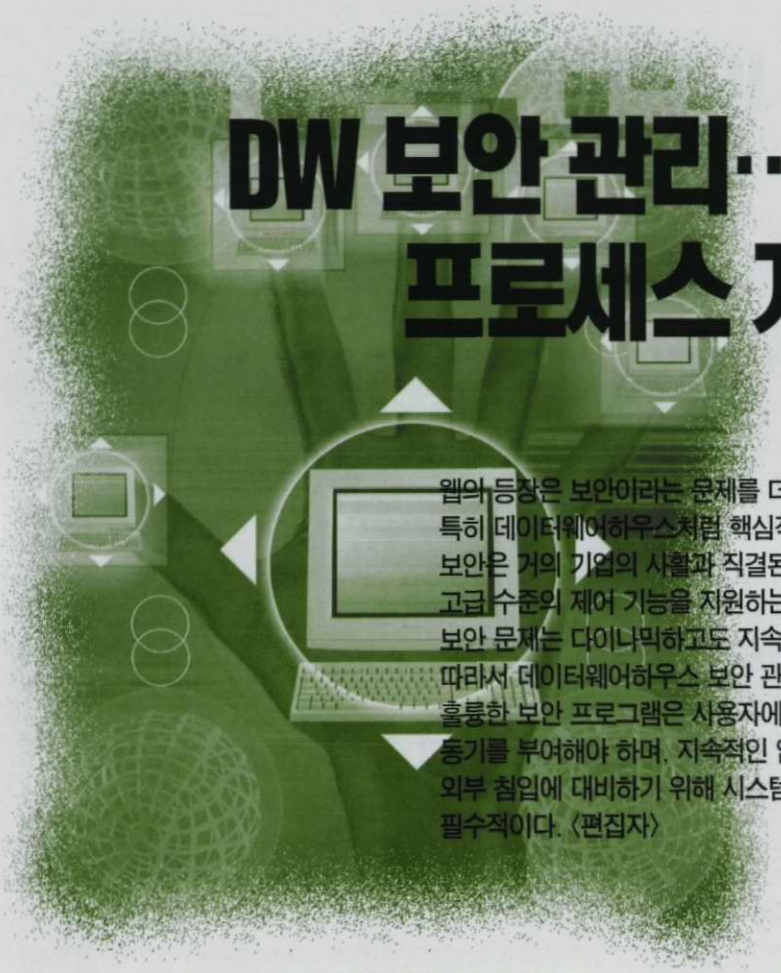
DW 보안 관리… 프로세스 개선이 핵심



웹의 등장은 보안이라는 문제를 더욱 중요하게 부각시켰다. 특히 데이터웨어하우스처럼 핵심적인 대규모의 시스템 환경에 있어서의 보안은 거의 기업의 사활과 직결된다고 볼 수 있다. 고급 수준의 제어 기능을 지원하는 보안환경은 이제 필수적인 요소이다. 보안 문제는 다이나믹하고도 지속적으로 변화되고 있다. 따라서 데이터웨어하우스 보안 관리자는 프로세스를 계속해서 관리해야 한다. 훌륭한 보안 프로그램은 사용자에게 보안의 중요성을 지속적으로 알리고 동기를 부여해야 하며, 지속적인 업데이트가 가능해야 한다. 외부 침입에 대비하기 위해 시스템 전체를 지속적으로 스캔하는 것도 필수적이다. 〈편집자〉

보안은 대부분의 데이터웨어하우스 관리자들이 기피하는 사안이다. 보안은 복잡 미묘하면서도 흥미로운 퍼즐게임과 유사하다. 일반적으로 데이터웨어하우스 전문가들은 퍼즐게임을 즐기기 때문에 웨어하우스 관리자들이 보안을 기피한다는 사실은 놀라운 일이 아니다.

보안은 사용자의 신분 확인을 위한 생명공학 스캔 장비, 고급 암호화를 기반으로 하는 가상 사설 네트웍(VPN), LDAP를 지원하는 신형 네트웍 서버 등과 같이 다양하고 흥미로운 하드웨어 및 소프트웨어 기술과 깊은 관련을 가지고 있다.

웹의 성장

보안은 해커, 크래커, 산업 스파이 등이 컴퓨터 시스템이나 데이터웨어하우스에 문제를 유발시키고자 위협하려는 데에 병적으로 집착하고 있기 때문에 결코 무시할 수 없는 사안이다. 이는 상업적인 측면에서 중요도가 매우 높기 때문에 관리자들은 보안 환경을 구축하기 위해 엄청난 비용을 지불하는 일도 마다하지 않는다.

