인터넷 모범상점 인증제도와 보안관리

정태명 / 성균관대학교 컴퓨터공학과 교수

인터넷 사용이 폭발적으로 증가하고 있다. 이와 함께 자연스러운 사회 변화가 나타나고 있는데 그것이 바로 인터넷을 이용한 상거래 행위, 즉 전자상거래이다. 현재 전자 상거래는 차세대의 변화의 주역으로 관심의 대상으로서 점차 활성화되고 있다. 그러나, 실상 우리 나라에서 전자상거래를 통한 매출은 인터넷의 성장률과 비교해 아주 미약한 상태이다. 그 원인으로는 여러 가지가 있을 수 있으나, 가장 대표적인 이유는 전자상거래의 주체인 인터넷 상점(internet shopping mall)에 대한 신뢰 때문이라고 생각된다. 즉 소비자가 안심하고 거래하기에는 여러 가지로 미비한 점이 있다는 것이다. 따라서, 한국정보통신진흥협회는 민간차원에서 모범상점(safe mall)의 요건을 갖춘 업체들을 선별하여 모범상점 마크를 수여하고 있다. 모범상점의 요건은 사용자의 편리성, 상품에 대한 신뢰성, 거래 및 가격정책의 투명성, 소비자의 신뢰도 등 여러 가지 형태가 있을 수 있으나 한국정보통신진흥협회의 인증제도는 소비자의 신뢰도에 초점을 두어 소비자 보호, 개인정보 보호, 시스템 안정성의 3개 부문에서의 우수성을 바탕으로 심사하고 있다. 본 고에서는 이러한 세 분야 중 특별히 보안의 문제에 대해 살펴보고자 한다.

인터넷상점의 보안은 일반상점 보안의 확장형으로 생각하면 쉽게 이해될 수 있다. 일반상점의 보안을 위해 우리는 다음과 같은 세 가지 단계의 조치를 취하는 것이 일반적이다.

▲ 한 개 혹은 두 개의 출입문을 만들고, 각 문에 자물쇠를 설치한다. 이를 통해 우리는 절도 등의 범죄 행위로부터 1차적인 격리를 기대하게 된다.

▲ 일반적으로 자물쇠를 설치한 것만으로는 완전한 보안이 이루어졌다고는 생각하지 않으므로 도난방지용 센서를 중요 지점에 설치하고 이를 통해 상시 감시체제를 유지한다.

▲ 더욱 안전한 보안을 요할 때에는 각 지점의 안전 상태를 수시로 점검함으로서 철저한 보안을 유지하도록 한다.

보안의 문제는 창과 방패의 관계에서 "새로운 창의 출현이 방패를 이기고 다시 창을 이길 수 있는 방패가 만들어지는 현상"과 같이 어떠한 경우에도 전문적인 범죄자들에게 보안의 위협을 받을 수는 있다. 그러나, 이러한 안전 장치를 통해 우선적으로 일반적인 침입이나 실수로 인한 피해를 방지할 수 있으며, 전문적인 범죄자의 침입 행위도 어느 정도 예방할 수 있게

된다. 강력한 보안 조치는 적어도 범죄자가 다른 목표물을 선호하도록 유도하는 효과를 가져올 수 있다.

인터넷 상점에서도 마찬가지로 다음과 같은 세 단계의 보안 조치를 통해 내부 정보를 인터넷 자체가 가진 데이터의 도용, 변조, 탈취 등의 인터넷 공격으로부터 보호할 수 있다.

▲ 인터넷 상점의 출입문(gateway)을 최소한의 수로 제한하고 각 출입문에 방화벽(firewall)을 설치하여 1차적인 침입 및 내부 사용자의 실수로 인한 정보의 유출 등을 방지한다.

▲ 방화벽의 기능만으로는 완전한 보안이 불가능하므로 인프라 내부의 중요 서버 등에 침입차단시스템(Intrusion Detection System)을 설치하고 이를 통해 침입의 가능성이 있는 행위를 감지하고 대응하는 역할을 하도록 한다.

▲ 더욱 세밀한 보안 유지를 위해 보안 취약성을 점검하는 소프트웨어 등을 설치하고, 보안의 취약성을 수시로 점검하도록 한다.

