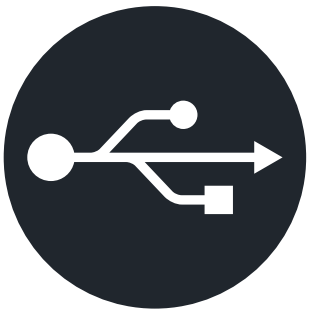
Jak umożliwić korzystanie z pamięci USB

bez narażania bezpieczeństwa punktów końcowych

#KingstonIsWithYou #KingstonIronkey

Wprowadzenie

W momencie swojej premiery w styczniu 1996 r. oficjalna specyfikacja USB 1.0 zwiastowała nową erę uniformizacji, wygody i wszechstronności zarówno dla producentów urządzeń peryferyjnych, jak i użytkowników końcowych. 27 lat później zachowuje wsteczną zgodność ze wszystkimi poprzednimi wersjami, a USB pozostaje kamieniem węgielnym w kategorii interfejsu sprzętu komputerowego – poczynając od serwerów, a kończąc na smartfonach.



Prostota rozwiązania typu plug-and-play i stale rosnąca szybkość sprawiły, że jednymi z największych „zwycięzców" stały się przenośne pamięci USB. Jednak tego typu wygoda wiąże się z pewnym kompromisem, jeśli chodzi o bezpieczeństwo danych. W dzisiejszym świecie bez zastosowania odpowiednich rozwiązań, takich jak ochrona punktów końcowych w komputerach-hostach czy odpowiednie praktyki w dziedzinie bezpieczeństwa danych, użytkownicy nieostrożnie korzystający z przenośnych urządzeń pamięci USB narażają siebie i innych na potencjalne naruszenie bezpieczeństwa danych. Może to być kosztowne dla użytkownika, a nawet zagrozić całej organizacji lub instytucji rządowej.

Oprócz zapewnienia ochrony środowiska hosta należy także zadbać, aby pamięć USB była zabezpieczona hasłem oraz przez funkcję szyfrowania sprzętowego w samym urządzeniu. Zapewnia to najlepszą ochronę przed naruszeniem bezpieczeństwa. Omówimy kilka najlepszych metod pozwalających bezpieczniej korzystać z pamięci USB, a także dokładniej przyjrzymy się urządzeniom pamięci USB jako takim.

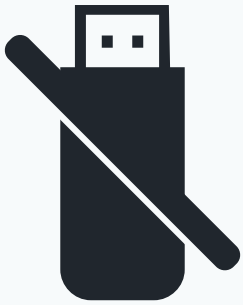
Podczas gdy idealne jest podejście łączone, to ogromne znaczenie ma solidność szyfrowania i komponentów sprzętowych samej pamięci USB. Zapewniają one korzyści w różnych branżach, poczynając od finansów, poprzez opiekę zdrowotną i produkcję, a kończąc na zastosowaniach wojskowych. Odgrywają także rolę w pracy zdalnej, gdy dostęp do sieci jest niemożliwy, podatny na zagrożenia lub niepraktyczny.

Urządzenia pamięci USB z szyfrowaniem sprzętowym są dostępne z różnymi certyfikatami i oferują szereg funkcji bezpieczeństwa. Sprawdzając ich zalety i możliwości personalizacji, warto zauważyć, że ich przydatność jako samodzielnych rozwiązań przejawia się w możliwości ich zastosowania we wszystkich aspektach wrażliwych środowisk.

Zarządzanie portami: pamięć USB w połączeniu z oprogramowaniem chroniącym przed utratą danych w punktach końcowych

Od dziesięcioleci aplikacje antywirusowe i chroniące przed złośliwym oprogramowaniem zapewniają ochronę na najbardziej podstawowym poziomie – poprzez automatyczne skanowanie pobieranych plików i podłączanych urządzeń oraz raportowanie lub podejmowanie działania wobec podejrzanej zawartości. Ochrona, jaką zapewnia oprogramowanie antywirusowe nowej generacji (NGAV), idzie o krok dalej. Zamiast polegać wyłącznie na stale aktualizowanej bazie sygnatur wirusów, NGAV dodaje funkcje uczenia maszynowego i wykrywania behawioralnego, które mogą rozpoznawać nieznane zagrożenia i przeciwdziałać im.

