

Jetico BestCrypt

Zaszyfrujmy świat

Każdy z nas odczuwa naturalną potrzebę zaszyfrowania pewnych danych tak, aby były one dostępne tylko wtedy, kiedy my z nich skorzystamy.

PAWEŁ LESZEK

Jetico BestCrypt [1] to program do szyfrowania systemu plików. Umożliwia on tworzenie, montowanie i zarządzanie szyfrowanymi „kontenerami” (szyfrowanymi woluminami), które zachowują się jak każdy inny dysk po zamontowaniu. Jednak po odmontowaniu ich zawartość binarna jest zaszyfrowana. Dzięki temu dane są chronione – tak że nawet w przypadku kradzieży pliku-kontenera będzie on bezużyteczny dla włamywaczy (pod warunkiem, że nie znają oni hasła chroniącego zawartość).

Kontenery BestCrypt są zwykłymi plikami, które można np. przechowywać na płytach CD-ROM czy innych nośnikach. Można je również umieszczać na udziałach dyskowych. Wersja BestCrypt dla Windows ma dodatkowo możliwość szyfrowania pliku pamięci wirtualnej.

Ze stron WWW producenta można ściągnąć wersję testową BestCrypt – zarówno dla Linuksa jak i Windows. Pakiet instalacyjny jest dystrybuowany w postaci kodu źródłowego. Kompilacja jest łatwa i dobrze opisana – najkrócej rzecz ujmując, należy mieć wcześniej zainstalowany i skonfigurowany kod źródłowy jądra. Komponenty obsługujące poszczególne algorytmy szyfrujące są zaimplementowane jako tradycyjne moduły jądra systemu. Jest to uciążliwe dla początkujących użytkowników, którzy nie zamierzają kompilować jądra. Nie należy również zapomnieć o ściągnięciu pakietu z dokumentacją do programu (jest dostępna w postaci spakowanych plików HTML).

Używamy BestCrypt

Głównym programem narzędziowym BestCrypt jest *bctool*.

Stworzenie kontenera BestCrypt container jest banalne, oto przykład utworzenia kontenera o nazwie *test*:

```
bctool new test -s 150M -a twofish
-d „moj testowy kontener”
Enter password:
Verify password:
```

Do stworzenia kontenera użyliśmy, jak widać, narzędzia *bctool* z opcją „new”, po której podajemy nazwę pliku kontenera, jego rozmiar, algorytm szyfrujący oraz opis woluminu. Przy tworzeniu kontenera BestCrypt poprosi o zdefiniowanie hasła dostępu do kontenera. Warto używać jak najdłuższych haseł, ponieważ utrudni to ewentualnym włamywaczom złamanie hasła metodą „prób i błędów”.

Trzeba pamiętać, że mimo, iż wszystkie z obsługiwanych przez BestCrypt algorytmów (AES, RC6, Twofish, Blowfish, 3DES, IDEA, CAST GOST), za wyjątkiem pojedynczego DES, używają kluczy o długości 128 bitów, klucz kontenera jest kodowany przy użyciu hasła użytkownika. Proste do odgadnięcia hasło sprawi, że zawartość kontenera będzie łatwo dostępna, bez względu na to, jak silny algorytm został wykorzystany.

Trzeba również pamiętać, że zapomnianego hasła nie można w żaden sposób odzyskać, zatem warto je dobrze zapamiętać, w najgorszym wypadku przechowywać w bezpieczny sposób. Utrata hasła jest równoważna utracie dostępu do danych przechowywanych w kontenerze.

Po stworzeniu kontenera musimy w nim jeszcze utworzyć jakiś system plików, można w tym celu posłużyć się poleceniem:

```
bctool format -t msdos./test
```

Przełącznik *-t* określa, jaki system plików ma wykorzystywać kontener. Po utworzeniu i sformatowaniu kontenera BestCrypt, można go zamontować poleceniem:

```
bctool mount -t ↵
```

```
vfat./test./mnt/szyfrowane
```

Od momentu zamontowania zawartość kontenera jest dostępna tak jak każdy inny dysk. Domyślnie właścicielem plików jest użytkownik, który go zamontował (maska 0700, czyli *drwx*). Zatem użytkownicy inni niż root nie mają dostępu do plików przechowywanych w kontenerze, chyba że uprawnienia zostaną ręcznie zmienione. Nie jest to problemem, ponieważ montując kontener można przy użyciu opcji *-o*, *-g* oraz *-m* odpowiednio ustawić prawa użytkownika i grupy. Po zakończeniu pracy odmontowujemy kontener poleceniem:

```
bctool umount./mnt/test
```

Od tej chwili kontener jest zwykłym plikiem, który można swobodnie przenosić i archiwizować. Dodatkowo można dokupić (niestety osobną) aplikację BCWipe, która usuwa fizycznie dane z dysku, przez nadpisanie ich przypadkowymi danymi.

Wrażenia

Moje osobiste wrażenia z pracy z BestCrypt są pozytywne. Od razu widać, że nie jest to kolejna aplikacja przeniesiona „na siłę” do Linuksa, ale jest napisana w sposób zgodny z tym, czego oczekuje zaawansowany użytkownik. Przede wszystkim można z nim wygodnie pracować z wiersza poleceń, narzędzie *bctool* można bez problemu wywoływać z poziomu skryptów.

Jest to w dodatku oprogramowanie Open Source – jego kod źródłowy jest swobodnie dostępny. Również w ogólnej opinii BestCrypt uchodzi za wysokiej klasy oprogramowanie – stabilne, oferujące wiele algorytmów szyfrowania. Co więcej – jeśli nadal używasz z jakichś powodów MS Windows – również dla tego systemu jest dostępny BestCrypt. Licencja BestCrypt na jedno stanowisko kosztuje około 90 dolarów. ■

INFO

[1] BestCrypt: <http://www.jetico.com>