규제 준수와 데이터베이스 보안의 유형별 고찰

Regulatory Compliance and type of Database Security Analysis

이병엽
배재대학교

Byoung-Yup Lee
Pai-Chai University

요약

기업은 개인정보의 보호를 위해 다양한 방안들을 마련해 이러한 규제를 준수하며 내부에 관리중인 개인정보에 대해 보안을 강화하기 위해 빠르게 보안 솔루션을 도입하고 있다. 이에 수많은 데이터들이 저장되어 사용되고 있는 DBMS 측면에서 이러한 규제를 준수하는 동시에 효과적으로 데이터 보안을 확보하기 위한 방안을 암호화, 접근제어, 감사로 구분하여 각각의 대한 구현방법 및 해당 솔루션들을 비교하여 이를 통해 최적의 데이터 보안 방안을 모색할 수 있도록 한다.

Ⅰ. 서론

개인정보 유출 문제는 비단 국내만의 문제는 아니며, 전세계적으로 관심이 집중되는 이슈 중 하나라 할 수 있다. 그림 2와 같이 미국의 오픈 시큐리티 파운데이션(Open Security Foundation)에 따르면 유출된 개인정보가 08년 86,311,058개에서 09년 218,756,349개로 전년대비 153%로 상당히 증가 하였다. 유출된 개인정보는 상당히 증가한 것과 달리 공개적으로 보고된 개인정보 유출 사건 건수는 08년 717건에서 09년 436건으로 줄어 들었다. 이는 개인정보 유출 사건의 피해 규모가 대형화되고 있다는 것을 의미 한다[3][4]. 따라서 이러한 개인정보의 유출이 개인 에게만 피해를 발생하는 것 뿐만은 아니다. 현재 미션 크리티컬한 비즈니스를 영위하고 있는 수많은 온라인, 오프라인 기업들에게 기업 이미지 혹은 브랜드 이미지라는 것은 이미 단순한 이름 그 이상의 것을 제공하고 있다.

기업은 어떠한 방법으로 데이터, 특히 이슈가 되고 있는 개인정보에 대한 보안을 확보하는 동시에 강화된 규제들을 손쉽게 준수하는 것과 같은 효율적인 보안 확보방안에 대해 데이터가 저장되어 있는 DBMS 측면에서 3가지로 분류하여 각각의 데이터 보안확보 유형 및 구현 방법에 대해 알아보고자 한다.

Ⅱ. 본론

데이터 암호화란 데이터 보안확보 유형 중 가장 일반화되어 있는 방식으로 기업 내 저장되어 관리되고 있는 데이터를 인증 받은 암호화 알고리즘을 통해 암호화하여 허가받지 않은 사용자에 의한 데이터 미디어(Disk) 및 백업본이 유출되더라고 이를 이용해 민감한 개인정보를 도용하지 못하도록 할 뿐만 아니라 네트워크를 통해 전송되는 데이터 패킷까지도 암호화하여 스니핑과 같은 해킹 기술을 이용하더라도 그림 5과 같이 데이터를 안전하게 관리할 수 있도록 한다 하지만, 이러한 데이터 암호화를 구현 시 고려해야 되는 사항은 어떠한 것들이 있는지 이에 대한 고찰이 필요하다.

첫째, 어플리케이션의 수정이 필요한지의 여부다. 대부분의 경우 데이터를 암호화하는 시스템들은 지금까지 잘 사용해 오던 시스템일 경우가 많으며, 이러한 경우

에 잘 사용해오던 수많은 어플리케이션 코드의 수정이 동반되어야 한다면 보안확보에 소요되는 경비가 지나치게 많이 소모될 뿐만 아니라 너무 번거롭기까지 하게 된다. 따라서 보안의 도입시 어플리케이션의 도입 여부는 반드시 점검해 보아야 할 사항이다.

둘째, 성능을 유지할 수 있느냐의 여부다. 데이터를 암호화한다는 것은 특정 알고리즘에 의해 해당 데이터를 변환하고 이를 필요시 다시 원래의 데이터로 복호화해야 하기 때문에 이에 소모되는 리소스 (CPU 파워와 같은)가 더 많이 소비되기 때문에 시스템 성능의 하락을 수반하는 경우가 많다. 이를 얼마나 최소화할 수 있는 것이 데이터 암호화의 또 다른 관건이며 O사 과 같은 DBMS 벤더들은 이러한 암/복호화를 커널 내부에서 수행케 함으로서 성능 하락을 최소화 할 수 있는 메커니즘을 제공한다[1].

인터넷의 급격한 확산으로 인해 수많은 어플리케이션들이 불특정 다수의 사용자에게 개방되어 있고 사용자 인증을 위해 개인 정보를 필요로 함에 따라 대부분의 기업들이 개인 정보를 자체 관리함으로서 개인정보 보호를 강화하기 위한 조치가 국내에서 방송통신위원회 주도로 대통령령으로 시행하게 되었으며 2009년 적용 대상 업체의 확대로 인해 국내 대부분의 기업에서는 이를 반드시 준수해야 하며 위반 시 벌금 및 처벌을 받게 된다.[2]

암호화, 접근제어, 감사의 세 가지 유형으로 구분한 데이터 보안 확보의 유형은 향후, 모바일 환경의 대두와 클라우딩 컴퓨팅으로 인한 IT 환경의 변화에 따라 지금까지의 보안 솔루션 벤더와 기업 모두에게 새로운 도전이 될 것이며 이러한 변화를 적극적으로 수용하며 지속적인 투자 및 연구개발을 통해 발전시키는 동시에 보다 다양한 기술과의 융합(압축과 같은)을 통해 그 영역을 확대 시키는 것이야 말로 현 보안 솔루션의 과제라 할 수 있다.

Ⅲ. 결론

다양한 보안 솔루션들이 존재하며 각각의 기술을 가지고 수많은 기업에서 사용되고 있는 이러한 솔루션들 중 최상의 선택을 한다는 것은 매우 어려운 일이다. 다만 위에서 언급한 세 가지의 보안유형으로 살펴보면 암호화, 접근제어, 감사의 측면에서 DBMS 벤더의 솔루션들이 가장 기술적으로 앞서 있으며 이는 성능부하 및 우회차단, 통합감사와 같은 요건들을 가장 잘 충족하고 있다고 할 수 있다.

최상의 보안 솔루션은 없다. 다만 항상 데이터 보안에 관심을 갖고 이를 유지 및 발전시킬 수 있는 의지와 이를 도와줄 수 있는 신뢰할 수 있는 솔루션의 결합을 통해 최선을 다하는 것이야 말로 최상의 보안 확보 유형이라 할 수 있다.

■ 참 고 문 헌 ■

[1] http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asointro.htm#i1008719
Advanced Security Administrator's Guide.

[2] http://law.go.kr/LSW/lsSc.do?menuId=0&p1=&query=%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D+%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84+%EB%B0%8F+%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8+%EB%93%B1%EC%97%90+%EA%B4%80%ED%95%9C+%EB%B2%95%EB%A5%A0&x=3&y=9
정보통신망 이용촉진 및 정보보호 등에 관한 법률/시행령,/시행규칙

[3] http://blog.daum.net/kcc1335/1890

[4] http://datalossdb.org