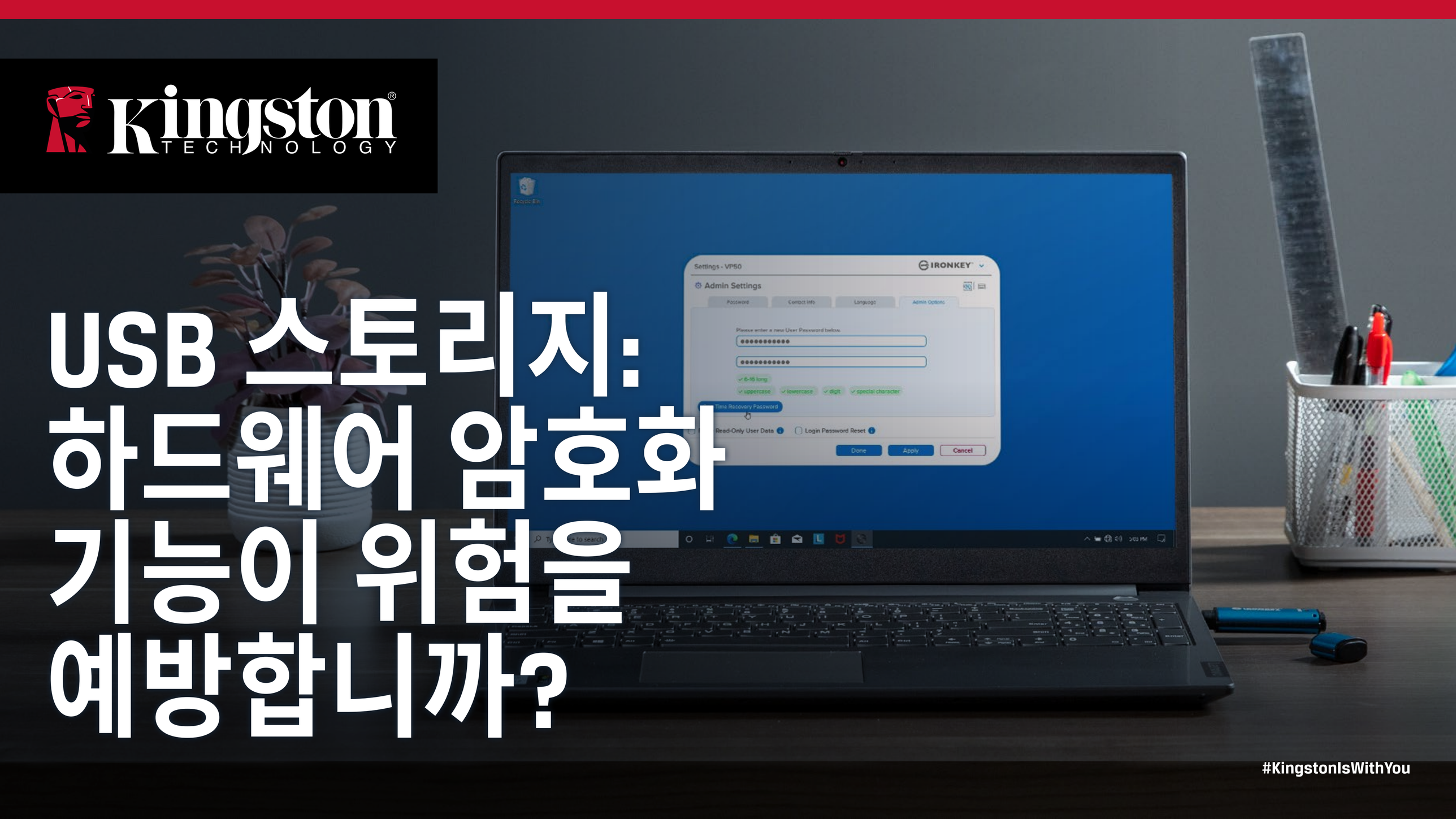
Kingston TECHNOLOGY

USB 스토리지: 하드웨어 암호화 기능이 위험을 예방합니까?