Nie jest to jednak jedyna dostępna broń, a ci, którzy chcieliby zapewnić „kuloodporną" ochronę urządzeniom peryferyjnym użytkownika i nie tylko, mogą wykorzystać oprogramowanie chroniące przed utratą danych w punktach końcowych (DLP), które pozwala na całkowite zablokowanie dostępu do portów USB i innych punktów dostępu.



Podejście polegające na blokowaniu wszystkich portów z pewnością może wyeliminować ryzyko i w niektórych przypadkach może być pożądane, jednak takie postępowanie często okazuje bronią obosieczną, której użycie przynosi niepożądane skutki.

Mimo to niektórzy administratorzy IT wolą odrzucać prośby o otwarcie portów USB w komputerach użytkowników, ponieważ umożliwiłoby to bezpośrednie przejście przez zaporę przedsiębiorstwa. Taka ostrożność jest zrozumiała, ale jeśli chodzi o umożliwienie dostępu do pamięci USB, przyznanie tego uprawnienia nie musi być ogromnym problemem w zakresie bezpieczeństwa, jeśli zostaną spełnione określone warunki.

Zasadniczym wymogiem jest pakiet aplikacji do zarządzania punktami końcowymi, który obejmuje skanowanie w poszukiwaniu zagrożeń w rozwiązaniach antywirusowych i chroniących przed złośliwym oprogramowaniem, a także scentralizowane monitorowanie i zarządzanie wszystkimi punktami końcowymi użytkownika.

Ogólnie rzecz biorąc, to proste podejście pojawia się pod różnymi postaciami w ujednoliconych rozwiązaniach popularnych dostawców, takich jak m.in. McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection czy WinMagic SecureDoc.

Zaawansowane funkcje „białej listy"

Jeśli chodzi o zabezpieczanie urządzeń pamięci USB, metoda zależy od wymaganego poziomu ochrony. Prostym, ale skutecznym podejściem jest umieszczenie na „białej liście" urządzeń pamięci USB poprzez wykorzystanie wartości ich identyfikatorów dostawcy (VID) oraz identyfikatorów produktu (PID). Jedynym wyróżnikiem w przypadku wszystkich urządzeń peryferyjnych USB jest to, że każdy producent ma unikalny identyfikator VID, natomiast PID zmienia się wraz z każdym nowo wprowadzanym produktem.

W przypadku „białej listy" wykorzystanie samego identyfikatora VID producenta nie byłoby skuteczne w zapewnieniu bezpieczeństwa, ponieważ dopuszczałoby wszystkie urządzenia USB, które kiedykolwiek wyprodukowano. Identyfikator PID oferuje większe możliwości i pozwala, aby tylko określony model miał dostęp do systemu hosta.

Chociaż jest to lepsze rozwiązanie, nadal nie jest idealne. Urządzenia pamięci USB cieszą się ogromną popularnością, ponieważ umożliwiają użytkownikom zakup własnych urządzeń spośród dozwolonych modeli. Dlatego firma Kingston Technology oferuje dostosowane do indywidualnych potrzeb rozwiązanie zwiększające bezpieczeństwo urządzeń pamięci USB.

W ramach oferowanego przez nią programu personalizacji możliwe jest stworzenie i zastosowanie dla wielu szyfrowanych urządzeń pamięci flash USB niestandardowych profili PID, specyficznych dla danej organizacji. Firmy wdrażające urządzenia z dostosowanym identyfikatorem produktu nie tylko mogą łatwiej korzystać z funkcji „białej listy", ale także ze znacznie większej ochrony. W przypadku braku pasującego niestandardowego identyfikatora PID nawet pozornie identyczne urządzenia zakupione samodzielnie przez pracowników nie uzyskają dostępu.

