# Dlaczego nadal warto korzystać z pamięci USB?

#KingstonIsWithYou

# Dlaczego nadal warto korzystać z pamięci USB?

## Przedmowa i zawartość

Żyjemy w erze cyfrowej, w której 60% wszystkich danych firm na świecie jest przechowywane w chmurze[1], a dyskusja na temat znaczenia technologii pamięci masowej, stworzonej blisko trzydzieści lat temu, może wydawać się nieco nie na miejscu. Jednak od czasu wprowadzenia na rynek ta podstawowa pamięć podlegała i nadal podlega zmianom.

Już dawno minęły czasy, kiedy korzystanie z urządzeń pamięci USB było po prostu standardowym sposobem na zapewnienie połączenia między plikami, dyskami i aplikacjami. Współczesne rozwiązania nie tylko charakteryzują się znacznie większą szybkością transferu danych, ale także zapewniają niezawodność i bezpieczeństwo przenośnych nośników pamięci, które są niezbędne w wielu sytuacjach. Ale dlaczego nadal warto korzystać z pamięci USB, skoro rozwiązania do przechowywania w chmurze pozornie mogą zaoferować wiele podobnych korzyści?

W tej publikacji rozważamy, gdzie w świecie zdominowanym przez usługi w chmurze jest miejsce na urządzenia pamięci flash USB. W oparciu o spostrzeżenia czołowych ekspertów branżowych przeanalizujemy, w jaki sposób współczesne organizacje wykorzystują pamięć USB i omówimy jej znaczenie w odniesieniu do technologii szyfrowania opartego na oprogramowaniu, niezależnych środowisk pamięci masowej oraz bezpieczeństwa danych w punktach końcowych.

| Spis treści | Strony |
|---|---|
| Autorzy | 3 |
| Ewolucja pamięci flash USB | 4 |
| Przenośna pamięć masowa, która odpowiada zmieniającym się potrzebom | 5-6 |
| Szyfrowanie sprzętowe i programowe | 7-8 |
| Rosnąca potrzeba ochrony danych wrażliwych | 9 |
| Ochrona wrażliwych danych finansowych | 10 |
| Bezpieczny dostęp do danych medycznych pacjentów | 11 |
| Przyszłość pamięci USB w erze przechowywania danych w chmurze | 12-13 |
| Podsumowanie i informacje o firmie Kingston | 14 |

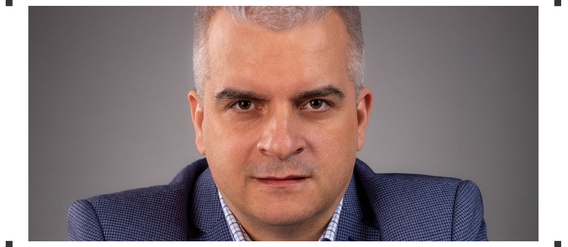
# Dlaczego nadal warto korzystać z pamięci USB?

## Autorzy

Autorami opracowania są trzej branżowi eksperci w dziedzinie IT i nowych technologii.

### Rafael Bloom

Rafael jest wysokiej klasy specjalistą w dziedzinie produktów technologicznych, komunikacji marketingowej i rozwoju biznesu. Jego praktyka doradcza koncentruje się na nowych wyzwaniach organizacyjnych, produktowych i komunikacyjnych, które są związane ze zmianami w technologi i prawie. Ta bardzo zróżnicowana praca wymaga specjalistycznej wiedzy w dziedzinie zarządzania informacjami i zapewnienia zgodności z przepisami w procesie projektowania, ochrony poufności danych i korzystania z nowych technologii, takich jak AdTech, technologia mobilna 5G czy systemy sztucznej inteligencji i uczenia maszynowego.



