Zabezpieczenie danych na Pendrive

Jedną z korzyści wprowadzenia nowej ustawy o ochronie danych osobowych (RODO) jest rosnąca świadomość użytkowników, jak ważne mogą być dane przechowywane na komputerach i jak ważne jest ich odpowiednie zabezpieczenie.

Oprócz zabezpieczenia komputerów stacjonarnych oraz laptopów ważne jest, aby mieć świadomość, że kolejnym słabym ogniwem w bezpieczeństwie danych mogą być dyski przenośne i pendrivy. Pendrivy często są wykorzystywane do przechowywania kopii plików, które wykorzystujemy w bieżącej pracy, często też się zdaża, że zawierają one dane osobowe, które powinny być chronione.

Poniżej przedstawiam trzy sposoby na ochronnę danych, zwracając uwagę na wady i zalety każdego z rozwiązań.

1 sposób – ochrona sprzętowa

Najprostszym sposobem jest zakup urządzeń, które mają wbudowane odpowiednie zabezpieczenia. Przykładem takiego pendrive może być urządzenie Kingston DataTraveler Vault Privacy 8GB USB 3.0 256bit AES Encrypted.

Jest to pendrive, który posiada wbudowane mechanizmy szyfrujące blokujące dostęp do zawartości hasłem.

zalety

- sprzętowe rozwiązanie wbudowane w urządzenie
- możliwość pracy w trybie do odczytu
- możliwość dokupienia ochrony antywirusowej
- brak konieczności stosowania dodatkowego oprogramowania
- automatyczne blokowanie i formatowanie po wpisaniu 10 razy błędnego hasła

wady

- wysoka cena w stosunku do pojemności

2 sposób – Bitlocker

Ten sposób jest równie prosty co pierwszy, niestety jego zastosowanie jest ograniczone. Funkcja Bitlocker została wbudowana przez firmę Microsoft w system operacyjny Windows od wersji 7 do 10, również w rozwiązaniach serwerowych. Funkcja ta pozwala na zaszyforwanie dysków komputera, dysków przenośnych oraz pendrive.

Niestety, największą wadą tego rozwiązania jest ograniczenie funkcjonalności do wersji Windows Pro oraz Enterprise, oznacza to, że użytkownicy posiadający system w wersji Windows Home nie mogą szyfrować ai odczytywać dysków zabezpieczonych funkcją Bitlocker.

zalety

- łatwa do uruchomienia
- zabezpieczenie danych hasłem
- zabezpiecza całe urządzenie lub dysk

wady

- nie występuje w wersji Home systemu Windows

3 sposób – VeraCrypt

VeraCrypt jest następcą programu TrueCrypt, który był bardzo dobrym i bezpiecznym rozwiązaniem dla użytkowników wielu systemów operacyjnych, nie tylko Microsoft Windows ale również Linux. VeraCrypt jest rozwiązaniem nadal rozwijanym i stanowi darmową alternatywę zapewniającą wysoki poziom bezpieczeństwa danych.

Jego dużą zaletą jest możliwość zaszyfrowania całego dysku ale również utworzenia tzw. kontenera o dowolnej pojemności zabezpieczonego hasłem. Kontener taki po zamontowaniu widoczny jest w systemie jako dodatkowy dysk, a po odmonotowaniu zachowuje się jak zwykły plik, który można kopiować i archiwizować.

Należy pamiętać, że aby używać dysków zabezpieczonych przy pomocy programu VeraCrypt, konieczne jest jego zainstalowanie na każdym komputerze, na którym ma być montowany dysk lub pendrive.

zalety

- dowolny tryb szyfrowania
- możliwość zaszyforwania całego pendriva lub utworzenia kontenera
- darmowy

wady

- wymaga dodatkowego oprogramowania

Zagrożenia związane z niepowołanym dostępem do danych zgromadzonych na pamięciach USB oraz niebezpieczeństwa czyhające na nieostrożnych użytkowników przypadkowych pendrive'ów pozostają od lat niezmienne. Do dyspozycji mamy jednak wiele mniej lub bardziej udanych rozwiązań ochronnych — oto kilka ciekawostek z tej dziedziny.