Chociaż wykorzystanie niestandardowych identyfikatorów PID umożliwia administratorom IT szybkie i łatwe udostępnianie nowych urządzeń pamięci USB, bardziej zaawansowaną alternatywą jest użycie numerów seryjnych poszczególnych urządzeń, które znajdują się na większości szyfrowanych pamięci USB firmy Kingston. To rozwiązanie wymaga, aby

każdy unikalny numer seryjny urządzenia był zarejestrowany w aplikacji do zarządzania punktami końcowymi. Wymaga to wstępnego przetworzenia danych przez pracowników działu IT, a firma Kingston może dostarczyć listę numerów seryjnych do każdego zamówienia. Mają one zawsze postać alfanumeryczną i nie są sekwencyjne. Wybór tej metody pozwala na stosowanie znacznie bardziej elastycznych zasad opartych na posiadaniu indywidualnego urządzenia pamięci, z dodatkową możliwością precyzyjnego śledzenia pochodzenia urządzeń, co może być nieocenione w „dochodzeniowych" scenariuszach IT. Niektóre pamięci firmy Kingston mają na obudowie numer seryjny i kod kreskowy do skanowania elektronicznego, natomiast inne mogą zostać w nie zaopatrzone na potrzeby zamawiającej firmy. Elementy te można wykorzystać do śledzenia urządzeń pamięci.

Domyślnie systemy zarządzania punktami końcowymi zapewniają dostęp do identyfikatorów VID/PID w celu blokowania portów i umieszczania na „białej liście". Firma Kingston oferuje bardziej wszechstronny sposób wykorzystania tych funkcji, aby umożliwić zastosowanie bardziej przyjaznych i pomysłowych zasad, które ułatwią korzystanie z urządzeń pamięci USB. Wprowadzenie odpowiedniej metody identyfikacji sprawia, że całościowe blokowanie wszystkich portów staje się nie tylko zbyt uproszczonym, ale wręcz zbędnym rozwiązaniem.

Bezpieczne, zgodne z wymogami rozwiązania dla użytkowników zdalnych

Jeśli chodzi o bezpieczeństwo, urządzenia z „białej listy" rozwiązują tylko połowę problemu lub, innymi słowy, stanowią tylko połowę rozwiązania.

Wygoda i prostota urządzeń pamięci USB sprawia, że są one niezbędne w wielu firmach i instytucjach, w których przenośność jest kluczem do bezproblemowego transferu danych. W większości środowisk, ze względu na konieczność zapewnienia zgodności i „higieny" środowiska IT, niezbędne jest wyposażenie pracowników w szyfrowane urządzenia pamięci USB do takich zadań. Dzięki jednoczesnemu zastosowaniu szyfrowania i ochrony hasłem, przenośna pamięć jest wyposażona w zabezpieczenia uniemożliwiające dostęp do poufnych danych w przypadku zgubienia, kradzieży lub pozostawienia urządzenia w potencjalnie podatnej na zagrożenia sytuacji.

Nie jest to uniwersalne rozwiązanie, ponieważ techniki szyfrowania są różne, a najważniejsze różnice wychodzą na światło dzienne przy porównaniu rozwiązań oprogramowania i szyfrowania sprzętowego. Co jest zatem lepsze? To zależy od potrzeb użytkownika, ale bardziej zasadne wydaje się pytanie: „Co jest bezpieczniejsze?".

Szyfrowanie programowe to zasadniczo rozwiązanie budżetowe, które może być zadowalające w niektórych sektorach przy działalności na mniejszą skalę. Może być ono również odpowiednie dla firm, w których transfery danych nie są uważane za wrażliwe i których obawy dotyczą bardziej zgodności z wewnętrznymi wymogami.

