論文
3-12-5

EC 환경변화에 대응하기 위한 정보보호에 관한 연구 (A study on the information protection to prepare for the change of EC environment.)

신 영 균*
(Yeong-Gyun Shin)

요 약

EC환경 변화에 대응하기 위한 정보보호 요인은 인터넷 사이버몰 구축과 소비자 보호 규정, 개인정보 보호 및 시스템 보안에 대한 규정이 중요요인으로 제시되었다. 심사기준과 함께 심사방법도 중요요인으로 도출되었으며, 인터넷 사이버몰 평가에 대한 소비자의 관심을 유발시켜 소비자 권익보호에도 기여할 것으로 사료된다. 또한 전자상거래에 대한 기술수준, 기술의 연구 개발, 개발된 기술의 실용화 등도 상당히 의미있는 요인으로 제시되었다.

ABSTRACT

The major factors for the information protection to prepare for the change of the EC environment are found to be the construction of internet cyber-mall, the consumer-protecting regulations and the private information and system security regulations. The standards and methods of the their judgement is also important factors and are believed to attract the consumers' interest about the assessment of the internet cyber-mall and eventually serve the rights and interests of the consumers. The technology-level for the business transaction, the research and development of its technology and putting it into practical use are also found to be significant factors.

1. 서론

최근 가상공간을 무대로하는 전자상거래(EC)가 일반인들에게 급속하게 확산되고 있다. 인터넷 이용자 역시 폭발적으로 늘어나고, 컴퓨터 및 통신기술이 급격히 변화되면서 전자상거래는 시·공간을 뛰어 넘고 있어 이를 보호할 수 있는 정보보호에 대한 중요성이 강조되고 있다. 한편 정부에서도 정보보호 제품 전반에 적용되는 공통기반기술, 서버·네트워크·유무선 단말시스템 등을 보호하는 시스템 네트워크 보호기술, 전자상거래 등 용응서비스의 안전성을 확보하기 위한 응용서비스 보호기술등으로 구분하여 집중연구 토록 구상하고 있다.

따라서 국가정보화 정책과 인터넷의 급속한 성장으로 다양한 컨테츠개발과 멀티미디어 보급, 전자결

* 종신회원 : 대구산업정보대학 컴퓨터정보계열 교수

논문접수 : 2002. 12. 24.
심사완료 : 2003. 1. 10.

※ 본 연구는 2002년 대구산업정보대학 교내연구비 지원에 의한 것임.

재, 전자상거래등 복합적인 네트워크서비스가 가능하여 지고 있다. 이와같은 발전은 서버구축과 간단한 업무까지도 자체적으로 해결하려는 긍정적인 효과도 있지만, 인터넷과 네트워크를 이용하여 쉽게 해킹을 당하여 정보를 유출할 수 도 있다.

본 연구에서는 전자상거래상에서 정보를 보호하기 위해 먼저 정보보호 침해실태와 사례를 고찰하고, 전자상거래 구축에 필요한 선행적 연구를 통해 환경적 변화요인을 추출하여 최적의 방향을 제시하고자 한다.

2. 정보보호에 침해실태 고찰

2.1 EC를 위한 환경변화 요인

전자상거래를 이용한 상품구매가 증가함에 따라 이제는 안심하게 거래할 수 있는 인터넷 사이버몰에 대한 판단기준이 절실히 요구되고 있다. 최근 각종 조사에 따르면 전자상거래가 확산되지 않는 이유로 인터넷 사이버몰에 등록할 때 요구되는 개인 신상정보의 유출 우려가 가장 큰 것으로 나타나고 있다. 이에 소비자에게 우후죽순처럼 생겨나고 있어 인터넷 사이버몰중에서 믿을 수 있는 것을 찾기 위한 환경적 변화요인이 요구되고 있다.

또한 인터넷을 이용하고 있는 많은 사용자들은 정보보호에 대해 노출되어 있다. 특히 전자상거래를 이용하고 있는 사용자들도 보안에 대해 투명성을 보장한다고는 할 수 있으나, 투명한 접근은 보안상의 문제점을 야기시킬 수 있다. 본장에서는 전자상거래상에서 정보보호를 위협하는 요소와 침해사례를 고찰한다.

