KINGSTON IRONKEY™

Hardwareverschlüsselung im Vergleich zu Softwareverschlüsselung

Die wichtigsten Unterschiede und welche Option für Ihre Anforderungen die bessere ist.

Im andauernden Kampf um Datensicherheit liegt der Unterschied zwischen Hardware- und Softwareverschlüsselung darin, wo die Sicherheitsmaßnahmen angesiedelt sind und wie anfällig sie im praktischen Einsatz sind. Bei USB-Sticks und SSDs hängt es davon ab, wo die Verschlüsselung integriert ist, wie sicher die Daten geschützt sind und inwieweit sie vom umgebenden System abhängig sind.

HARDWARE	VS	SOFTWARE
Verwaltung von Verschlüsselungsschlüsseln Verschlüsselungsschlüssel werden intern von der Hardware erzeugt und sicher auf dem Laufwerk gespeichert.		**Verwaltung von Verschlüsselungsschlüsseln** Das Passwort des Benutzers wird direkt als Verschlüsselungsschlüssel verwendet, und die Schlüssel können sich im Systemspeicher befinden.
Schutz vor Brute-Force-Angriffen Entwickelt zum Schutz vor Brute-Force-Angriffen, indem die Anzahl der Versuche begrenzt wird, bevor sich das Laufwerk selbst löscht, wodurch verhindert wird, dass jemand an die Daten gelangen kann, falls das Laufwerk verloren geht oder gestohlen wird.		**Schutz vor Brute-Force-Angriffen** Empfindlich für Brute-Force-Angriffe, denn der Computer versucht, die Anzahl der Entschlüsselungsversuche zu begrenzen, doch Hacker können auf den Arbeitsspeicher des Computers zugreifen und den Versuchszähler zurücksetzen.
Software- oder Treiberanforderungen Auf dem Host-System sind keine Treiber oder Softwareinstallationen erforderlich.		**Software- oder Treiberanforderungen** Erfordert die Installation von Software und Treibern. Die Betriebssystemkompatibilität kann variieren.
Ressourcen zur Verschlüsselung Verwendet einen speziellen kryptografischen Prozessor, der direkt in das Laufwerk integriert ist.		**Ressourcen zur Verschlüsselung** Nutzt die CPU und die Systemressourcen des Host-Computers, um Daten zu verschlüsseln und zu entschlüsseln.
Abhängigkeit vom Host-System/Offenlegung Die Sicherheitsfunktionen sind innerhalb des Geräts isoliert und bleiben auch dann geschützt, wenn das Gerät mit nicht vertrauenswürdigen oder infizierten Computern verbunden ist.		**Abhängigkeit vom Host-System/Offenlegung** Die Sicherheit hängt vom Betriebssystem des Hosts ab und ist gefährdeter, wenn der Computer mit Malware infiziert ist.
Verschlüsselungsstatus Die Verschlüsselung ist so ausgelegt, dass sie immer aktiv ist und nicht entfernt oder umgangen werden kann.		**Verschlüsselungsstatus** Die Verschlüsselung kann aktiviert, deaktiviert oder falsch konfiguriert sein.
Auswirkungen auf die Leistung Kaum Auswirkungen auf die Leistung, da die Verschlüsselung auf den Hardware-Prozessor ausgelagert wird.		**Auswirkungen auf die Leistung** Dies kann die Leistung beeinträchtigen, da die Verschlüsselung CPU-Ressourcen beansprucht.
Flexibilität Die Verschlüsselung ist an den jeweiligen USB-Stick oder die jeweilige SSD gebunden.		**Flexibilität** Kann in jedem beliebigen Speichermedium implementiert werden.

Softwareverschlüsselung bietet Flexibilität, während Hardwareverschlüsselung die Sicherheit isoliert und weniger anfällig für Risiken auf Systemebene macht. Wenn Sie verstehen, wie die einzelnen Maßnahmen Daten schützen und den Zugriff regeln, können Sie das geeignete Sicherheitsniveau für Ihre Arbeitsabläufe und Ihr Risikoprofil auswählen.

www.kingston.com/ironkey