데이터 보안 강화 방법

잠재적인 데이터 침해 요소에 대해 대응할 때 데이터 소유권자와 시스템 관리자들은 제일 먼저 가장 뻔한 보안 관점에서 고려한다. 데이터 접속권한을 획득하려는 악의적인 의도를 가진 개별적 공격을 막는 것이다.

하지만 데이터 안전에는 비밀 데이터가 있어서는 안되는 곳에서 발견되지 않도록 하는 등 여러 측면을 고려해야 할 필요가 있다.

1.**악의적인 공격으로부터의 데이터 안전**

해커나 다른 불법적인 목적의 개인들로부터 데이터를 보호하는 것은 종종 꼭 해내야만 하는, 최우선 순위다.

IT 보안 전문가들의 영역은 보호 기술의 배치, 사용자 계정 및 승인 관리, 임직원의 퇴직 또는 직위 변경 시 계정의 디프로비저닝(deprovisioning)을 포함하고 있으며, 넓게는 공격을 탐지하는 침입 탐지과 필요하다면 접속을 끊어버리는 역할도 맡고 있지만, 이에 국한되지 않는다.

**2. 비인가 접속으로부터의 데이터 안전**

비인가 접속은 악의적인 공격보다 범위가 넓다. 비인가 접속은 접속을 허용해서는 안되는 이들이 데이터에 접속하거나 질의를 하게끔 하는 등 승인을 형편없이 규정해놓은 데서 기인한다.

 예를 들어 BI 사용자는 영업 성과를 분석하는 동안 인사나 급여정보에 접속할 수 있는 권한을 획득한다.

 이런 비인가 접속권한 형태는 악의적인 공격보다는 위험이 덜하며 부분적으로 명확하게 커뮤니케이션된 거버넌스 정책과 사용자의 프로의식을 통해 그 위험성을 완화시킬 수 있다. 예를 들어 비밀 데이터에 접속할 권한을 갖고 있다고 해서 그것을 필히 본다는 것은 아니다.

**3. 비일상적인 추출로부터의 데이터 안전**

사용자들은 그들 사업의 정상적인 프로세스 내에서 특정 데이터셋에 접속권한을 갖고 있을 지 모른다. 그러나 그들이 대량의 기록을 추출하려고 시도할 때에는 분명 다른 이유가 있는 것이다.

 사용자가 히스토리컬 보고서를 처리할 필요가 있는 것은 그들이 내일 고객 데이터베이스와 함께 회사를 나올 계획이든지, 혹은 소셜 엔지니어링 공격의 피해자일수도, 혹은 그들의 권한을 탈취당했을 수도 있다.

 한 사용자의 일상적이고 예상되는 행동의 범위를 확인하고 매일 일상적으로 사용하는 데이터가 어떤 것인지에 따라 장소를 제한하는 것은 데이터 유출을 막는데 중요한 수단이다.

**4. 의도치 않은 사용으로부터의 데이터 안전**

특정 환경에서의 사용했을 때, 같은 데이터라도 쓰임에 따라 엄청난 피해를 줄수 있다.

 좋은 데이터 거버넌스 정책은 데이터를 어떤 상황에서 사용할 수 있는 지 명확하게 규정해 놓은 것이다. 수많은 데이터가 무계획적으로 사용되고 있기 때문에 이는 항상 쉽지 않다.

 이런 상황에서 이를 제대로 적용하지 못하더라도 데이터 관리자는 이 정책의 취지만이라도 지켜야 한다.

**5. 예상치 못한 전송으로부터의 데이터 안전**

소스데이터는 안전할 수도 있다. 하지만 그러나 리포트, 추출, 그리고 다른 대상 데이터셋은 그렇지 못하다.

 노트북이 도난당하면 얼마나 많은 비밀정보들이 거기에 담겨져 있었는지가 기사와 뉴스의 소재가 되어 왔다.

 또한 데이터가 자체 데이터베이스에서 떠날 때, 이 데이터는 이메일, USB 스틱, 드롭박스 계정, 하드드라이브 등 극히 보안이 안되는 곳으로 흘러간다.

 이는 IT 부서가 대량의 파일들을 전송하기 위한 편리하고 안전한 방법을 제공하지 못하기 때문이다. 그래서 사용자들은 자신만의 전송 방법들을 알아낸 것이다.

 데이터 안전은 IT 인프라스트럭처 전반에 대한 것으로 확대되며 사용자의 행동과 편의 또한 계산해 넣어야 한다. 뿐만 아니라 간단한 데이터 조작 처리 업무를 확대해 명확한 가이드라인을 수립해야 한다.​