가. 위험요인

정보보호를 위협하는 해킹, 바이러스 및 기타 요인들을 가장 인위적인 요인으로 볼 수 있다. 해킹이란 "시스템관리자가 구축해 놓은 보안망을 어떤 목적에서건 무력화 시켰을 경우 이에 따른 모든 행동을 해킹이라고 한다"라고 정의하고 있다. 이는 보통 시스템 관리자의 권한을 불법적으로 획득할 경우, 또는 이를 악용해서 다른 사람에게 피해를 준 경우를 해킹이라고정의하고 있다[정태명]. 해킹은 일반적으로 침입(Intrusion), 서비스거부(Denial of Services), 정보유출(Information Theft)을 목적으로 하고 있으며, 해킹은 다음과 같이 3단계로 구분한다.

- 1단계 : 목표로 한 호스트 내부에 잠입하여 셀을 사용할 수 있는 사용자의 권한을 얻어내는 것이다. 이를 실행하기 위해 사용자의 패스워드를 알아내어 이용한다.
- 2단계 : 목표로 하였던 호스트 내부에 잠입하여 호스트관리자의 권한을 획득한다. 이는 호스트 내부OS의 보안상 취약점을 이용하는 것이다.
- 3단계 : 시스템관리자의 "root" 권한을 획득한 이후 자신이 다시 침입할 수 있도록 하는 방법이다.

나. 해킹방법

1) Social Engineering방법은 시스템관리자를 속이는 방법으로 정당한 사용자인 것처럼 속이고 접속한다. 이는 신분확인 과정을 거치지만 통상적인 질의 응답 경우가 많아 사용자정보의 노출이 많다.
2) Impersonation방법은 정당한 사용자 ID를 도용하는 경우로서, 네트워크 접근시 ID와 패스워드를 도용한다. 이 경우 물리적인 사용자확인 또는 링크레벨의 암호화 등이 필요하다.
3) Exploits는 시스템의 버그를 이용하여 보안 취약점을 활용한다. 이는 취약점 분석 프로그램을 이용하여 취약점을 파악한 다음 파일서버, POP서버등에 침입하는 방법이다.
4) Transitive Trust방법은 호스트가 신뢰하는 시스템이나 네트워크로로 위장하는 방법이다. TCP/IP 프로토콜의 결점으로 지적되는 Source IP를 통해서 인증하는 호스트 인증문제와 순차번호 생성문제를 이용해서 호스트의 IP 주소를 바꾸어서 공격자가 신뢰관계에 있는 호스트로 위장해서 시스템에 공격하는 형태이다,
5) Data Driven Attack방법은 불법프로그램을 이식하는 경우로서, 만약 Postscript 파일을 메일로 보냈다면 수신자가 이를 파일로 변환할 때 불법 명령들이 수행될 수 있도록 한다. 방화벽

시스템을 이용한 스크린서비스의 제한이 요구된다.

6) Infrastructure Attack방법은 시스템이나 네트워크 프로토콜등의 구조적인 문제점을 공격하는 수법으로 DNS Spoofing, ICMP폭탄, Source Routing방법을 이용한다.
7) Denial of Service Attack방법은 시스템의 정상적인 동작을 방해한다. 이는 대량의 데이터패킷을 네트워크 또는 전자우편으로 보내는 해킹공격이다.

2.2 정보보호 침해 및 사례분석

"해킹 바이러스 통계 및 분석" 결과 모두 1379건의 해킹과 4274건의 바이러스 피해가 발생하였다. 해킹피해를 유형별로 살펴보면 불법자원 사용이 538건(37%)으로 가장 많았으며 불법침입 479건(32%)과 침입시도 467건(31%)으로 그 뒤를 이었다. 이외에 자료변조 및 삭제 3건, 홈페이지 변조 2건이 발생했다. 기관별로는 기업의 피해가 203건, 대학은 40% 가량 줄어든 82건에 그쳤다. 우리나라를 경유하는 외국 해킹은 801건으로 늘어났다. 지역별로는 미주지역에 대한 공격이 60% 이상 줄어든 반면 아시아와 유럽은 각각 70%와 30% 가량 늘어났다. 특히 일본과 이스라엘을 대상으로 하는 해킹공격이 크게 증가했다.