Niedawno ogromną popularnością cieszył się USB killer v2.0, czyli urządzenie zdolne do fizycznego niszczenia komputerów po jego podłączeniu do interfejsu USB. Dziś przedstawimy dwa ciekawe rozwiązania, z których jedno mogłoby uchronić nas nie tylko przed „zabójcą" komputerów, ale również przed dowolną infekcją pochodzącą z pamięci USB.

Fizyczna ochrona USB

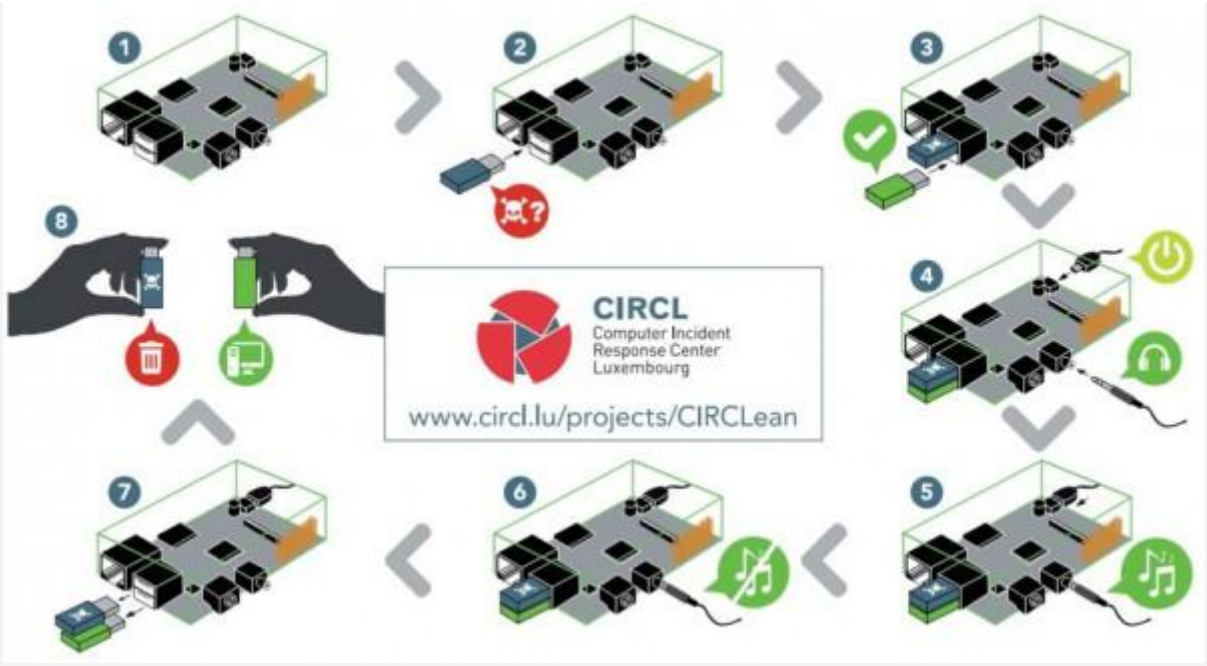
3 Digits Combination USB Flash Drive Security Lock to, jak wskazuje sama nazwa, fizyczne zabezpieczenie przeznaczone do ochrony nośników USB przed niepowołanym użyciem.

USB Security Lock (źródło: usb.brando.com)

Urządzenie jest wyposażone w zamek szyfrowy (kombinacja 3 cyfr) i pozwala na fizyczne zablokowanie możliwości podłączenia napędu do jakiegokolwiek urządzenia. W taki sposób możemy ochronić nasze urządzenie USB przed ingerencją (odczytem lub modyfikacją jakichkolwiek danych) za strony przypadkowego intruza.

Sanityzacja nośników przed użyciem

Nieco inne zastosowanie ma natomiast CIRCLean. Ten projekt opracowany przez Computer Incident Response Center Luxembourg pozwala na szybkie i wygodne dotarcie do treści zawartych na dowolnym nośniku USB bez narażania się na typowe zagrożenia z tym związane. CIRCLean może nas nawet ochronić przed słynnym USB killerem — spójrzmy więc jak to działa.