Jednak modus operandi szyfrowania programowego jest również jego piętą achillesową, ponieważ wymaga aplikacji klienckich, które potrzebują komputera do wykonywania zadań szyfrowania. W związku z tym urządzenie magazynujące szyfrowane programowo jest bezpieczne tylko w takim stopniu, w jakim bezpieczny jest obsługujący je komputer.

Większa jest również podatność na wykorzystanie, ponieważ hakerzy mający dostęp do pamięci komputera mogą odczytać klucze szyfrowania/deszyfrowania. Również dane zapisane w pamięci mogą być narażone na brutalny atak, ponieważ ochrona dostępu hasłem nie jest potrzebna, jeśli można uzyskać dostęp do zaszyfrowanych plików i je skopiować.

Warto także pamiętać, że szyfrowanie programowe może czasem wymagać aktualizacji oprogramowania, co może komplikować wdrożenie, powodując dodatkowe obciążenie dla pracowników działu IT. Co najgorsze, szyfrowanie programowe może zostać całkowicie wyłączone przez sfrustrowanych pracowników, którzy mają problemy z korzystaniem z pamięci na różnych platformach. Użytkownik może skopiować dane z szyfrowanej pamięci do komputera, sformatować ją jako pamięć nieszyfrowaną, a następnie ponownie skopiować dane do pamięci. W takim przypadku dane będą niezabezpieczone i narażone na naruszenie. Biorąc pod uwagę wymóg zgodności z przepisami i regulacjami dotyczącymi poufności danych, jest to niedopuszczalne, ponieważ zabezpieczenie pamięci USB można skutecznie wyłączyć.

Szyfrowanie na chipie: odporne i szybkie rozwiązanie

Natomiast szyfrowana sprzętowo pamięć USB działa niezależnie od komputera, ponieważ zawiera dedykowany procesor wbudowany w samo urządzenie pamięci, który zarządza szyfrowaniem. Dzięki temu ma stale włączony proces szyfrowania z ochroną przed siłowymi atakami z wykorzystaniem hasła. Zaszyfrowane dane nie są dostępne i nie można ich skopiować.

Szyfrowane sprzętowo pamięci USB firmy Kingston klasy korporacyjnej i wojskowej wykorzystują 256-bitowe szyfrowanie AES w trybie XTS. Uznana na całym świecie 256-bitowa technika szyfrowania AES zapewnia bardzo skuteczne zabezpieczenie danych. Wykorzystując dwa oddzielne klucze na różnych etapach procesu szyfrowania/deszyfrowania, tryb XTS zapewnia podobny efekt jak dwukrotne szyfrowanie danych.

W praktyce klucz szyfrujący pochodzi z generatora liczb losowych kontrolera pamięci, który jest odblokowywany przez hasło użytkownika. Ponieważ uwierzytelnianie odbywa się w sprzętowej warstwie kryptograficznej urządzenia, klucze szyfrujące i inne krytyczne funkcje bezpieczeństwa są chronione przed typowymi zagrożeniami, takimi jak luka BadUSB, ataki oparte na twardym resecie, użycie złośliwego kodu czy ataki siłowe.

Jedną z najbardziej bezpośrednich korzyści szyfrowania sprzętowego jest to, że wydajność pamięci jest znacznie lepsza niż pamięci szyfrowanej programowo, ponieważ nie występuje przenoszenie zadań szyfrowania na komputer pełniący funkcję hosta. Wszystko odbywa się w urządzeniu pamięci.

Pamięci USB firmy Kingston z szyfrowaniem sprzętowym, takie jak IronKey D500S, to urządzenia chronione hasłem, które są gotowe do użycia natychmiast po wyjęciu z opakowania. W praktyce na początku widoczny jest tylko chroniony przed zapisem wolumin programu uruchamiającego, ponieważ zawiera on aplikację używaną do uwierzytelniania hasła i odblokowywania głównego szyfrowanego woluminu magazynu. Ta procedura pozwala uniknąć instalacji jakiegokolwiek sterownika lub oprogramowania na komputerze pełniącym funkcję hosta.