Cyber118에 접수된 전체 상담건수는 5,278건으로 해킹상담이 3,001건(56.9%), 바 이러스상담이 1,790건(33.9%), 일반상담이 487건(9.2%)접수되었다. 美-中 사이버전과 관련된 Sadmind/IIS 웜 공격에 관한 상담이 많이 접수되었다. Sadmind/IIS 웜은 Solaris 시스템을 공격숙주로 WindowsNT/2000 시스템의 홈페 이지를 변조시키는 웜으로 국내 많은 시스템이 이와 관련한 취약점을 패치하지 않아 많은 피해를 보았다. 또한 WindowsNT/2000 시스템을 공격하는 CodeRed, CodeBlue 웜과 Windows98/NT/2000 시스템을 공격하는 Nimda 웜이 발생하여 WindowsNT /2000 서버 관리자들로부터 많은 상담이 접수되었다.

바이러스상담을 살펴보면 전체 바이러스 상담 1,790건 중 CIH 바이러스가 총 1,033 건으로 가장 많이 접수되었으며 다음으로 Sircam 바이러스 293건, Hybris 바이러스 80건 순으로 접수되었다. 매년 4월 26일에 활동하는 CIH 바이러스는 2000년도 상담건수 2,374 건에 비하면 무려 50% 이상이 감소한 수치로 일반기업은 물론 개인 PC 사용자 모두 CIH 바이러스에 대한 인식이 높아졌음을 알 수 있다. 월별 상담현황을 보면 CIH 바이러스나 美-中 사이버전 사고와 관련된 Sadmind/IIS 웜, CodeRed 웜, Nimda 웜처럼 국내에 대규모적인 해킹 바이러스 피해가 발생될 경우 Cyber118에 예방 및 대응을 위한 문의가 집중되고 있음을 알 수 있다.

3. 정보보호기술과 인증방법

전자상거래의 보호기술에는 인터넷 웹보호, 암호 및 인증, 전자우편 보호, 전자화폐 보호 등이 있다. 본 장에서는 이들 요인을 중심으로 장·단점을 고찰한다.

3.1 인터넷 웹보호

인터넷이 확장 보급 되었을 때 컴퓨터 내에 저장되어 있는 각종 정보나 중요문서에 대한 보안이 요구되었다. 특히 TCP/IP프로토콜에 의해 동작되는 인터넷이 보급되면서 메시지 도청, 메시지위조, 메시지 변조, 송수신 부인, 불필요한 접근 등으로 보안에 대한 중요성이 더욱 증가하게 되었다. 이후 TELNET, FTP, SMPT 및 HTTP 서비스가 보급되었지만 TCP/IP네트워크를 이용하여 동작하기 때문에 자료에 대한 기밀성, 무결성, 인증, 봉쇄 및 접근제어에 대한 상당한 취약성을 가지고 있다. 이를 해결하기 위한 네트워크로는 SSL, TLS, IPsec, S/MIME 및 PGP 등을 통해 보안을 제공할 수 있다.

1) Secure Socket Layer(SSL)은 TCP/IP계층과 어플리케이션 계층 사이에 위치하며, 데이터를 송수신하는 컴퓨터사이 종단간 보안서비스를 제공한다. 클라이언트와 서버가 SSL을 이용해 연결할 경우 먼저 SSL Handshake Protocal을 수행하여 한 세션 동안 보안서비스사용에 제공되는 세션키, 암호알고리즘, 인증서 등과 같은 암호 매계변수를 서로 공유한다. 이들 요인은 기밀성을 요구하는 어플리케이션 각각에

대한 여러 가지 암호알고리즘을 제공하며, 서버와 클라이언트간에 서로 인증이 용이하다. 또한 내부적으로 데이터 전송을 방해할 수 없도록 하거나 재전송 공격에 이용할 수 없도록 하는 기밀성을 유지하고 있다.