데이터웨어하우스와 데이터웨어하우징에서 보안을 기피하는 이유는 무엇일까? 일반적으로 보안 문제는 제어와 기피의 문제라 할 수 있다. 또한 데이터웨어하우징 분야에서는 상대적으로 낮은 비중을 차지하고 있다.

숙련된(?) 데이터웨어하우스 관리자라면 데이터웨어하우스로 인해 야기된 업무상의 문제에만 전념할 것이다. 제어나 관리 문제에 대해서는 논의하는 것 자체를 기피하는 것이다. 그리고 보안 문제는 너무 복잡하고 일반화돼 있어서 실마리를 찾는 것조차 힘들다.

웹의 출현으로 인해 보안 문제는 더욱 심각하게 다뤄지고 있다. 네트웍 환경이 기업을 지배하고 있으며 복합적인 웹 환경과

별도로 1-2대의 시스템으로 독립적인 네트웍 환경을 구축하는 경우도 있다. 대부분의 사용자들이 웹을 사용할 수 밖에 없으며 웹에서 서비스를 구현하는 것도 거의 필수적인 상황이다. 보안은 웨어하우스 관리에 필수요소라 할 수 있으며 문제가 발생할 경우 해결책을 찾기 위해 지속적으로 노력해야 한다.

이 기사는 데이터웨어하우스 보안과 관련해 광범위하고 완벽한 해결책을 제시하려는 목적을 가진 것이 아니다. 다만, 데이터웨어하우스 관리자들이 직면하고 있는 주요 현안들을 해결할 수 있도록 보다 효과적이고 체계적인 보안환경 구축 방법을 설명하려는 것이다.

또 사용자가 구현할 수 있거나 사용자가 선호하는 솔루션과 전혀 다른 완벽한 솔루션에 대해 다루게 된다. 어떤 경우에나 비교와 논의가 가능하다.

보안 프레임웍

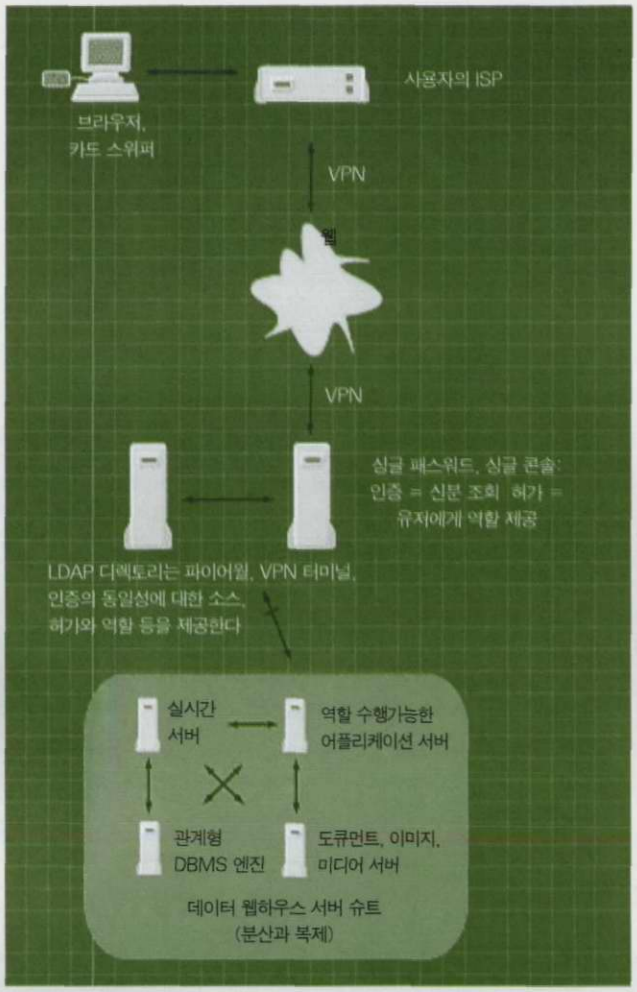
여기서 설명하는 보안 프레임웍은 사용자가 기업내부의 민감한 데이터에 액세스 할 수 있도록 한다. 프레임웍은 직원, 협력업체, 고객들을 물리적인 위치에 상관없이 단일 보안 솔루션을 통해 보호한다. 보안 대상은 웹의 외부나 안전한 기업 인트라넷 내부에 존재할 수 있다.