Co więcej, pamięci USB firmy Kingston z funkcją szyfrowania sprzętowego są wyposażone w podpisane cyfrowo sterowniki oprogramowania, które uniemożliwiają jakąkolwiek manipulację. Obecność tej dodatkowej warstwy zabezpieczeń zapewnia ochronę przed atakami przez lukę BadUSB, właściwą dla oprogramowania sprzętowego urządzeń USB. W przeciwnym razie mogłoby to prowadzić do niejawnie wykonywanych poleceń lub uruchomienia złośliwego kodu na komputerze pełniącym funkcję hosta.

Oczywiście podejście polegające na zablokowaniu wszystkich portów ograniczyłoby ryzyko ataku z wykorzystaniem luki BadUSB, ale po co poświęcać wydajność pracy, stosując tak przestarzałe praktyki? Jak podkreślono wyżej, możliwe jest zapewnienie bezpiecznego środowiska z wykorzystaniem przenośnych urządzeń pamięci dzięki zastosowaniu prostych procedur zakupu i wdrożenia szyfrowanych sprzętowo pamięci USB.

Bezpieczna i zgodna z wymogami praca zdalna

W przypadku osób pracujących zdalnie przebywanie z dala od bezpiecznego środowiska pracy w organizacji wymaga zrewidowania strategii, a także nowego spojrzenia na priorytety.

Jeśli chodzi o plan zapewnienia bezpieczeństwa pracy zdalnej, to czy jest jakaś korzyść z blokowania portów USB w laptopie pracownika tylko po to, aby łączył się on przez Internet z serwerem w celu przesłania lub pobrania dokumentów? Na przykład w podróży jedyną dostępną alternatywą może być otwarte połączenie internetowe, zapewniane przez niezabezpieczony lub niezaufany punkt dostępowy Wi-Fi, co rodzi wiele zagrożeń, które znacznie zwiększają prawdopodobieństwo naruszenia bezpieczeństwa danych. Działania takie jak przechwytywanie

danych i inwigilacja poprzez spoofing, ataki Man-In-the-Middle (MitM) i podsłuchiwanie sieci, to tylko kilka z coraz bardziej wyrafinowanych metod hakerskich, które wykorzystują cyberprzestępcy. Nawet sieci VPN nie są już w pełni bezpieczne.

Połączenie sieciowe organizacji z Internetem to tylko kolejny punkt końcowy, który ze względu na nieuniknioną ekspozycję jest jednocześnie wyjątkowo wrażliwym i narażonym na ataki punktem wejściowym. Otwarcie go na zdalny dostęp niesie ze sobą odrębne zagrożenia, zwłaszcza w przypadku danych wrażliwych.

Zaopatrzenie pracowników zdalnych w urządzenia pamięci USB zabezpieczone hasłem i szyfrowane sprzętowo skutecznie eliminuje potencjalne luki sieciowe. Jednak wprowadzenie takiego rozwiązania wymaga dokładnego sprawdzenia dostępnych urządzeń pamięci USB i tego, jak spełniają one wymogi określonego środowiska pracy zdalnej. Nie sprowadza się to wyłącznie do wyboru pojemności pamięci lub tego, czy powinna ona mieć zarejestrowany numer seryjny. Istotna jest również fizyczna konstrukcja samego urządzenia.

Zabezpieczenie przed ingerencją: solidne rozwiązania

Podstawową kwestią jest to, czy szyfrowana sprzętowo pamięć USB jest zabezpieczona przed ingerencją. To, jak dobrze dane urządzenie jest zabezpieczone przed naruszeniem, określają takie standardy, jak FIPS 140-3, który ma kilka poziomów odpowiadających odporności fizycznej konstrukcji urządzenia pamięci bez uwzględniania metod kryptograficznych.