2) TLS는 IETF에서 SSL v3.0을 표준화 하기위해 제안된 보안 프로토콜로서 pre_master_secret 정보를 이용하여 키를 생성한다. 이는 특허등의 문제로 표준화에 걸림돌로 작용하는 암호알고리즘에 대한 교체에 주로 사용된다.
3) IPsec는 네트워크 보안을 위해 TCP/IP프로토콜의 IP계층에서 보안서비스를 제공하기 위한 IPsec이고, 다른 하나는 TCP계층위에서 클라이언트/서버 어플리케이션 사이에 보안서비스를 제공하기 위한 TLS(Transport Layer Security)가 있다. 이들 요인은 인증과 암호화에 필요한 암호알고리즘 키를 생성하고 분배를 할 수 있다. 또한 보안프로토콜 각각에 대한 보안 매개변수(알고리즘 식별자, 모드, 키)를 정의하고, 관리함으로서 데이터에 대한 무결성, 기밀성, 접근제어 및 재전송공격에 대한 정보를 보호할 수 있다.

3.2 암호 및 인증

암호기술은 암호키 사용방법에 따라 대칭키 방법과 비대칭키 방식이 있다. 대칭키 암호화 방법은 키의 길이가 상대적으로 짧고 알고리즘구성이 치환 순열구조이다. 수행속도가 빠르고 대량의 정보를 처리하는데 적합하지만 상호간에 비밀키를 공유하고 있어야 되기 때문에 키 교환과정에 많은 위험성이 존재한다. 반면 비대칭키 암호화방식은 평문에 암호/복호화 키가 분리되어 있다. 이는 공개키와 비밀키가 생성되어, 공개키는 통신하고자 하는 상대방에게 공개하고 자신은 고유의 비밀키만 안전하게 보관한다.

3.3 전자우편 보호

전자우편서비스는 LAN 및 Web환경을 기반으로 하는 EC분야에 적용할 수 있다. 특히 E-mail을 이용한 정보교환은 특정사용자나 다수의 사용자에게 네트워크를 통하여 메시지를 전달할 수 있게 해주며 시간적 공간적 제약을 받지 않고 있다. 특히 PEM(Privacy Enhanced Mail)은 전자우편 보호도구로서 사용되며 기밀성, 인증, 무결성, 부인방지 등의 기능을 제공한다.

3.4 전자화폐 보호

전자화폐는 디지털데이타를 기반으로 하는 사회의 가상공간에서 동전이나 지폐의 역할을 수행하기 위한 화폐이다. 전자화폐는 소비자에게 현금을 지불할 때 편리성, 기업에게는 결제의 즉시성, 은행에게는 비용삭감, 발행체에게는 신규의 비즈니스 기회 부여의 잇점도 있으나, 익명성 · 양도성 · 유통성 · 운용비용등 법적, 제도적 등의 문제도 있다.

3.5 전자지불 시스템

전자상거래에서 전자지불 방법에는 지불브로커(Payment Broker)시스템과 전자화폐(Electronic Cash) 시스템으로 분류할 수 있다. 지불브로커시스템은 독립적인 신용구조를 갖고있지 않고 신용카드나 은행의 계좌입금을 통해 네트워크상에서 지불하는 구조이며, 전자화폐시스템은 플라스틱카드 위에 부착된 IC칩을 이용해 off-line으로 대금을 결재하는 방법이다. 이러한 기능은 실거래에서 편리한것 도 있으나, 이중사용과 복사가능성, 비효율성에 대한 세심한 주의를 요한다.