CIRCLean — zasada działania

W skrócie CIRCLean to oprogramowanie, które pozwala na przekształcenie platformy RaspberryPi w stację unieszkodliwiającą wszystkie potencjalne zagrożenia znajdujące się na niezaufanym urządzeniu USB.
Sanityzacja odbywa się przez podłączenie nieznanego urządzenia do jednego z portów USB i przeniesienie jego zawartości w bezpieczny sposób na inny nośnik USB. Potencjalnie niebezpieczne dokumenty, takie jak PDF, są w trakcie całego procesu konwertowane na inne bezpieczniejsze formaty tak, by można było dotrzeć do pierwotnych treści bez konieczności podłączania potencjalnie niebezpiecznego/zainfekowanego urządzenia.

Biorąc pod uwagę to, że nawet najlepsze oprogramowanie antywirusowe nie da nam pełnej ochrony w trakcie korzystania z danych i dokumentów nieznanego pochodzenia, taki pomysł może być rzeczywiście bardzo skuteczny i może nas nawet uchronić przed atakami 0-day.
Ocenę praktycznej przydatności tego typu rozwiązań pozostawiam czytelnikom — zachęcam również do dzielenia się własnymi przemyśleniami na temat bezpieczeństwa pamięci USB, które od lat stanowi niezmiennie poważne wyzwanie.

Przykład niedawnego naruszenia bezpieczeństwa danych przenoszonych na nieszyfrowanej pamięci USB

Pochodzący z 30. października 2017 r. przykład dotyczy portu lotniczego Heathrow w Londynie, gdzie do przechowywania danych poza chmurą wykorzystuje się nieszyfrowane pamięci USB. Niestety, dane nie były standardowo przechowywane na szyfrowanych pamięciach USB. Niewdrożenie odpowiednich standardów bezpieczeństwa danych i zabezpieczeń przed utratą danych z wykorzystaniem szyfrowanych pamięci USB doprowadziło do groźnego dla UE poważnego naruszenia bezpieczeństwa poufnych i zastrzeżonych informacji.

Londyn – nieszyfrowana pamięć USB doprowadziła do wycieku poufnych lub zastrzeżonych plików:

- Pamięć zawierała 76 folderów / 174 dokumenty
- Informacje o środkach ochrony Królowej
- Pliki wskazywały rodzaje dokumentów tożsamości niezbędnych do wchodzenia do stref zastrzeżonych
- Harmonogram patroli ochrony
- Mapy rozmieszczenia kamer przemysłowych
- Jeden dokument mówił o niedawnych atakach terrorystycznych i omawiał typ zagrożenia dla lotniska

Podobne do tego przypadki utraty pamięci USB mają miejsce dużo częściej, niż się przypuszcza i stanowią najlepszy przykład powodów, dla których wdrożenie standardu / polityki użytkowania szyfrowanych pamięci USB przez pracowników każdej organizacji powinno mieć najwyższy i najpilniejszy priorytet. Więcej informacji

Wystarczy skorzystać z oferty szyfrowanych pamięci USB firmy Kingston, wśród których znaleźć można cieszące się doskonałą renomą pamięci linii IronKey, które zapewniają zgodność ze wszystkimi wymaganiami biznesowymi i rządowymi. Więcej informacji

Na co zwracać uwagę?

Istnieje jeden niezmienny czynnik w postaci elementu ludzkiego / zagrożenia od wewnątrz, który objawia się poluzowaniem standardów, polityk oraz brakiem rozliczalności i odpowiedzialności. Dane, informacje identyfikowalne osobowo oraz poufne są nadal kluczowymi elementami, które wymagają najbardziej ścisłej ochrony.

Przechowywanie danych poza chmurą na szyfrowanych pamięciach USB to konieczność!

Analiza ostatnich naruszeń bezpieczeństwa danych, ich wycieków i przejęć wskazuje jednoznacznie, że większości z tych incydentów można było zapobiec. Przyczynami większości z tych incydentów były proste przeoczenia, od nieuwagi, niewłaściwie określonych priorytetów po niewdrożenie odpowiednich standardów, polityk i procedur.

Obszar ten obejmuje bezpieczeństwo, ochronę i zabezpieczenie informacji o obywatelach / pracownikach, od danych osobowych po informacje zdrowotne i finansowe. Ponadto konieczne jest również zapewnienie ochrony poufnych informacji firmy, dotyczących bezpieczeństwa narodowego, strategii obrony kraju i danych wywiadowczych.

Czy warto trafić na nagłówki gazet?