이러한 프레임웍을 선택한 이유는 간편하지만 막강한 기능을 지원하기 때문이다. 보안은 지속적으로 이뤄져야 하는 절차이다. 절대 일시적인 솔루션으로 생각해서는 안된다. 데이터웨어하우스 팀의 보안 관리자는 지속적으로 프레임웍의 구성 요소를 반복적으로 확인해 보안 환경을 수시로 수정하고 강화해야 한다.

데이터의 컨텐츠가 변경되고 사용자의 역할에 변화가 발생할 수 있다. 사용자 자신이 변경되거나 개별적인 역할이 변경되는 것도 가능하다. 기술도 변하고 해커나 악의를 품은 개별 사용자들의 위협 수단도 지속적으로 변화된다. 따라서 무엇보다 보안을 웨어하우스에서 이뤄지는 동적인 절차로 인식하는 것이 중요하다.

현재 운영하고 있는 웨어하우스 보안 프레임웍은 다음 4가지 구성 요소를 기반으로 이뤄진다(〈그림〉 참조).

▲ 2가지 요소 인증
▲ 안전한 연결
▲ 확실한 사용자 역할 정의
▲ 역할에 따라 관리되는 웹하우스 객체 액세스



〈그림〉 확장형 웨어하우스 시스템의 PC 사용자가 플라스틱 토큰을 인식시키고 인증을 받기 위해 PNI를 제시하는 과정

현재 사용되고 있는 기존 텍스트 비밀번호는 보안 문제에서 가장 큰 비중을 차지하고 있다. 비밀번호 문제를 완벽하게 해결한다면 보안 문제는 더 이상 신경쓸 것이 없다고 해도 과언이 아니다. 그러나 비밀번호는 쉽게 추측할 수 있다.

사용자가 직접 입력한 비밀번호는 너무 짧은 것이 사실이다. 짧은 비밀번호는 암호화한다고 하더라도 쉽게 공격할 수 있다. 사용자들은 비밀번호 관리를 효율적으로 수행하지 못하고 있다. 그리고 이를 비난할 근거도 마땅치 않다. 비밀번호는 복잡하고 관리가 쉽지 않다.

보안 환경에서는 비밀번호가 "사용자의 인식(what-you-know)"만을 기준으로 삼기 때문에 한가지 요소 인증을 의미한다. 불행스럽게도 한가지 요소 인증에서는 다른 사용자의 비밀번호를 알고 있을 경우 손쉽게 다른 사용자의 권리나 권한을 오용

할 수 있다.

2가지 요소 인증으로 인해 보안 환경은 획기적으로 개선될 수 있다. "사용자의 소유(what-you-have)" 또는 "사용자의 특성(what-you-are)"이 두번째 요소가 된다. 인코딩된 자기 성분의 고유 플라스틱이나 토큰를 갖고 있다면 두가지 요소 인증 시스템을 쉽게 이해할 수 있다. ATM 카드를 자동지급기에서 사용하거나 현금을 인출할 경우 두가지 요소 인증을 사용하게 된다. 이와 같은 두가지 요소에는 플라스틱 토큰과 PIN(Personal Identification Number)이 있다.

두가지 요소 시스템은 비밀번호를 사용하는 것보다 시스템 구성이 훨씬 어렵다. 특수한 플라스틱 카드를 만들거나 PIN을 발급하기 위해서는 확실한 고급 기술이 필요하다. ATM 방식의 두가지 요소 보안은 데이터웨어하우스에 적합해 실용화 단계에 이르고 있다.

보안 솔루션을 평가할 경우 소요되는 비용과 복잡성을 포괄적으로 살펴봐야 한다. 불법적인 보안 토큰을 만들거나 위협 또는 폭력적인 방법으로 액세스하려는 침입자들은 현재 선보이고 있는 대부분의 솔루션들이 가지고 있는 기술을 앞지르고 있다. 이들 보안 솔루션이 충분한 보호 기능을 지원하지 못하고 있는 것이다.

