Wpisz szukaną frazę...

Windows

Jak zmienić metodę szyfrowania dysku BitLocker i siłę szyfrowania w systemie Windows 11

@ Kabson 2024-05-18 0 64

Przeczytasz w 3 min.

W tym wpisie wyjaśnię Wam w jaki sposób zmienić siłę szyfrowania i jego algorytm w systemowym narzędziu BitLocker.

Spis treści

Czym jest Bitlocker ?

BitLocker to narzędzie do szyfrowania dysków dostępne w systemach Windows, które zapewnia ochronę danych poprzez szyfrowanie całych dysków. Umożliwia zabezpieczenie danych przechowywanych na komputerze, zarówno na dyskach wewnętrznych, jak i zewnętrznych, przed nieautoryzowanym dostępem. BitLocker można włączyć dla dysków systemowych (tych, na których zainstalowany jest system operacyjny), jak i dysków stałych oraz wymiennych, takich jak dyski USB. Dzięki BitLocker dane są chronione nawet w przypadku kradzieży lub zgubienia urządzenia.

Czy Bitlocker da się złamać ?

Jak wiadomo nie ma dobrych zabezpieczeń
Chociaż BitLocker je
bezpiecznych narzędzi do szyfrowania dysków, ale

żadna technologia nie jest całkowicie odporna na złamanie.

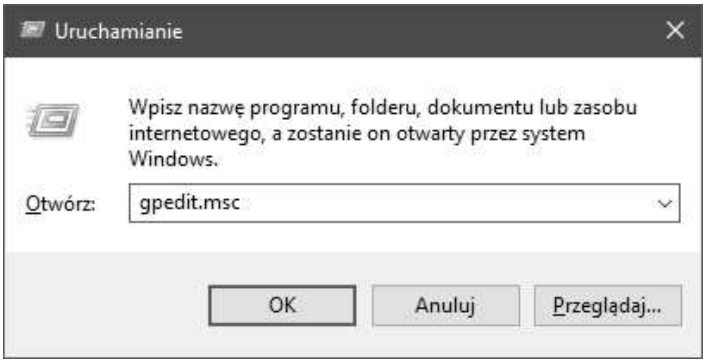
BitLocker można w teorii złamać nawet prostym atakiem typu "*brute force*", czyli próbą odgadnięcia hasła poprzez sprawdzanie wszystkich możliwych kombinacji. Jednak jeżeli hasło jest mocne (długie i skomplikowane), taka metoda jest praktycznie niemożliwa do skutecznego przeprowadzenia w rozsądnym czasie.

Istnieją również inne metody "obejścia" tego szyfrowania, jednak w domowych warunkach... praktycznie nikt nie znając naszego hasła nie jest w stanie dobrać się do naszych zaszyfrowanych danych.

Zmieniamy metodę szyfrowania funkcji Bitlocker.

Jeżeli czujemy się niepewni co do aktualnego poziomu zabezpieczeń, możemy zmienić siłę (i algorytm), z jakim BitLocker szyfruje nasze dane. Oto kroki, które należy wykonać, aby dostosować ustawienia szyfrowania w systemie Windows 11.

Uruchamiamy Edytor lokalnych zasad grupy. Najszybciej uruchomimy go wpisując w polecenie uruchamianie `gpedit.msc`.

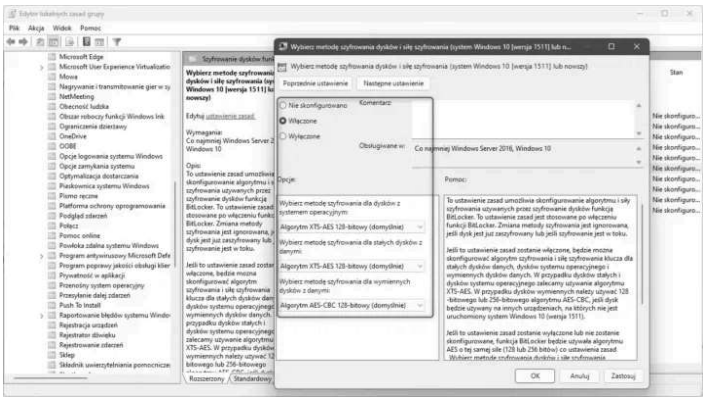


Następnie przechodzimy pod:

```
Konfiguracja kom
tracyjne > Składniki systemu Windows > Sz
```

```
yfrowanie dysków funkcją BitLocker > Wybi
erz metodę szyfrowania dysków i siłę szyf
rowania (system Windows 10 wersja [1511]
i nowszy)
```

i wybieramy nową metodę szyfrowania dysków twardych:



Algorytmy wykorzywane przez BitLocker

Metody szyfrowania wykorzystywane przez BitLocker są dwie, w każdej z nich mamy do wybory klucz 128, badż bezpieczniejszy 256 bitowy.