#KingstonIsWithYou

USB 스토리지: 하드웨어 암호화 기능이 위험을 예방합니까?

서문 및 목차

사이버보안은 그 어느 때 보다 기업에게 더 큰 우려로 떠오르고 있지만 너무나 많은 기관들은 사이버보안 위협에 대한 지식이 없고 이에 준비가 되어 있지 않습니다. 미국 기업 중 단 50%만이 사이버보안 계획을 실행하고 있고, 이중 23%는 COVID-19 팬데믹이 시작된 이후로 사이버보안 계획을 최신화하지 못한 상황으로 UpCity에 따르면 많은 기업들이 원격 또는 하이브리드 작업 모델을 다른 곳으로 이전하고 있는 것으로 나타났습니다. 사이버공격의 빈도가 전 세계적으로 늘어가고 있고, 랜섬웨어 공격을 받은 기업의 숫자가 2020년 37%에서 2021년 66%로 늘었습니다[1].

사이버공격으로 인한 금전적 손실, 데이터 손실, 안전뿐만 아니라 취약한 사이버보안은 비지니스에 심각한 영향을 미칠 수 있으며, 이로 인해 단기 및 장기적으로 다양한 형태로 기업에 부정적인 영향을 줄 수 있습니다.

사이버보안 위협을 유발하는 공통적인 매체 한 가지는 USB 드라이브입니다. 이는 사용하기 간편해서 기기에 꽂기만 하면 바로 사용할 수 있기 때문에 여러 기관에서 그 사용이 보편화되어 있습니다. 하지만 바로 이 간편성 때문에 USB 드라이브는 공격에 매우 취약하고, 드라이브 한 개를 다른 곳에 두거나 도난을 당하기만 해도 악의적인 사람은 민감한 데이터에 액세스할 수 있습니다. 이러한 점 때문에 암호화는 USB 드라이브 사용을 안전화하고 개인 및 기관의 모든 관련 위험을 완화하는 데 상당한 역할을 할 수 있습니다. 이 eBook에는 다음 질문에 대한 답변이 제시되어 있습니다.

- 왜 USB의 암호화가 사이버공격을 방어하는 데 중요할까요?
- 어떤 기관이 스스로를 취약하게 만들까요?
- 자체적인 방어를 위해 기관은 무엇을 해야 할까요?

USB 스토리지: 하드웨어 암호화 기능이 위험을 예방합니까?

기고자

이 eBook은 IT 및 신생 기술의 주요 산업 인사와 당사의 자체 기술 전문가의 도움을 얻어 제작했습니다.

David Clarke

David는 Thompson Reuter가 선정한 “영국의 소셜 미디어, 위험 관리, 규정 준수 및 레그테크 분야에서 가장 영향력 있는 이론가 및 사상가 30명” 중 최고 영향력 있는 10명으로 인정받고 있으며, Kingston Technology의 최고 글로벌 전문가 50명에 선정되었습니다.

Pasi Siukonen

Pasi는 Kingston 제춤의 PR, 마케팅, 필드세일즈, 기술 지원 및 고객서비스 등 Kingston 부서를 지원하는 전문가팀을 총괄하고 있습니다. 그의 주요 담당 제품은 Flash 및 SSD 제품 라인입니다.

