문에서는 정보통신과 보안망을 취급하는 전산 담당자에 의한 시스템 침입, 데이터 베이스 위, 변조와 유출, 영업비밀 침해 등의 보안 침해사고의 사례와 판결을 연구하였다.

연구 결과 일상적인 유지 및 보수 등의 업무 이외에 데이터를 직접적으로 조작하거나 다운로드 하는 경우에는 복수의 관리자가 참여하여 시스템상으로 복수 인증을 거치도록 하고, 더불어 지위고하를 불문하고 복수의 참여자가 상호 승인을 받았을때에 관련 작업이 가능하도록 하는 등 제도적, 시스템적인 보안정책이 요구된다.

향후 연구에서는 시스템 관리자(전산 담당자)의 관리와 교육 및 전산 시스템적 보안성 강화에 대한 추가 연구가 필요하다.

참고문헌

[1] 국가정보원, “2002 해킹사고 사례분석”
[2] 국가사이버안전센터, “2003년도 사이버 침해사고 사례분석”
[3] 경찰청, “사이버범죄 사범별 수사기법”
[4] 판결, “서울중앙지방법원 2008고합4,” -재판장 판사 이경춘, 문종철, 윤성열
[5] 판결, “서울고등법원 2008노743,” -재판장 판사 조희대, 판사 신헌석, 판사 성충용
[6] 판결, “서울중앙지방법원 2012노1588,” -재판장 판사 이종언, 판사 윤현규, 판사 경정원
[7] 정보통신망이용촉진및정보보호등에관한법률 -법률 제11048호(2012. 9. 16 시행)
[8] 개인정보보호법-법률 제10465호(2012. 3. 30 시행)