Powiązany certyfikat FIPS-197 obejmuje wyłącznie atrybuty szyfrowania sprzętowego i takie urządzenia, jak pamięć USB IronKey Vault Privacy 50 i zewnętrzne dyski SSD Vault Privacy 80 – przeznaczone dla przedsiębiorstw, w których wymagania dotyczące bezpieczeństwa danych nie są tak wygórowane, jak w zastosowaniach wojskowych. Pamięci te są tańsze, ale nie zapewniają ochrony przed fizyczną ingerencją.

W przypadku certyfikatu FIPS 140-3 Level 3 (w toku) metody zastosowane w celu ujawnienia manipulacji przy urządzeniu są klasyfikowane jako rozwiązania klasy wojskowej. Firma Kingston dostarcza urządzenia pamięci z certyfikatem FIPS 140-3 Level 3 przedsiębiorstwom oraz instytucjom rządowym i wojskowym na całym świecie.

Zastosowanie żywicy epoksydowej do pokrycia wszystkich obwodów pamięci odpowiedzialnych za zabezpieczenie, a także do sklejenia elementów wewnętrznych z obudową, zapewnia kolejną barierę ochronną. Każda próba otwarcia metalowej obudowy byłaby niezwykle trudna i spowodowałaby pęknięcie wewnętrznych układów i innych komponentów, skutkując utratą funkcjonalności pamięci. Po nałożeniu twardej i nieprzezroczystej żywicy epoksydowej ingerencja w kluczowe komponenty staje się praktycznie niemożliwa. Takie dodatkowe zabezpieczenie mają urządzenia Kingston IronKey D500S i S1000.

Zabezpieczenia przed ingerencją nie ograniczają się wyłącznie do rozwiązań fizycznych, a pamięć Kingston IronKey S1000 wynosi je na nowy poziom. Wewnętrzny układ kryptograficzny pamięci IronKey S1000 potrafi wykrywać wszelkie fizyczne manipulacje i sprawia, że urządzenie staje się bezużyteczne, gdy tylko zostanie włączone. Wykorzystanie szyfrowanych sprzętowo pamięci USB w celu zapewnienia dostępu do poufnych plików i ich przenoszenia to pragmatyczne podejście, które ułatwia pracę zdalną i skutecznie gwarantuje bezpieczeństwo w terenie.

Należy dokładnie sprawdzić funkcje zabezpieczeń urządzeń pamięci USB i same urządzenia, aby mieć pewność, że spełnią one określone potrzeby w danym zastosowaniu. Podejmując decyzję, warto sprawdzić każdą pamięć USB w poszczególnych zastosowaniach, biorąc także pod uwagę wiarygodne certyfikaty. Bez względu na priorytety organizacji Kingston oferuje wybór szyfrowanych sprzętowo pamięci USB i opcji personalizacji w przystępnych cenach, które są przeznaczone do wszystkich rodzajów środowisk – poczynając od zapewnienia podstawowej zgodności, a kończąc na najbardziej wymagających zastosowaniach wojskowych.

Bezpieczeństwo przede wszystkim: bez sieci i bez problemów

Współczesne biuro nie ma granic, a w związku z rozwojem modelu pracy zdalnej z domu wiele firm dostrzega problemy związane z lukami w zabezpieczeniach dostępu zdalnego. Wiele organizacji staje w obliczu tych wyzwań po raz pierwszy i poszukuje bezpieczniejszych sposobów dostosowania się do tego rozwijającego się trendu.

Aby zaspokoić tę potrzebę w wielu branżach, urządzenia pamięci USB z funkcją szyfrowania sprzętowego mają już ugruntowaną pozycję i stanowią bezpieczne rozwiązanie. W porównaniu z nim przesyłanie danych za pośrednictwem sieci może być niepraktyczne lub niepożądane z wielu powodów.