Przepisy od 2018 roku: bez zachowania zgodności zagrożenie ogromnymi grzywnami i pozwami

Zarówno **Ogólne Rozporządzenie o Ochronie Danych Osobowych w UE (EU GDPR)** i amerykańskie przepisy **NYDFS - 23 NYCRR 500** zalecają szyfrowanie danych:

- Standardy bezpieczeństwa przetwarzania danych
  - Organizacje szyfrują dane wrażliwe – w trakcie tranzytu i przechowywania.
- EU GDPR: Szyfrowanie danych osobowych (Artykuł 32, Bezpieczeństwo przetwarzania)
  - **Więcej informacji**
- NYDFS: Szyfrowanie danych wrażliwych – w trakcie tranzytu i przechowywania. (Sekcja 500.15, Szyfrowanie danych niepublicznych)
  - **Więcej informacji**

3 najważniejsze sprawy

Przechowywanie danych w chmurze / poza chmurą

Jak wiadomo, rozwiązania chmurowe są świetne, ale czy w każdym przypadku?

- Nieprzerwany dostęp – ale czy Internet jest dostępny zawsze i wszędzie?
- Niezawodny / bezpieczny dostęp – ale czy można ufać bezpłatnym sieciom Wi-Fi?
  - Patrz artykuł Krack - Wi-Fi WPA2 security cracked
- Następny atak cybernetyczny – czy będzie to złośliwe oprogramowanie, a może wymuszające okup?

Dzięki szyfrowanym pamięciom USB (przy połączeniu z siecią Wi-Fi lub bez) mamy pewność, że dane są chronione, dostępne, a utrata pamięci nie jest równoznaczna z udostępnieniem danych osobom postronnym.

Uzupełnienie istniejących zabezpieczeń punktów końcowych na poziomie urządzeń dzięki rozwiązaniom zapobiegającym utracie danych (Data Loss Prevention – DLP).

Szyfrowane pamięci USB marki Kingston / IronKey są doskonałym rozwiązaniem, pozwalającym uniknąć blokowania wszystkich portów USB. Nikomu chyba nie zależy na celowym obniżeniu efektywności lub produktywności pracowników mobilnych.

Zabezpieczenie punktów końcowych udostępnia wiele korzyści w odniesieniu do polityk zarządzania użytkownikami i grupami użytkowników.

- Określenie, kto może mieć dostęp do portów USB
- Wydanie firmowych szyfrowanych pamięci USB firmy Kingston
- Dopuszczenie tylko konkretnego modelu pamięci USB – działa tylko 1 model szyfrowanych pamięci USB
- Zablokowanie dostępu innych podłączanych urządzeń – działają tylko firmowe szyfrowane pamięci USB
- Dopuszczanie lub ograniczanie możliwości zapisywania plików na szyfrowanych pamięciach USB
- Kontrola kopiowanych plików oraz godzin użycia pamięci po raz ostatni

Zarządzanie zagrożeniami i redukcja ryzyka

Rodzina szyfrowanych pamięci USB firmy Kingston, obejmująca renomowane rozwiązania IronKey, zapewnia wielopoziomowe bezpieczeństwo, ochronę danych oraz funkcje zarządzania ryzykiem.

- Ochrona danych przechowywanych na szyfrowanych pamięciach USB w pełni zgodna z przepisami
- 256-bitowe szyfrowanie sprzętowe AES w trybie XTS
- Zgodność za standardem FIPS 197 lub FIPS 140-2 Level 3

Dostępne rozwiązania zarządzane

Błyskawiczna kontrola nad wszystkimi szyfrowanymi pamięciami USB, od poziomu globalnego po pojedyncze urządzenia

- Safeconsole - DTVP 3.0 i DT4000G2 Managed
- IronKey EMS - IronKey D300 Managed i IronKey S1000 Enterprise

Więcej informacji

Infografika dotycząca unijnego ogólnego rozporządzenia o ochronie danych oraz wymogu szyfrowania danych

- https://www.kingston.com/pl/community/articledetail/articleid/45589

Szyfrowane pamięci flash USB

DataTraveler Locker+ G3

DataTraveler 2000

DataTraveler Vault Privacy 3.0

DataTraveler 4000G2DM

IronKey

IronKey D300/IronKey D300 Managed

Ironkey S1000/Ironkey S1000 Enterprise