
# 소프트웨어 암호화 및 규정 준수: 주요 보안 위험성이 있는 저렴한 솔루션

## 규정 및 준수 요건

데이터 보안은 IT 부서에만 해당되곤 했지만 지속적인 소비자 데이터 위반 때문에 전 세계의 정부들은 개인적으로 식별 가능한 모든 데이터를 암호화하고 보호하기 위해 기업들에게 점점 더 많은 요건을 강요했습니다.

건강 관리 분야의 HIPAA부터 EMEA의 GDPR 및 캘리포니아의 CCPA까지, 보호된 데이터 클래스의 암호화는 규정을 통해 관리되고 있습니다. 규정 및 관련 벌금과 소송 관련 위험성이 급증함으로 인해 지난 3년 이상 동안 규정 준수 조직들이 기하급수적으로 증가했습니다.

이러한 변화 때문에 IT 부서들은 보안과 증가하는 비용을 따라가기 위해 노력했습니다. COVID 팬데믹 때문에 데이터 암호화에 초점을 맞추지 않고 추가적인 하드웨어 및 방화벽 투자에 예산이 소비되고 있습니다.

실제로 Microsoft BitLocker® 또는 Symantec, McAfee 등과 같은 회사들의 엔드포인트 관리 소프트웨어를 사용하는 소프트웨어 암호화가 강세를 보이고 있습니다. 몇몇 기업들과 소비자들은 일부 판매사가 제공하는 소프트웨어 "볼트" 드라이브가 장착된 표준 USB 드라이브 역시 사용합니다.

## 암호화 및 전송 중 데이터(DATA-IN-TRANSIT)

직원과 소비자는 그들의 데이터를 보유하고 있어야 할 필요가 있습니다. 직원과 소비자는 선택사항으로 다음을 사용할 수 있습니다.

1. 클라우드 서비스: 이는 인터넷 연결이 가능한 모든 장치에서 액세스할 수 있기 때문에 훌륭한 방법입니다. 그러나 유연성에는 비용이 따릅니다. 클라우드 상의 데이터 저장 공간은 사용자나 기업의 데이터 통제를 없애고 클라우드 서버가 잠금 해제되거나 접근이 허용된 상태로 남아있는 경우에서 볼 수 있듯이 잠재적인 위험성이 있습니다.
2. 표준 USB 드라이브: USB 드라이브를 가지고 다니는 것이 더 안전해 보일 수 있지만 드라이브 분실로 인한 데이터 노출 위험성이 매우 클 수 있습니다. 예를 들어, 비밀 정보가 들어 있는 분실 USB 드라이브가 발견되었다거나 세탁물 속바지에 분실된 USB 드라이브가 가득 들어있었던 사례들이 있습니다.
3. 하드웨어 암호화 USB 드라이브: 이러한 USB 드라이브에는 내장형 암호화 컨트롤러 및 액세스 제어를 포함하는 사용자 지정 아키텍처가 담겨 있습니다. 데이터는 일반적으로 XTS 모드에서 가장 강력한 AES-256비트 암호화를 사용하여 암호화되며, 기타 물리적 공격 및 펌웨어 기반 공격을 완화하는 가능한 보호 조치도 함께 사용됩니다. 이러한 드라이브는 보안 장치를 전문으로 하는 기업에서 제조하며, 표준 USB 드라이브보다 가격이 더 비싸긴 하지만 더 훌륭한 데이터 보안을 제공합니다. FIPS 197 또는 FIPS 140-2 Level 3 드라이브는 보다 뛰어난 수준의 보호를 더해주고 안심할 수 있게 해줍니다.
4. 소프트웨어 암호화를 사용한 표준 USB 드라이브: 규정에서 요구하는 보안을 위해 BitLocker를 이용한 소프트웨어 암호화나 기타 도구를 사용할 수 있습니다. 이러한 것들은 상대적으로 가격이 덜 비싸고 동일한 AES-256 XTS 암호화를 제공하기 때문에 적당한 선택사항이라고 할 수 있습니다.

대부분의 경우 기업 및 산업계가 네 번째 선택사항인 소프트웨어 암호화를 사용하는 표준 USB를 선택하는 경향이 있는 것도 놀라운 일이 아닙니다. 왜냐하면 BitLocker나 기타 데이터 볼트 유틸리티와 같은 소프트웨어 암호화가 "무료"이기 때문입니다.

## 소프트웨어 암호화는 규정을 준수한 것이 아닙니다


기업 보안 전문가의 경우 소프트웨어 암호화는 더 값비싼 하드웨어 암호화 USB 드라이브와 완전히 동일한 암호화 기능을 제공할 수 있습니다. 그러나 이것은 올바른 방법일까요? 예산이 제한되어 있기 때문에 기업들은 소프트웨어 기반 암호화의 어두운 면을 알지 못한 채 규정 준수 목적으로 소프트웨어 암호화로 몰려듭니다.