물론 인터넷에서 100% 보안 유지를 기대하기는 거의 불가능하다고 여겨지기는 하나 이밖에도 더욱 강화된 보안을 위해서는 계속적으로 보안 전문가의 자문(consulting)을 받기도 한다. 이러한 보안 조치는 일반 상점에서보다 인터넷 상점에서 더욱 중요하게 여겨진다. 그 이유는 일반 상점의 경우에는 상품이나 현금의 도난으로 그 피해 정도가 국한될 수 있으나, 인터넷 상점들의 경우에는 소비자 개인의 정보가 관련이 되므로 피해의 정도가 상점 자체를 넘어 개인들에게까지 확대될 수가 있기 때문이다. 예를 들면, 인터넷 상점에 저장된 개인 신용카드의 유출은 범죄자에 의해 개인의 경제적 손실과 혼란을 가져올 수 있으며, 작게는 개인 전자우편 주소 등의 유출로 인하여 스팸 메일을 이용한 불편을 초래할 수 있다. 또한, 정보의 유출과 범죄의 행위가 흔적이 없이 발생할 수 있으므로 계속적인 피해를 야기할 수도 있다.

따라서, 모범상점 인증제도의 보안 심사를 통한 목표는 "상기한 보안 기능이 인터넷 상점에서 제대로 실현되고 있는 지를 확인하고 이에 대한 마크를 부여함으로서 소비자들로 하여금 자신의 정보에 대한

인터넷 상점에서의 보안유지는 일반상점에서보다 훨씬 더 중요하다 그 이유는 일반 상점의 경우에는 상품이나 현금의 도난으로 그 피해 정도가 국한될 수 있으나, 인터넷 상점들의 경우에는 소비자 개인의 정보가 관련이 되므로 피해의 정도가 상점 자체를 넘어 개인들에게까지 확대될 수가 있기 때문이다.

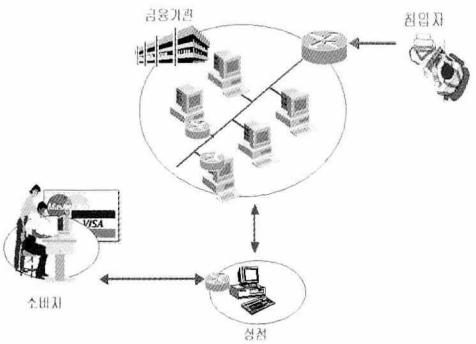
안전을 신뢰하도록 하여 궁극적으로는 전자상거래의 활성화를 유도하는 것"이다. 특히 인터넷상의 보안은 개인의 손을 통해 이루어지기보다는 정보통신이라는 매체를 이용하므로 보안 시스템의 사용이 없이는 거의 불가능하다고 볼 수 있다. 따라서, 단순한 의지만으로는 보안 유지가 실현될 수 없으며, 보안 도구를 사용하는 사실이 확인되어야 한다. 이에 근거하여 모범 상점 인증제도의 보안 관련 항목은 인프라 보안의 3박자인 방화벽, 침입탐지시스템, 취약성분석 소프트웨어의 설치 및 사용 유무를 확인하고 있다. 다음은 이러한 세 가지 보안 도구에 대해 간략히 살펴보기로 한다.

방화벽 : 방화벽은 〈그림 1〉에서 보는 바와 같이 인터넷 상점의 길목에 위치하여 인터넷 상점에 출입하는 모든 패킷을 일일이 점검하고 이미 설정된 정책에 따라 패킷의 출입 여부를 제한하는 것이다. 일

반 상점과 비교해 예를 들면, 주류를 판매하는 상점에서 미성년자를 출입시키지 않거나, 주류 판매와 관련이 없는 사람들의 출입을 제한하는 역할을 한다. 방화벽은 일반적으로 패킷의 통과 여부를 직접 제한하는 패킷필터링방식과 프락시(proxy)로서 중계 기능을 담당하면서 서비스를 제한하는 프락시 서버 방식을 구현하며, 이들 방식은 내부 전산망을 외부의 침입으로부터 보호하고, 내부 사용자의 정보 유출을 방지하는 역할을 한다.

침입탐지시스템 : 침입탐지시스템은 인터넷 모범 상점 인프라의 중요 부분에 설치되어 인터넷의 패킷 정보 뿐 아니라, 사용자의 행위, 통계적인 시스템의 변화 등을 고려하여 침입 여부를 판단하게 되고, 이미 설정된 대응 정책에 따라 이에 적절한 대응행위를 취하게 된다. 〈그림 2〉는 전자 상거래를 형성하는 상점과 금융기관에 설치된 침입 탐지 시스템을 보여주고 있다. 일반적으로 침입의 형태는 인터넷 상점의 전산자원을 고갈시키는 서비스 거부행위(Deni- al of Service), 정보를 탈취하는 행위, 정보를 파괴하는 행위, 정보를 변조하는 행위 등으로 나타나게 되는데, 대부분의 경우 이러한 침입의 행위가 복합적으로 이루어진다. 예를 들면, 방화벽이 설치된 시스템의 메모리 자원을 고갈시켜 방화벽의 기능을 상실하게 한 후, 인터넷 상점 내부 시스템에 침입하여 개인 정보를 습득하여 네트워크를 통해 자신의 시스템으로 옮겨 놓고 자신의 침입 사실을 은닉하기 위하여 시스템 파일을 변조하거나 지워 버리게 되는 것이다.