W branży finansowej organy regulacyjne często wymagają udostępniania danych, aby sprawdzić sposób działania firmy i przestrzeganie przez nią przepisów. Ryzyko ekspozycji na zagrożenie jest zbyt duże, aby brać pod uwagę korzystanie z sieci do przesyłania poufnych dokumentów zawierających szczegółowe dane dotyczące inwestycji, transakcji rynkowych i innych poufnych operacji bankowych. Prostym i skutecznym rozwiązaniem jest dostarczenie takich informacji na szyfrowanym sprzętowo nośniku USB.

Korzystanie z bezpiecznych pamięci USB do przenoszenia plików w środowiskach związanych z opieką medyczną jest na porządku dziennym. Służy to również wygodzie lekarzy, którzy mogą dzięki temu analizować dane, wykorzystać je w badaniach lub przedstawić określone przypadki studentom. Istnieją również bardziej praktyczne potrzeby, zwłaszcza w przypadku dedykowanych systemów, takich jak medyczne urządzenia do obrazowania, w przypadku których dostęp do sieci jest niemożliwy lub niebezpieczny. Dzięki zastosowaniu spełniających wymogi, szyfrowanych sprzętowo urządzeń pamięci USB, pliki można łatwo przenosić w celu wykorzystania w innym miejscu.

Co robić, a czego się wystrzegać

✓ **Wybierz spełniające wymogi, bezpieczne pamięci** i zapoznaj się z ich specyfikacjami, aby zakupić urządzenia odpowiadające potrzebom danego zastosowania.

✗ **Nie stosuj w żadnej postaci podejścia „przynieś własne urządzenie (BYOD)** – dla każdej firmy utrata niezaszyfrowanych pamięci to zbyt wysoka cena, jeśli chodzi o szkody finansowe i związane z reputacją.

✓ **Wdróż pakiet oprogramowania do zarządzania punktami końcowymi** i korzystaj z pamięci USB szyfrowanych sprzętowo, które oferują różnicujące funkcje „białej listy".

✗ **Nie licz na to, że „jakoś to będzie".** Prawidłowo oceń wymagania dotyczące lokalnego i zdalnego środowiska pracy.

✓ **Szkol personel** w dziedzinie bezpieczeństwa. W interesie pracowników jest to, aby ich firma była chroniona przed naruszeniem bezpieczeństwa.

✗ **Zapewnienie bezpieczeństwa nie może być tak uciążliwe**, aby użytkownicy szukali rozwiązań typu „shadow IT". To, że zawsze stosowano ogólne zasady, nie oznacza, że sprawdzą się one we wszystkich scenariuszach. Środowisko pracy się zmienia i wybierając właściwe rozwiązania, można stworzyć i egzekwować nowe zasady.

W takim przypadku doskonale sprawdza się pamięć Kingston IronKey Keypad 200 (KP200). Jako nośnik niezależny od systemu operacyjnego nie ma ona woluminu programu uruchamiającego do wprowadzania hasła, lecz klawiaturę alfanumeryczną, która odblokowuje urządzenie, umożliwiając korzystanie z niego na dowolnej platformie. Podobnie jak wielofunkcyjny szwajcarski scyzoryk doskonale sprawdza się w wielu zastosowaniach, w tym również w produkcji – np. w celu bezpiecznego przenoszenia aplikacji stworzonych przez dział IT ds. badań i rozwoju do maszyn sterowanych przez platformy technologii operacyjnych (OT). W przypadku operacji na platformach mieszanych, które również wykorzystują system Linux, pamięć KP200 jest jednym z najprostszych dostępnych i bezpiecznych rozwiązań.