소프트웨어 암호화 USB 드라이브의 문제점은 무엇입니까? 저장된 상태의 데이터(data-at-rest)와 전송 중인 데이터(data-in-transit)가 AES-256 XTS 등급으로 암호화되지 않습니까? 일반적으로, 그렇습니다. 문제는 바로 소프트웨어 암호화가 "제거할 수 있는 암호화"로 여겨진다는 데 있습니다.

잠시만요, 제거할 수 있다구요? 그 말은 사용자가 소프트웨어 암호화가 적용된 USB 드라이브의 암호화를 비활성화할 수 있다는 뜻입니까?

정답을 말하자면, 맞습니다. 사용자는 소프트웨어 암호화 기능을 자신의 USB 드라이브에서 제거할 수 있습니다. 왜 그렇게 하겠냐구요? 왜냐하면 일단 그렇게 하는 것이 가능하고, 또 사용자들이 암호를 사용하지 않고 파일에 액세스하기를 원하거나 단지 암호를 잊어버렸지만 USB 드라이브를 사용해야 하기 때문입니다.

## 암호화 USB 드라이브에서 소프트웨어 암호화를 제거하는 방법

데이터에 액세스하기 위해 복잡한 암호나 기타 암호를 입력하고 싶어하지 않는 사용자의 경우 다음의 간편한 과정을 거치면 됩니다.

1. 소프트웨어 암호화 드라이브를 컴퓨터에 삽입합니다
2. 드라이브를 포맷합니다
3. 드라이브를 포맷하고 나면 모든 암호화가 제거됩니다
4. 비밀 또는 기밀 정보가 들어 있는 파일을 드라이브에 복사하여 쉽게 액세스할 수 있습니다

이것은 사용자들이 제한이 걸려 있지 않은 컴퓨터를 사용하여 쉽게 할 수 있는 방법입니다. IT 부서에서는 회사 컴퓨터에서 포맷 명령어 사용을 제한했지만 회사 컴퓨터가 아닌 다른 모든 컴퓨터에서 이를 쉽게 수행할 수 있습니다.

규정 준수 목적 - 데이터 암호화 제거가 용이하다는 것은 위의 방법을 통해 암호화가 제거되고 나면 비록 드라이브에 암호화된 상태로 있었던 데이터가 영영 유실된 것으로 여겨진다 하더라도 회사에서 제공한 드라이브가 이제 암호화되지 않은 상태임을 의미합니다. 암호화를 제거하고 난 드라이브에 복사된 모든 데이터는 보안이 유지되지 않고 잠재적으로 규정 준수에서 벗어난 것으로 여겨지며, 이로 인해 HIPAA, GDPR, CCPA, 그 외 다수의 규정을 위반할 위험이 있습니다.

## 암호화되지 않은 드라이브 분실로 인한 결과

기업에서 지정한 USB 드라이브를 분실했다가 찾은 경우, 해당 기업이 처음에는 이를 몰랐다가 나중에 소셜 미디어를 통해 그 점을 알게 되더라도, 특별 규정 준수 요건으로 인해 기업에 다음과 같은 처분이 내려질 가능성이 있습니다.

1. 어떤 데이터를 유실했는지 규명하기 위한 법의학 조사 수행
2. 법률 부서와 상의하여 법률 위반이 발생했는지 확인
3. 고객에게 알려야 하는지 결정

이러한 사례는 단 하나의 USB 드라이브 분실이 값비싼 결과를 가져올 수 있음을 보여줍니다. 시간당 수백 달러를 뛰어 넘는 법률 비용을 감안하면 이러한 규정 준수 프로세스는 수백만 달러의 비용으로 이어질 수 있으며, 그에 더해 벌금, 고객 및 기타 소송 그리고 데이터 노출로 인한 난처한 상황을 감당해야 할 가능성도 있습니다.

낮은 비용으로 구현할 수 있다는 이유로 소프트웨어 암호화를 고려할 때 이러한 위험성과 그로 인한 막대한 재정적 결과는 고려되지 않습니다.

회사 네트워크에서 암호화되지 않은 USB 드라이브 사용을 허용하는 것에는 또 다른 위험성이 있습니다. 흔히 이를 가리켜 “BadUSB”라고 합니다. BadUSB는 사이버 범죄자가 USB 저장 드라이브를 통해 기업의 방화벽을 침범하고 기업의 사이버 방어를 뚫어 악성 프로그램을 침투시키기 위해 사용해 왔던 악성 프로그램의 일종입니다.

### BadUSB


USB 드라이브가 컴퓨터에 삽입되면 펌웨어를 통해 컴퓨터의 칩셋 컨트롤러가 USB 드라이브 컨트롤러와 응답 확인(handshake)을 시작합니다. 이러한 응답 교환은 Microsoft/macOS/Linux 등의 운영 체제에서 USB 드라이브가 연결되었음을 알아채기도 전에 발생합니다. 모든 USB 드라이브에는 드라이브가 USB 포트에 연결될 때 실행되는 펌웨어가 있습니다.

