**데이터 보안 강화 방법 5가지**

최근 방영된 유퀴즈온더블럭이라는 예능 프로그램에서 화이트 해커 박찬암님을 소개해주며 일상에서 우리의 개인정보를 보호하고 해킹으로부터 예방할 수 있는 방법 몇 가지가 공유되었다. 그 예능 프로그램을 보고 난 뒤 나의 개인정보가 생각보다 많은 곳에 노출되어 있다는 것을 생각하게 되었고 무엇보다 나의 데이터가 결코 안전하리라는 보장이 없다는 것도 느끼며 스스로 개인정보를 더 잘 관리해야 한다는 경각심도 들었다.

그만큼 개개인의 정보는 생각보다 많은 곳에 노출이 되어 있고 시대가 흐를수록 공유라는 개념 아래에 정보의 접근성도 더 좋아질 것이다. 그렇지만 나의 정보에 권한이 없는 사용자가 침입을 하려고 할 때만큼은 나의 것을 지키기 위해서는 분명 사전에 조치할 수 있는 몇 가지 방법들이 있다. 나의 정보 및 데이터의 보안을 강화하여 지켜낼 수 있는 방법은 총 5가지로 가장 값진 데이터 파악, 크리덴셜 정리와 엄격한 내부 보안 경계선, 데이터 암호화 상태 유지 및 클라이언트 보호가 있다.

제일 먼저 나에게 놓인 데이터들 중 비즈니스적 가치가 가장 큰 데이터를 파악하고 그것의 민감도에 따라 데이터를 정리해야 한다. 우리가 생각하는 것보다 나의 개인적이고 프라이버시가 존중되어야 할 정보들이 생각보다 주변에 널려 있다는 사실을 간과해서는 안 되며 내가 애용하는 저장소들을 한 번씩 더 살펴볼 필요가 있다. 포털 사이트에서 무료로 제공해주는 클라우드 용량, 또는 유료로 대용량을 사용하는 유저들도 있다. 귀중한 데이터일수록 핵심 데이터로 정리를 하여 규모를 크지 않게 유지하는 것이 비결이다. 제일 예방에 적합한 습관은 데이터의 유효성을 관리하여 데이터의 사용 가치가 사라지면 바로 폐기를 하는 것이다.

내가 현재 종사하고 있는 곳에서 전산 관리 담당자는 각 그룹에게 알맞은 권한을 할당해주어서 나의 파트에서 필요한 데이터까지만 접속하여 데이터를 공유할 수 있다. 이와 같이 기업의 관리자들은 제한된 범위를 가지고 각 부서에 맡는 권한을 할당해줄 필요가 있으며 이 훈련이 데이터를 그 누구에게도 작은 범위라도 새어낼 위험을 대폭 낮출 수 있다. 엄격한 내부 그리고 외부의 규정으로 인하여 더욱 더 기업의 데이터베이스 그리고 회사원들의 개인 계정 정보들이 외부 그리고 내부의 양쪽의 침입으로부터 동시에 보호할 수 있는 것이다.

데이터 관리자들을 제외하고 각종의 크리덴셜을 최대한 노출시키지 않는 것을 주의해야한다. 예를 들면 Microsoft office를 깔고 회사의 모든 컴퓨터에 적용을 시킬 때 필요한 크리덴셜 암호들을 공유해서 남용하게 만들어서는 안 되며 직접 관리자들이 회사 컴퓨터에 필요할 때 탑재를 시켜야 한다. 그만큼 중요한 데이터의 크리덴셜들의 노출이 적어야 남용하는 사례도 적을 것이며 더 멀리 나아가 유출이 없어 외부적인 접근의 위험도 낮을 것이다.

더욱 더 철저히 데이터들을 암호화하여 데이터가 외부적인 흔적과 접근이 인지가 되면 바로 신호를 줄 수 있도록 준비시키는 것이 중요하다. 또한 내부적인 사원들의 주의하는 것이 아닌 클라이언트 즉 데이터를 이용하는 모든 이용자들을 보호하여 그들에게 필요한 데이터 보호 교육 및 주의점을 가르치고 어떻게 데이터를 활용하는지 각인을 시킬 필요가 있다. 결국 하나의 성벽이 무너지면 그 다음의 성벽이 무너지는 것은 시간 문제일 뿐이다.

이와 같이 다양한 방법으로 사소한 것부터 중요한 데이터를 외/내부의 침입으로부터 보호하고 정보를 그래도 유지하고 지켜내는 지 알아보았다. 이 외로도 바이러스 백신 소프트웨어를 업데이트하는 방법, 방화벽 사용, 승인된 기기만 접근 허용, 와이파이 암호 설정 등등 다양한 보안 강화 방법이 있다. 이러한 습관을 통하여서 개인의 그리고 기업의 소중한 정보를 최대한 누출되는 것을 막으며 악용되는 사례가 없도록 건강한 데이터 유저가 되자.