데이터웨어하우스 사용자가 플라스틱 토큰과 비밀번호를 기반으로 두가지 요소 인증 시스템을 채택한 경우 PC에는 카드인식 장비가 부착돼야 한다. 〈그림〉은 확장형 웨어하우스 시스템의 PC 사용자가 플라스틱 토큰을 인식시키고 인증을 받기 위해 PIN를 제시하는 과정을 설명한 것이다.

두가지 요소 인증

PC용 카드인식 장비는 이미 판매되고 있으며 가격은 계속해서 하락하고 있다. 이 장비는 I/O 포트나 PCMCIA 카드를 통해 외부장비로 연결할 수 있다. PCMCIA 카드는 이동형 PC의 표준으로 인식되고 있지만 데스크탑 시스템에서는 매우 불편하다. 플라스틱 토큰에는 임베드 형태의 마이크로칩이 포함돼 있고 정교한 "스마트카드"는 위조가 원천적으로 불가능하다.

다른 형태의 두가지 요소 인증 시스템에서는 사용자의 인식과 특성을 결합한다. 사용자의 특성은 지문 감식기, 서명 분석기, 망막 감식기 같은 생명공학 스캔 장비를 통해 결정한다. 이론적으로는 이러한 형태의 인증이 플라스틱 카드보다 훨씬 안전하다. 사용자 특성 시스템의 유일한 단점은 생명공학 입력 장비가 고가라는 점과 실생활에서 사용할 경우의 안정성 및 번거로움 등을 들 수 있다.

엄지손가락의 지문이 제대로 인식되지 않았다는 이유로 PC를 사용할 수 없다는 것은 참을 수 없는 일이다. 좀더 정교한 사용자 특성 인증 시스템은 자동 지급기 같은 고가의 터미널에 적합하지만 저가의 PC에는 어울리지 않는다.

위치에 상관없이 비밀번호와 플라스틱 토큰을 기반으로 웨어하우스 사용자를 위해 두가지 요소 인증 시스템을 구축하는 것이 최소한의 보안을 위한 솔루션이 될 수 있다. 그리고 카드 인식 장비를 이동형 및 데스크탑 PC에 부착할 수 있는 기술을 선택해야 한다. 카드와 비밀번호 관리는 보다 주의깊게 수행돼야 한다. 카드의 유효기간과 갱신 조건에 따라 신규 카드를 발급하고 오래된 카드를 폐기 처분하는 것도 중요하다.

객체 액세스

인증된 사용자에게 적절한 역할을 지정하면 정보가 요청될 때마다 지정된 역할을 활용할 수 있어야 한다. 이 과정에서 웹 인터페이스의 활용이 확대되면서 여러 가지 편리함을 누릴 수 있게 됐다. 웹 브라우저를 통해 원격 정보를 확인하려면 내부적으로 웹 서버가 있고 어플리케이션 서버에 의해 화면에 표시될 정보가 결정된다는 사실을 알아야 한다.

웨어하우스 보안 프레임웍에서는 원격 정보에 대한 액세스가 역할을 수행할 어플리케이션 서버에 의해 관리된다. 즉 모든 어플리케이션 서버를 수정해 페이지 이미지와 역할을 연결시킨다. 그 다음 연결된 사용자가 지정된 역할을 수행하는 경우에만 어플리케이션 서버에서 페이지를 전송하도록 하는 것이다.

역할을 수행할 어플리케이션 서버에서는 기존 제품과 연계해

보안 시스템을 자체적으로 구축할 수 없다. 각 어플리케이션 서버는 가능한 역할을 전송하도록 수정해야 한다. 이러한 작업은 매우 지루해 보이지만 보안 관리에는 이상적이다.

어플리케이션 서버는 유사한 아키텍처를 갖고 있으며 웹 서버에서 페이지 이미지를 렌더링하도록 정의하는 작업을 수행한다. 대부분의 어플리케이션 서버는 다양한 소스와 포맷에서 정보에 액세스하고 이를 결합할 수 있다. 이러한 이유 때문에 어플리케이션 서버에서 동일한 보안 솔루션을 적용하지 않는 것이다. 개별 데이터 소스는 종류와 포맷이 다양해 종합적인 단일 보안 솔루션에서는 처리할 수 없다.

역할을 수행할 어플리케이션 서버 방식을 사용하면 기존의 로우레벨 데이터베이스 테이블에서와 마찬가지로 파워포인트 프레젠테이션 같은 복합 멀티미디어 보고서에 대해 액세스 권한을 손쉽게 지정할 수 있다. 고급 수준의 보안제어 확인 기능은 현재 널리 사용되고 있는 멀티미디어 정보 환경에 적합하다. 로우레벨 데이터 객체에서 보안을 구현하는 작업은 제대로 수행되지 않는다.