일반 드라이브와 암호화된 드라이브의 차이점

일반(암호화되지 않음) 드라이브는 액세스와 사용이 매우 간편한 반면, 암호화된 하드웨어는 물리적 및 디지털 측면에서 보안을 몇 단계 더 강화할 수 있어서 USB 스토리지가 훨씬 더 안전해집니다. 암호화되지 않은 일반 드라이브는 사용하기 간편하고, 비용이 저렴하고, 휴대하기 간편해서 사용자가 편리하게 사용할 수 있는 반면, 민감한 데이터를 도용하거나, 기업 네트워크로의 악성소프트웨어 또는 랜섬웨어의 침투 등을 의도하는 악의적인 사람도 편리하게 사용할 수 있습니다. USB가 너무나 빈번하게 사용되므로 사이버공격의 가능성도 그만큼 높습니다. 일반 드라이브와 관련된 주요 위험에는 두 가지가 있습니다:

- **랜섬웨어 공격:** 이러한 USB 기반 공격의 수법은 악성 소프트웨어를 기업의 네트워크로 침투시켜 네트워크를 암호화함으로써 기업 정보 및/또는 시스템을 위험에 처하게 합니다. 이러한 공격은 종종 BadUSB로 인해 야기되고 이는 가장 널리 알려진 종류의 악성 소프트웨어가 되었습니다.
- **데이터 도용:** 적절한 보안 장치를 설치하지 않고도 드라이브를 분실 또는 도난 당하거나 제대로 간수하지 못하기만 해도 악의적인 사람은 드라이브에 저장된 데이터가 고객 정보, 원시 코드 또는 민감한 재무 및 성과 데이터 등 종류와 관계없이 데이터에 쉽게 액세스할 수 있습니다.

BadUSB는 보호기능이 없는 펌웨어를 사용하여 USB 드라이브의 취약성을 악용할 수 있는 공격으로서 악성 소프트웨어로 프로그래밍될 수 있습니다. 이러한 악성 도구들은 놀라울 정도로 일반화되어 사이버범죄자들이 쉽게 사용할 수 있지만, 이러한 악성 도구에 대한 인식 수준은 여전히 낮으며, 이러한 공격은 일반 드라이브의 펌웨어를 해킹된 펌웨어로 교체하여 USB 드라이브가 키보드로 위장하고 방화벽을 공격하는 스크립트를 기본적으로 실행하는 방식으로 매우 쉽게 수행할 수 있습니다. 대부분의 사이버공격은 악의적인 의도와 관계없이 인식하지 못하는 내부자들을 통해서 실행되므로 기업들이 보호되고 디지털 서명된 펌웨어가 설치된 암호화된 드라이브를 사용하고 사이버공격을 예방하여 사이버범죄자들의 범죄 성공률을 낮추는 것이 가장 중요합니다.

> 인프라의 재건 비용 및 랜섬 및 기타 도용으로 인한 피해 비용은 USB의 관리 비용과 비교할 때 막대합니다.
> - David Clarke

왜 암호화된 USB를 사용할까요?

암호화된 드라이브는 안에 담긴 데이터뿐만 아니라 드라이브에 연결할 장치를 보호하도록 특수 설계되어 있어 모든 기관의 IT 장비에서 중요한 도구입니다. 사이버보안 위협이 점점 고도화됨에 따라 암호화된 드라이브의 기능도 함께 고도화되어 이러한 장치를 악용하려는 사이버범죄자들보다 앞서 나가고 있습니다. Kingston IronKey™ 하드웨어 암호화된 제품군에서 알 수 있는 바와 같이 가장 강력한 모드의 AES 256 비트 암호화, 단단하고 변조 방지처리된 케이스, 디지털 서명된 펌웨어, 가상 키보드, 복소 또는 패스프레이즈 모드 등과 같은 기능이 지난 수년간 개발되고 추가되어 사용자를 각종 공격으로부터 완전히 보호하도록 보장합니다.