〈그림1〉 전자상거래 상점 보호를 위한 방화벽의 설치도



〈그림2〉 전자 상거래 환경에서의 침입 탐지 시스템 설치도

침입 탐지 시스템은 침입의 상황을 실시간으로 경보하고, 침입에 대한 통계 보고를 작성하며, 때로는 탐지된 침입에 대해 대응하는 기능을 하게 된다. 인터넷을 통한 침입은 바이러스의 형태를 제외하고도 현재 500여개의 종류가 알려져 있으며 계속적으로 증가하는 추세에 있다. 작년에 약 200여개가 알려져 있던 것과 비교하면 기하급수적인 증가가 예상된다.

취약성 분석 소프트웨어 : 취약성 분석 소프트웨어는 시스템의 취약한 부분들을 점검하고 이에 대한 대응책을 제시하는 소프트웨어로서 패스워드의 적합성,

시스템 파일 내용의 변조 등을 점검하게 된다. 기존에 알려진 취약성들을 주로 살펴보게 되는데, 이를 통하여 침입의 가능성을 최소화하게 되며 트로이목마와 같은 침입을 방지할 수 있게 된다. 또한 취약성 분석 소프트웨어는 전문가의 자문을 받기 위한 기초자료로 활용될 수도 있다.

인터넷은 정보의 변조, 도용, 탈취 등의 침입에 항상 노출되어 있으므로 사실상 전자상거래는 범죄의 위험 속에서 실현되는 행위로 볼 수 있다. 때문에 보안의 중요성은 더욱 강조되고 있으며 이를 간과하고는 결코 전자상거래의 활성화를 기대할 수 없다. 모범상점에 대한 인증 제도는 이러한 의미에서 꼭 필요한 제도로 이해될 수 있으며, 모범 상점으로 인증된 기업들의 노력을 통하여 제도가 안정화된다면 전자상거래 시대의 새로운 도약을 기대할 수 있을 것이다. 모범상점 인증 제도는 이러한 기업의 노력을 지속적으로 모니터링하고, 보안 교육 등을 통해 협력할 계획으로 있다. 뿐만 아니라, 본 제도를 미국의 Trust-e 마크, 일본의 프라이버시 마크, 유럽의 VIP 제도와 같은 국제적인 신뢰를 얻는 인증 제도로 승화시키려는 계획을 갖고 있다.

회원사 소식

LG정보통신, 디지털 사내방송 "디지넷" 개국

LG정보통신(대표 서평원)이 새로운 형태의 사내 커뮤니케이션 문화를 선보여 화제다.

이 회사는 지난달부터 설치작업에 들어가 약 2주간의 시험방송을 마치고 이달 1일부터 첨단디지털사내방송인 디지넷(Digi Net)을 개국, 본격적인 방송에 들어갔다고 밝혔다.

디지넷은 사내 13개 장소에 기존의 종이게시판을 대신할 액정표시장치(LCD) 모니터를 설치해 기업내 커뮤니케이션을 정확하고 빠르게 더많은 사람에게 제공한다는 개념에서 출발했다. 이 시스템은 LG강남타워 6개층에 설치된 13대의 LCD모니터를 통해 자사 임직원과 고객들에게 하루 11시간 동안 방송되는 사내커뮤니케이션 수단이다. 전달되는 정보도 회사소개, 빌딩안내, 환영메시지는 물론 사내 주요뉴스, 이벤트, 경조사 등으로서 문자와 함께 영상에 이르기까지 광범위하다. 이 회사는 『최근 여의도에서 역삼동 신사옥인 LG강남타워로 이전하면서 첨단통신업체의 이미지를 바탕으로 시행하는 새로운 사내커뮤니케이션 기업문화 이미지를 확립하기 위해 한달간 이 작업을 시행해 왔다』고 시행취지를 설명했다. 종전까지 디지털방식의 LCD를 통해 텍스트뉴스를 제공하는 대표적인 건물로는 엘리베이터에 이를 활용하고 있는 포스코빌딩이 꼽혀 왔다.