KINGSTON IRONKEY™

Szyfrowanie sprzętowe a programowe

Poznaj najważniejsze różnice i sprawdź, które rozwiązanie lepiej odpowiada Twoim potrzebom.

W nieustannej walce o bezpieczeństwo danych różnica między szyfrowaniem sprzętowym a programowym sprowadza się do tego, gdzie działają mechanizmy zabezpieczeń i w jakim stopniu są one narażone na zagrożenia w rzeczywistych warunkach użytkowania. W przypadku pamięci USB i dysków SSD sposób działania szyfrowania wpływa zarówno na poziom ochrony danych, jak i stopień zależności od systemu, z którym współpracuje nośnik.

SPRZĘTOWE	VS.	PROGRAMOWE
Zarządzanie kluczami szyfrowania Klucze szyfrowania sa generowane przez mechanizmy sprzetowe i bezpiecznie przechowywane na nosniku.		**Zarządzanie kluczami szyfrowania** Hasło uzytkownika jest wykorzystywane bezposrednio jako klucz szyfrowania, a same klucze moga byc przechowywane w pamieci systemowej.
Ochrona przed atakami brute force Zaprojektowane z mysla o ochronie przed atakami brute force poprzez ograniczenie liczby prób uwierzytelnienia. Po przekroczeniu okreslonego limitu nosnik usuwa zapisane dane, uniemozliwiajac dostep do poufnych informacji w przypadku zgubienia lub kradziezy urzadzenia.		**Ochrona przed atakami brute force** Podatne na ataki brute force. Komputer próbuje ograniczac liczbe prób odszyfrowania danych, jednak hakerzy moga uzyskac dostep do pamieci komputera i zresetowac licznik prób.
Wymagania dotyczące oprogramowania lub sterowników Nie wymaga instalacji sterowników ani oprogramowania w systemie hosta.		**Wymagania dotyczące oprogramowania lub sterowników** Wymaga instalacji oprogramowania, a zgodność ze sterownikami i systemami operacyjnymi może być zróżnicowana.
Zasoby wykorzystywane do szyfrowania Wykorzystuje dedykowany procesor kryptograficzny wbudowany w nośnik danych.		**Zasoby wykorzystywane do szyfrowania** Wykorzystuje procesor i zasoby systemowe komputera do szyfrowania i odszyfrowywania danych.
Zależność od systemu hosta / podatność Mechanizmy zabezpieczeń są odizolowane wewnątrz urządzenia i pozostają skuteczne nawet po podłączeniu do nieznanego lub zainfekowanego komputera.		**Zależność od systemu hosta / podatność** Bezpieczeństwo zależy od systemu operacyjnego hosta i jest bardziej narażone na zagrożenia, jeśli komputer został zainfekowany złośliwym oprogramowaniem.
Stan szyfrowania Szyfrowanie jest zawsze włączone i nie można go wyłączyć ani obejść.		**Stan szyfrowania** Szyfrowanie można włączyć, wyłączyć lub nieprawidłowo skonfigurować.
Wpływ na wydajność Minimalny wpływ na wydajność, ponieważ szyfrowanie jest realizowane przez dedykowany procesor kryptograficzny.		**Wpływ na wydajność** Może obniżać wydajność, ponieważ szyfrowanie wykorzystuje zasoby procesora.
Elastyczność Szyfrowanie jest przypisane do konkretnego nośnika (pamięci USB lub dysku SSD).		**Elastyczność** Może być stosowane na niemal dowolnym nośniku danych.

Szyfrowanie programowe zapewnia większą elastyczność, natomiast szyfrowanie sprzętowe pozwala lepiej odizolować mechanizmy zabezpieczeń i ograniczyć narażenie na zagrożenia związane z systemem. Zrozumienie sposobu ochrony danych i kontroli dostępu w obu rozwiązaniach ułatwia wybór poziomu zabezpieczeń odpowiedniego do procesów pracy i profilu ryzyka.

www.kingston.com/ironkey