종종 사이버위험에 대한 이해가 부족하기 때문에 일반 드라이브가 다양한 취약성을 드러냄에도 불구하고 많은 기업들은 일반 드라이브 사용을 선택합니다. 플래시 드라이브에 대한 기업의 승인 절차 미비가 이러한 선택에 기여한 것처럼 드라이브 사용의 편리성 및 드라이브의 저렴한 비용, 암호화의 저렴한 비용도 기여합니다. ISO27001, GDPR, SOC2 및 WISP 정부의 우수관행와 같은 다양한 IT 및 사이버보안 기준을 준수하라는 우수관행 정책 또는 절차가 마련된 기업은 거의 없습니다. 이는 위험은 종종 증거가 아니라 의견에 근거하여 평가되고 많은 기관들은 공격에 취약한 상태가 된다는 의미입니다.

일부 사람들은 기존의 소프트웨어 암호화 도구를 사용하여 일반 드라이브를 사용하는 반면, 많은 소프트웨어 암호화 드라이브를 인터넷에서 누구나 사용할 수 있는 무료 또는 유료 도구로 해킹할 수 있기 때문에 이는 종종 허위 절약일 수 있습니다. 또한 사용자가 드라이브를 다시 포맷팅만 하면 드라이브에서 소프트웨어 암호화를 제거할 수 있어 편리하고 비지원 OS 플랫폼에서 드라이브를 사용할 수 있습니다. 하드웨어 암호화된 USB는 인터넷 상시 접속 시 암호화 기능이 실행되며 이는 끌 수 없고, 용도에 적합하고, 변조 방지 및 개봉 확인이 가능하도록 설계되어 드라이브의 진품 및 무결성을 보장합니다. IronKey VP50와 같은 암호화된 드라이브에는 비밀번호 시도 제한(억지기법 공격 보호) 및 가상 키보드(키 로깅 및 스크린 로깅 보호)의 2가지 기능이 더 포함되어 있으며 이는 인식하지 못하는 사용자로부터 비밀번호를 빼내려는 악의적인 사람들에 대한 우수산업기준을 준수함을 의미합니다.

> IronKey 드라이브는 펌웨어가 변조되었다고 탐지할 경우, 드라이브 기능을 정지시키고 부팅하지 못하게 함으로써 사이버보안을 강화합니다.
> - Pasi Siukonen

누가 위험에 직면할까요?

실제로 USB 액세스를 컨트롤할 수 없는 기업들이 위험에 처하고, 종종 이런 기업들은 자신들이 어떤 위험에 직면하고 있는지 정확하게 인식하지 못합니다. 하지만 여러 요인들로 인해 특정 기업은 사이버공격에 대한 보다 매력적인 표적이 되고 더 나아가 취약한 표적이 될 수 있습니다.

의료 기업 및 금융 기업의 데이터는 사이버범죄자들의 훨씬 매력적인 대상일뿐만 아니라 기관과 고객 모두에게 보다 심각한 영향을 줍니다. 2017년 영국에서 발생한 NHS를 표적으로 한 사이버공격으로 19,000건 이상의 예약이 취소되었고 NHS는 9천2백만 파운드 규모의 생산 손실뿐만 아니라 데이터 및 시스템 복구 비용의 피해를 겪었습니다. 이로 인해 환자들은 의료관리를 받지 못했을 뿐만 아니라 NHS는 이전의 사이버위험 공격에 대해 신속하게 또는 실질적으로 대응하지 못했다는 엄중한 비난을 받았습니다. 모든 기관들은 사이버보안에 대해 최신의 상태를 유지하고 충분한 정보를 가지고 있어야 하는 반면, 민감 정보, 특히 특수한 범주의 데이터를 취급하는 기관들은 사이버보안에 대한 경계심을 배가해야 합니다.

매출 측정을 기준으로 기업의 가치가 높을 수록 악의적인 사람에 대한 보상이 크므로 사이버위협으로부터 이들이 직면하는 위험도 더 커지게 됩니다. 하지만 그렇다고 해서 중소기업들은 사이버보안을 우려하지 않아도 된다는 의미는 아니며, 기업들은 보다 매력적인 공격 대상이 될 수 있는 반면 종종 사이버위협을 해결하는 자원과 전담 직원이 마련되어 있습니다. 다른 한편으로 많은 중소기업(SMB)에는 사이버보안 전담팀이 구축되지 않았고 고위 관리는 USB 관리를 하지 않도록 예외로 하고 있어서 SMB는 특히 사이버공격에 취약하고 심각한 결과를 초래합니다. 일부 연구 결과에 따르면 중소기업은 실제로 보다 더 사이버공격의 표적이 됩니다.