Szyfrowane sprzętowo urządzenia pamięci USB odgrywają istotną rolę również w działaniu organów ochrony porządku publicznego. Zapewniają ochronę i umożliwiają bezpieczne przekazywanie akt spraw, zdjęć i innych dowodów pracownikom terenowym, zespołom śledczym i technikom kryminalistycznym. Firma Kingston oferuje dodatkową korzyść, ponieważ może dostarczyć urządzenia pamięci z wewnętrznym numerem seryjnym nadrukowanym na zewnętrznej obudowie wraz z kodem kreskowym. Dzięki temu udostępnianie i katalogowanie urządzeń pamięci staje się proste i łatwe do śledzenia. Równie łatwe jak ręczne zarejestrowanie numeru seryjnego lub tak szybkie, jak zeskanowanie kodu kreskowego. Trudno wyobrazić sobie łatwiejszy sposób kontroli i zarządzania zapasami. To standardowe rozwiązanie w przypadku pamięci Kingston IronKey D500S, D500SM i S1000B/E jest również dostępne dla innych modeli z funkcją szyfrowania sprzętowego w ramach programu personalizacji firmy Kingston.

Bezpieczeństwo a przenośność pamięci: najnowocześniejsze rozwiązania

Zabezpieczenie hasłem, szyfrowanie sprzętowe, zabezpieczenia przed ingerencją, szczegółowe „białe listy" punktów końcowych, certyfikat FIPS 140-3 Level 3 klasy wojskowej (w toku) i błyskawiczna rejestracja danych to standardowe cechy pamięci USB firmy Kingston, które umożliwiają natychmiastowe wdrożenie.

Te solidne zabezpieczenia gwarantują, że pamięć USB i znajdujące się w niej dane pozostaną bezpieczne w środowisku hosta. Chociaż na papierze specyfikacje mogą wydawać się imponujące, losowy wybór modelu bez żadnej weryfikacji niekoniecznie zapewni idealne dopasowanie nośnika w niektórych organizacjach o bardziej rygorystycznych wymaganiach.

Jako niezależny producent firma Kingston oferuje szeroką gamę opcji spełniających potrzeby klientów. Dzięki programowi personalizacji firmy Kingston dostępne są zaawansowane rozwiązania, które zapewniają bezproblemowe korzystanie z pamięci przez użytkowników.

Bezpieczna personalizacja wykracza poza dostarczanie organizacji własnych identyfikatorów PID pamięci USB w celu umieszczenia na „białej liście". Profil bezpieczeństwa aplikacji uruchamiającej można również dostosować, korzystając z piętnastu różnych preferencyjnych ustawień, poczynając od danych kontaktowych i danych firmy, poprzez włączenie funkcji podpowiedzi do hasła, a kończąc na określeniu maksymalnej liczby prób wprowadzenia hasła. Możliwe jest umieszczenie elementów identyfikacji wizualnej firmy (logo) na obudowie, a poszczególne modele urządzeń pomięci są dostępne w różnych kolorach. Przy minimalnym zamówieniu pięćdziesięciu sztuk urządzeń wszystkie te cechy pozwalają na łatwe wdrożenie rozwiązania.

Jeśli organizacja nie dysponuje jeszcze aplikacją do zarządzania punktami końcowymi przystosowaną do zabezpieczania pamięci USB, oferujemy rozwiązanie, które umożliwia zarządzanie urządzeniami pamięci Kingston, oferując m.in. opcję zdalnego resetowania haseł.

Wszechobecność i wygoda korzystania ze standardu USB sprawiły, że przetrwał on wiele obiecujących technologii, a w przypadku wielu zastosowań pozwala na szybkie i wygodne korzystanie z urządzeń pamięci USB. Łatwo dostępne i zawsze bezpieczne szyfrowane pamięci USB oferują proste rozwiązanie, które można łatwo docenić.

Po co więc martwić się ryzykiem naruszenia danych sieciowych w środowiskach zdalnych? Dzięki szyfrowanym sprzętowo urządzeniom pamięci USB Kingston IronKey rozwiązanie jest w zasięgu ręki.

Aby dowiedzieć się więcej na temat rozwiązań firmy Kingston, odwiedź stronę kingston.com/ironkey lub zadaj szczegółowe pytanie jednemu z naszych ekspertów w dziedzinie szyfrowanych pamięci USB.

#KingstonIsWithYou #KingstonIronkey