4. 환경적 변화에 대한 대처방안

EC의 환경변화에 대응하기 위한 방안으로서는 다음과 같은 요인들이 중요요인으로 제시되었다. 인증방법에서는 인증을 받기위해 인증업무에 대한 종류, 수행방법 및 절차, 이용조건, 업무수행에 대한 필요한 요인을 명기하여야 한다. 전자서명 생성키 관리 방안에서는 인증을 받은 사용자에 대해서는 자신의 전자서명 생성키를 안전하게 보관 관리, 전자서명생성 키가 훼손, 도난, 유출되었을 때는 정보보호센터에 지체없이 통보하고 인증업무의 안전과 신뢰성을 확보할 수 있는 대책을 강구하여야 한다. 전자서명

키보호 방안으로서는 누구든지 타인의 전자서명생성키를 도용, 누설방지 및 인증서를 발급받아서는 안된다. 전자문서가 작성 및 송·수신된 때의 형태 또는 그와 같이 재현될 수 있는 형태로 보존 되어 있을 때 인증 받을 수 있다. 이때 작성자, 송신자, 수신자, 일시에 관한 사항에 관한요인이 제시되었으며, 사이버몰 운영자는 전자거래에 사용되는 컴퓨터등의 안전성을 확보하기 위하여 암호제품 및 사이버몰 운영·관리에 필요한 시설을 갖추어야 할 것으로 사료된다.

전자거래에서 전자거래 당사자등은 자료의 처리·전송 또는 보관되는 정보에 대한 부당한 접근과 이용·정보유출등을 방지할 수 있는 대책을 마련하여야 하며, 전자결제, 지적소유권의 보호에관한 사항이 중요요인으로 제시되었다. 사용자보호방안으로는 사용자에 대한 전자서명, 인증, 암호화등을 통해 개인보호와 신뢰성가 중요요인으로 제시되었다.

5. 결론

EC환경 변화에 대응하기 위한 정보보호 요인은 소비자가 신뢰할 수 있는 최소한의 인터넷 사이버몰 구축에 관한 중요성, 소비자 보호규정·정보통신망 이용촉진등에 관한 개인정보 보호 및 시스템 보안에 대한 규정이 중요요인으로 제시되었다. 심사기준과 함께 심사방법도 중요요인으로 도출되었으며, 인터넷 사이버몰 평가에 대한 소비자의 관심을 유발시켜 소비자 권익보호에도 기여할 것으로 사료된다. 또한 전자상거래에 대한 기술수준, 기술의 연구개발, 개발된 기술의 실용화등도 상당히 의미 있는 요인으로 제시되었다.

향후 전자상거래에서 신뢰할 수 있는 인터넷 사이버몰을 평가하는 모델제시와 사업자에게는 소비자에게 신뢰를 받을 수 있는 인터넷비지니스 모델이 추후 제시될 수 있는 유용한 사이버 공간으로 활용될 것으로 기대한다.

※ 참고문헌

[1] 김건량·장종수·손승원, "네트워크 보안정책 정보모델에 기반한 정책관리 도구의 구현, 한국정보처리학회논문지, Vol9-c, No5. P775, 2002

[2] 김선숙, 인터넷쇼핑몰 성공의 열쇠, 21세기사, 2002

[3] 보고서, "해킹 바이러스 통계 및 분석", 한국정보보호진흥원, 2002, 11

[4] 오명옥·김성열·배용근·정일용,"효율적인 그룹키분배 및 갱신을 위한 보안프로토콜 설계", 한국정보처리학회논문지, Vol9-c, No3. P331, 2002

[5] 이상하·조인준·천은홍·김동규, "역할기반 접근통제에서 역할계층에 따른 접근권한 상속의 표현, 한국정보처리학회 정보처리논문지, Vol7, No7, 2002, P2125

[6] 이만영외5, 전자상거래 보안기술, 생능출판사, 1999.8

[7] 정영훈·이태현·박판열·배재광, 인터넷 비즈니스 법률가이드, 2001

[8] 정태명,서광현,이동영, 인터넷 정보보호, T&T, 2002.5

[9] www.etnews.co.kr

[10] www.ectrust.net 전자상거래 소비자보호지원센터

[11] www.cyber118.or.kr 한국 정보보호진흥원

신 영 균

1981년 아주대학교 전자공학과 졸업
1985년 대구대학교 전자정보공학(석사)
1996년 대구가톨릭대학교(MIS전공)(박사)
1983년 ~ 현 대구산업정보대학 컴퓨터정보계열 부교수
관심분야 : 정보관리, 네트웍, EC