고위 관리직의 직원들의 경우 이러한 위험이 훨씬 크며, 이러한 사람들은 기관 내에서 추적이 수월하고 종종 간부 특권을 가지며 USB 관리 절차와 같은 사이버 통제조치가 이들에게는 적용되지 않아서 사이버범죄자들은 이들을 수익성 높은 표적으로 삼고 있습니다. 따라서 인터넷에 상시 접속되며 하드웨어 암호화된 드라이브뿐만 아니라 사이버보안에 대한 충분한 정보 및 다음의 우수기준 및 절차를 통해 오랫동안 위험을 줄이고 공격을 보호할 수 있습니다.

> 가장 최근에 일어난 많은 유출사건은 내부자들이 의도적으로 또는 비의도적으로 내부자의 도움을 사용하는 것을 전문으로 하는 악의적인 사람들이 저질렀습니다 - David Clarke

누가 위험에 직면할까요?

> 기관들은 사이버보안 위협을 막을 수 있는 충분한 조치를 취하지 않고 있습니다. - David Clarke

공급망은 기관이 가지는 잠재적 취약성의 다른 측면이고 모든 공급망 공격은 매우 일반적으로 일어납니다. 2013년 미국의 소매업체인 Target은 소매 이력 데이터의 최대 유출사건 중 하나로 타격을 입었고 4천만 명 이상의 고객에 대한 직불 카드 및 신용 카드의 정보가 유출되었습니다. Target 자체는 사이버보안에 대해 매우 우려했지만, 사고가 나기 6개월 전에 확대된 사이버보안 시스템을 설치했기 때문에 공격자들은 Target의 제 3자 공급업체 중 한 곳에 침투하고 공급업체를 통해 Target 메인 데이터 네트워크에 액세스했습니다. Target을 상대로 총 90건의 소송이 제기되었고, Target은 유출 사건에 대응하느라 6천1백만 달러의 손실을 입었으며, 공급망은 공격에 대한 직접적인 책임은 없지만 공급망의 사이버보안에 대한 취약성은 금전 및 평판 측면에서의 피해를 야기하기에 충분했습니다.

또한 직원의 차선책이 취약성의 원인이 될 수 있습니다. 직원들은 이러한 차선책을 사용함으로써 일상적인 업무를 보다 효율적으로 처리할 수 있지만 비밀번호 관리와 같은 기본적인 보안 프로세스 및 모범기준이 너무나 자주 간과될 것입니다. NCSC 및 CISA 지침은 상당히 간단하지만 특히 IT 및 사이버보안에 대해 친숙하지 않은 팀원들이 이를 실제로 실행하기 어려운 경우가 종종 있습니다. 사이버보안 전담팀을 구축하면 유용할 것이 분명하지만 하드웨어 암호화된 드라이브와 같은 적절한 도구를 직원에게 제공하면 직원의 차선책으로 인한 위험을 장기적으로 완화할 수 있습니다.

> 현재 하드웨어 암호화된 USB 드라이브는 여러 인터페이스(그래픽, 키패드, 터치스크린)부터 폭넓은 운영 체제 지원에 이르고 기관의 모든 요구사항을 충족하는 기능을 포함하는 기존의 사이버보안 정책을 채택하고 이에 통합하기 쉽습니다. - Pasi Siukonen

기관은 어떻게 사이버공격의 위험을 줄일 수 있으까요?