XTS-AES

XTS-AES (XEX-based Tweaked CodeBook mode with CipherText Stealing) to nowoczesny tryb szyfrowania blokowego, zaprojektowany specjalnie z myślą o szyfrowaniu dysków.

- **XTS-AES 128-bitowy**:
  - **Zalety**:
    - Zapewnia ochronę przed atakami manipulacyjnymi (np. modyfikacją poszczególnych bloków danych).
    - Oferuje wysoką wydajność przy zachowaniu solidnego poziomu bezpieczeństwa.
  - **Wady**:
    - 128-bi
      na at

do 256-bitowego klucza.

- **XTS-AES 256-bitowy**:
  - **Zalety**:
    - Najwyższy poziom bezpieczeństwa dzięki długiemu kluczowi 256-bitowemu.
    - Zapewnia ochronę przed atakami manipulacyjnymi.
    - Wysoka odporność na wszelkiego rodzaju ataki brute force.
  - **Wady**:
    - Może wpływać na wydajność systemu z powodu większego obciążenia obliczeniowego.

AES-CBC

AES-CBC (Cipher Block Chaining) to starszy, ale wciąż powszechnie używany tryb szyfrowania blokowego.

- **AES-CBC 128-bitowy**:
  - **Zalety**:
    - Dobre połączenie wydajności i bezpieczeństwa.
    - Mniej zasobożerne w porównaniu do 256-bitowego klucza.
  - **Wady**:
    - Mniej bezpieczny niż wersja z 256-bitowym kluczem, ale wciąż uważany za bardzo bezpieczny.
- **AES-CBC 256-bitowy**:
  - **Zalety**:
    - Bardzo silne szyfrowanie dzięki długiemu kluczowi 256-bitowemu.
    - Używany w wielu różnych aplikacjach i standardach bezpieczeństwa.
  - **Wady**:
    - CBC j
      atak

flipping attacks), choć te są trudn do przeprowadzenia w praktyce.
- Wolniejsze szyfrowanie i deszyfrowanie w porównaniu do trybu XTS.

Podsumowanie.

- **XTS-AES 128-bitowy**: Dobry kompromis między wydajnością a bezpieczeństwem, odpowiedni dla większości użytkowników.
- **XTS-AES 256-bitowy**: Najlepsze zabezpieczenie, rekomendowane dla najbardziej krytycznych danych.
- **AES-CBC 128-bitowy**: Wydajny i bezpieczny, ale mniej bezpieczny niż 256-bitowa wersja.
- **AES-CBC 256-bitowy**: Bardzo silne szyfrowanie, ale wolniejsze i mniej odporne na ataki manipulacyjne niż XTS.

Wybór odpowiedniej metody szyfrowania powinien zależeć od specyficznych potrzeb użytkownika oraz mocy obliczeniowej sprzętu. Dla większości zastosowań XTS-AES 128-bitowy lub 256-bitowy będzie najlepszym wyborem ze względu na optymalne połączenie bezpieczeństwa i wydajności.

Oczywiście wykorzystanie BitLocker nie jest jedyną metodą na szybkie szyfrowanie dysków w naszym systemie. Możecie również skorzystać np. z aplikacji VeraCrypt, o której już kiedyś na tym blogu wspominałem.

Dziękuję za uwagę.

BITLOCKER GPEDIT.MSC VERACRYPT WINDOWS

Kabson

MOŻE CIĘ ZAINTERESOWAĆ:

Jak usunąć wirusy z Windows za pomocą Linux'a

Dezaktywujemy przeglądarkę Edge w systemie Windows 10

Tworzymy bezpieczny folder w systemie Windows

Tworzymy kopię zapasową partycji za pomocą Rescuezilla

Masowa konwersja RAR oraz 7Zip do zip

Automatycznie przełączamy jasny/ciemny styl aplikacji w zależności od pory dnia

ZOSTAW KOMENTARZ

Twój komentarz

Imię (nick)*

Email*

Strona WWW

Zapisz moją nazwe
przeglądarce.

☐ ZASUBSKRYBUJ NASZ BLOG, ABY BYĆ NA BIEŻĄ
INFORMOWANYM O NOWYCH WPISACH.

Powodzenie!

CLOUDFLARE
Prywatność • Warunki

WYŚLIJ

POLUB NAS NA FACEBOOK'U:

Variatkowo.pl
376 followers

WESPRZYJ NAS !

OSTATNIO KOMENTOWANO:

Maria - **Jak dodać narzędzie Gpedit.msc do Windows 10 Home**

oprogramowanie.pro - **Jak dodać nowe rdzenie w Retroarch ?**

Kabson - **Emulujemy gry z XBOX 360 na PC (Xenia)**

MichalXD - **Emulujemy gry z XBOX 360 na PC (Xenia)**

Jacek W - **Moje 15 porad do trybu "przetrwania" w Fallout 4**