역할을 수행할 어플리케이션 서버를 사용하면 사용자 연결을 데이터베이스 시스템에 지정할 수 없다. 기업 인트라넷 사용자가 데이터베이스에 직접 연결돼 비밀번호를 통해서만 액세스가 가능한 경우 전체 시스템에 영향을 미칠 수 있다. 이러한 상황에서는 적어도 두가지 문제가 발생한다.

첫째, 동일한 사용자들이 위치에 상관없이 데이터에 대한 동일한 액세스를 요구하게 된다. 사용자들은 기업이나 가정의 원격 위치에서의 액세스를 필요로 한다. 물론, 원격 위치에서의 연결은 웹을 통해 이뤄진다. 둘째, 비밀번호를 사용한 데이터베이스로의 직접 연결은 LAN에서 텍스트를 기반으로 구현돼 모든 작업 내용이 패킷 스니퍼의 표적이 될 수 있다.

주요 데이터 소스에 직접적인 연결을 필요로 하는 DBA나 시스템 관리자들처럼 관리 사용자들은 패킷 필터링 게이트웨이를 거쳐 별도로 구축된 네트웍에 연결된 PC에서 업무를 수행해야 한다. 독립된 네트웍 환경은 일반적인 기업 인트라넷에서 침입이 불가능하다. DBA와 시스템 관리자들이 사용하는 PC는 물리적인 보안 환경이 구축돼야 한다.

보안 프로세스 관리

고급 수준의 제어 기능을 지원하는 보안환경은 이제 필수적인 요소이다. 지금까지 이러한 요구사항을 반영하기 위한 프레임웍에 대해 살펴봤다.

그러나 보안 프레임웍이나 기술이 그 자체만으로 하나의 솔루션이 될 수는 없다. 보안 문제는 다이나믹하고도 지속적으로 변화되고 있다. 데이터웨어하우스 보안 관리자는 끝없이 계속해서 프로세스를 관리해야 한다.

훌륭한 보안 프로그램은 사용자에게 지속적으로 보안의 중요성을 교육시키고 동기를 부여함으로써 보안에 대한 자부심을 갖고 적절한 환경을 관리할 수 있도록 해준다.

보안 환경을 강화하고 보안으로 인해 발생하는 비용부담을 실제 업무의 연장선상에서 이해할 수 있는 사례 연구를 수행하기 위해서는 경영진의 개입이 불가피하다.

대부분의 사용자들은 보안 절차를 눈으로 확인할 수 있기 때문에 공항의 보안에 대해 매우 관대하다. 이와 마찬가지로 기업의 직원들이나 웨어하우스 사용자들이 보안 체계를 명확히 파악할 수 있도록 유도한다면 만족감을 극대화할 수 있을 것이다.

지속적인 업데이트 이뤄져야

또, 훌륭한 보안 프로그램은 지속적인 업데이트가 가능해야 한다. 이미 직원과 협력업체의 액세스 권한을 업데이트하는 작업에 대해 언급했다. 보안 관리자는 웹사이트나 데이터웨어하우스를 대상으로 벌어지는 보안 위협과 새로운 형태의 악용 사례를 미리 파악, 대비해야 한다. 바이러스 정의도 수시로 업데이트된다.

훌륭한 보안 프로그램은 외부 침입에 대비하기 위해 시스템 전체를 지속적으로 스캔한다. 웹사이트에 대한 외부 침입기록을 지원하는 유틸리티가 다양하게 선보이고 있다. 컨설팅 업체들은 정기적으로 기업의 정보 인프라스트럭처를 분석해 취약 부분을 파악한다. 이러한 작업을 자주 수행할 필요는 없지만 적어도 분석 작업이 수행되는 동안에는 주의 깊게 살펴야 한다.

데이터웨어하우스에서 보안 프레임웍을 적절히 지정했다면 전담 보안 관리자를 충원하는 일만 남는다. 보안 관리자는 팀에 소속돼 전체 데이터웨어하우스 관리자의 명령을 받는다. 이 때에는 데이터웨어하우스 팀에서만 데이터 정보와 권한 허용을 관리할 수 있다.