기관의 관점에서 볼 때 엔드포인트의 보안을 유지하고 데이터를 보호하려면 여러 가지의 일을 실행해야 합니다. GRC(거버넌스, 위험, 규정 준수)를 포함하지 않는 사이버보안은 실패할 수 밖에 없으므로 여러 프로세스를 숙지하고 따르는 것은 기업의 자체적인 보호를 위해 매우 중요합니다. 또한 강력한 엔드포인트 보안 소프트웨어를 실행하면 많은 사이버위협을 무력화할 수 있을 뿐만 아니라 모든 보안 취약성에 대한 패치 프로그램에 관한 한 대응할 수 있습니다.

> 시행된 암호화 정책을 채택할지 여부는 데이터 백업을 선택할지 여부만큼이나 중요하거나 위험 관리에 대해 심지어 더 중요한 문제일 수 있습니다. - Pasi Siukonen

하지만 개인적 차원에서 암호화된 하드웨어는 사이버보안 위협에 대한 취약성을 대폭 줄일 수 있습니다. 원격 및 하이브리드 작업이 부상하고 지속되며, 특히 이런 현상에 지난 해 사이버공격의 증가와 맞물리는 상황에서 조직 내 모든 레벨의 직원들이 회사 데이터를 안전하게 처리하고 이전하고 판독하도록 보장하는 것이 그 어느 때보다 더 중요해지고 있습니다. 사용자는 하드웨어 암호화된 USB를 사용하여 플래시 드라이브의 휴대성 및 간편성으로부터 계속 혜택을 얻을 수 있는 동시에 플래시 드라이브 관련 위험을 상당히 줄일 수 있으며, 일반 드라이브를 다른 곳에 두거나 도난을 당하면 데이터, 금전, 평판 등을 잃을 수 있지만 하드웨어 암호화된 드라이브는 다양한 범위의 공격으로부터 민감한 데이터를 보호하도록 설계되었습니다. 그리고 사이버범죄자들이 새로운 공격방식을 개발함에 따라 암호화된 드라이브는 지속적으로 진화하여 새로운 위험에 맞설 것입니다.

사이버공격의 총 대응 비용은 엄청날 수 있습니다. 실질적으로 기관 차원에서 암호화된 드라이브를 채택하고 사용할 때 더 많은 승인 및 설치가 필요할 수 있는 반면, 이는 도용 피해액, 및 장기적인 평판 손상으로 인한 수익 손실 측면 모두에서 회사에 상당한 비용을 절감시킬 수 있습니다. 유출 사건 1건에 대한 소송 비용으로 하드웨어 암호화된 USB 드라이브의 추가 비용을 지불할 수 있습니다.

> 철저히 암호화된 USB 솔루션을 제공하겠다는 장기적인 약속을 기반으로 한 Kingston의 포트폴리오를 통해 모든 기관은 사이버보안 구성, 예를 들어 하드웨어 암호화를 실행한 산업 표준, 엔드포인트 정책 준수 설계 및 장치 관리 성능을 충족할 수 있습니다.
> - Pasi Siukonen

요약

Kingston은 항상 사이버보안 영역의 발전을 연구하여 IronKey 암호화된 드라이브는 최신의 요구사항으로 최신 상태를 유지하고 대기업과 중소기업 모두의 사이버보안 요구사항을 충족시키도록 보장합니다. 사이버보안에 대한 우려가 전 세계적으로 계속 증대되고 있는 가운데, Kingston은 적절한 도구와 정보의 자유로운 사용을 통해 기관은 이러한 문제를 정면으로 해결하는 동시에 기관 자체, 직원 및 고객을 보호하도록 철저히 준비할 수 있다고 확신합니다.

Kingston 소개

Kingston은 35년이 넘는 경험으로, 모바일 데이터 문제를 식별하고 해결할 지식을 보유하고 있으며, 그리하여 귀사 직원이 조직을 위태롭게 하지 않으면서 안전하게 업무를 할 수 있도록 도와드립니다.

#KingstonIsWithYou

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021