사이버 범죄자들은 이러한 응답 확인 메커니즘을 통해 USB 드라이브에서 실행되는 펌웨어를 악의적인 또 다른 펌웨어로 교체하는 방식으로 악성 프로그램을 심을 수 있다는 것을 알게 되었는데, 이러한 악의적인 펌웨어는 목표 컴퓨터 시스템이 USB 드라이브와 통신할 때 시스템에 악성 프로그램을 심습니다. 표준 USB 드라이브에는 컨트롤러에 의해 실행되는 내부 펌웨어에 대해 보안이 되지 않습니다. 이를 통해 양호한 USB 드라이브를 무기화하여 방화벽을 뚫고 사이버 방어에 구멍을 내기 위해 BadUSB가 탄생했습니다.

대부분의 기업은 자신들의 시스템에서 USB 사용을 금지하거나 심지어 USB 포트를 에폭시로 채우기까지 합니다. 그러나 여러 부류의 직원들이 데이터를 USB 드라이브에 담아 소지하고 다녀야 한다는 점을 알게 되었습니다. 예를 들어, 임원진이 데이터를 가지고 다니면서 작업을 하거나 그러한 데이터를 기업 클라우드에 액세스할 수 없는 외부 법률 또는 재정 고문에게 제공하기를 원하거나, 기업 하청업자들이 작업을 위해 데이터를 필요로 하지만 기업 데이터베이스에 액세스가 제한되어 있거나, 월별 보고서 마감을 서둘러야 하는 재무 분석가가 집에서 스프레드시트 작업을 해야 하는 경우가 있을 수 있습니다.

이전 분석에서 볼 수 있듯이 이러한 표준 USB 드라이브와 소프트웨어 암호화가 결합된 솔루션을 사용하는 데는 큰 위험이 따릅니다. 언뜻 보기에 더 저렴해 보이는 솔루션이 잠재적으로 매우 해롭고 훨씬 더 비싼 비용을 치르는 것으로 드러났습니다. 잠재적인 데이터 위반에 대해 변호사와 2~3시간 상담하는 비용만 해도 저렴한 솔루션 사용으로 절감된 비용을 날려버립니다.

## 하드웨어 암호화 USB 드라이브는 규정 준수를 위한 최상의 선택사항입니다

하드웨어 암호화 USB 드라이브를 최상의 선택으로 만들어주는 것은 다음과 같은 규제 적용입니다.

1. 하드웨어 암호화 USB 드라이브에는 암호화가 언제나 활성화되어 있습니다. 사용자가 암호화 기능을 꺼버리거나, 암호 규칙(최소 길이, 복잡성)을 재설정하거나 자동 암호 재시도를 비활성화할 수 있는 방법이 없습니다. 소프트웨어 사전 공격을 통한 반복적인 암호 추측을 막지 못하는 소프트웨어 암호화와는 다르게, 하드웨어 버전은 암호 재시도를 제한하며, 잘못된 암호를 10회 입력하거나 때로는 그보다 더 적은 횟수로 입력했을 때 데이터를 잠급니다. 이는 수퍼 컴퓨터 시대에 매우 안전한 방법입니다.
2. 하드웨어 암호화 드라이브는 프리미엄 암호화 컨트롤러를 사용하며 다음과 같이 다양한 보안 기능을 포함합니다. 항상 모든 보안 대책을 공개하지 않는다 하더라도 BadUSB로부터 보호할 대책이 갖춰져 있습니다. 공장에서 펌웨어를 하드웨어 암호화 드라이브에 로딩할 때에만 펌웨어를 디지털 방식으로 서명하고 로딩합니다. 즉, 그러한 암호화 USB가 삽입되면 암호화 컨트롤러가 먼저 디지털 서명을 통해 펌웨어의 무결성을 점검하고 검증을 통과하는 경우에 한하여 USB를 로드합니다. 펌웨어를 교체하려는 모든 시도는 드라이브를 차단하여 기능할 수 없게 하므로 위협이 되지 않습니다.
3. 하드웨어 암호화 USB 드라이브에는 특정 기업용으로 설정한 사용자 지정 제품 ID(PID)가 담겨 있습니다. 이러한 프리미엄 드라이브에는 내부에 디지털 식별자를 프로그래밍할 수 있으며, 이를 통해 드라이브가 기업 내부에서 또는 외부 방화벽을 거쳐 연결되는 경우 해당 드라이브가 기업 발행 드라이브인지 식별할 수 있습니다. 예를 들어, 어떤 직원이 회사 드라이브를 분실하고 동일한 모델을 소매점에서 구매한 경우 새로 구매한 드라이브는 회사 네트워크에서 인증되지 않습니다. 이러한 주문 제작은 USB 드라이브 사용에 또 다른 보안 계층을 추가해 줍니다.
4. 하드웨어 암호화 드라이브는 매우 신속하게 비용을 절감합니다. 위험 감축 및 제거만 해도 자금 회수 주기가 매우 짧게 단축됩니다.

Kingston은 세계 최대 암호화 USB 드라이브 제조업체로서 다양한 기능과 기준 가격의 드라이브 제품군을 제공합니다. 직접 Kingston에 문의하셔서 임원진, 직원, 하청업체 및 기타 관계자를 위한 암호화 USB 솔루션으로 규정 준수 유지에 도움될 수 있는 방법에 대해 논의하시기 바랍니다.