### Tomasz Surdyk

Dysponując ponad 24-letnim doświadczeniem w dziedzinie bezpieczeństwa IT w instytucjach rządowych, Tomasz jest wiodącym ekspertem, jeśli chodzi o bezpieczeństwo informacji, danych osobowych i cyberbezpieczeństwo. W przeszłości zajmował się kontrolą systemów i sieci teleinformatycznych przetwarzających informacje niejawne i dane osobowe w administracji rządowej, a także w NATO i UE. Od kilku lat jest właścicielem firmy specjalizującej się we wdrażaniu bezpiecznych rozwiązań, które pozwalają zwiększyć bezpieczeństwo informacji biznesowych i danych osobowych.

### David Clarke

David został uznany za jednego z 10 najbardziej wpływowych influencerów, którzy znaleźli się w rankingu Thomson Reuters „30 najbardziej wpływowych liderów opinii i intelektualistów w mediach społecznościowych w dziedzinie zarządzania ryzykiem, zapewnienia zgodności z przepisami i technologii regulacyjnych w Wielkiej Brytanii", a także trafił na listę 50 czołowych światowych ekspertów firmy Kingston Technology. W przeszłości David zajmował wiele stanowisk związanych z zarządzaniem bezpieczeństwem, takich jak Global Head of Security Service Delivery czy Head of Security Infrastructure, w firmach z indeksu Global FTSE 100.

# Ewolucja pamięci flash USB

Kiedy ponad dwadzieścia lat temu na rynku pojawiła się pierwsza pamięć z interfejsem Universal Serial Bus (USB), jej wszechstronna kompatybilność była przełomem w dziedzinie technologii komputerowych. Dzięki możliwości szerokiego udostępnienia wielu operacji na wielu urządzeniach pamięć USB wkrótce ewoluowała, oferując znacznie szybszy transfer danych, interfejs USB 3.0 i jeszcze większe możliwości w porównaniu z tymi, jakie oferowała pierwsza pamięć flash USB w 2000 roku.

Od tego czasu technologia przeszła długą drogę w kontekście przechowywania danych mobilnych i potrzeb związanych z bezpieczeństwem. W centrum uwagi znajduje się obecna generacja urządzeń pamięci USB, które zaprojektowano z myślą o bardzo konkretnych zastosowaniach. Z perspektywy przedsiębiorstw coraz częstsza praca zdalna i hybrydowa, korzystanie z usług w chmurze oraz obawy związane z cyberbezpieczeństwem wymuszają zapotrzebowanie na bardziej efektywne rozwiązania. Ponadto wymogi regulacyjne nakładają obowiązek przechowywania danych w sposób zgodny z przepisami. Presja ta jest często potęgowana przez rozproszone i złożone systemy, które mogą działać zarówno lokalnie, jak i w chmurze.

Do tego dochodzi kwestia rosnącej ilości ustrukturyzowanych i nieustrukturyzowanych danych, takich jak dokumenty, wiadomości e-mail, zdjęcia, filmy i metadane. Wszystko to potęguje złożoność zmieniających się potrzeb przedsiębiorstw w odniesieniu do pamięci masowej.

Ale skoro pamięć masowa w chmurze może sprostać wielu z tych wyzwań, jakie znaczenie we współczesnych realiach biznesowych ma pamięć USB?

> **Wiele osób uważa pamięci USB za staromodne lub trywialne, ponieważ w przeszłości były one używane jako mniej lub bardziej jednorazowe urządzenia o niskiej wydajności i niskim poziomie bezpieczeństwa.**
>
> **- Rafael Bloom**

# Przenośna pamięć masowa, która odpowiada zmieniającym się potrzebom

Co prawda pamięć USB przestała być używana jako przenośna pamięć masowa, ale pojawiły się wysokowydajne rozwiązania do tworzenia osobistych, bezpiecznych lokalnych kopii zapasowych z dodatkową warstwą ochrony danych i poufności. Może to być bardzo istotne, gdy mamy do czynienia z danymi wrażliwymi, w przypadku których musi być zapewniona zgodność z przepisami, takimi jak dokumentacja kadrowa, dane finansowe, dokumentacja medyczna, zabezpieczenie własności intelektualnej i wszelkie informacje umożliwiające identyfikację osób. Ponadto urządzenia obecnej generacji są wyposażone w funkcje szybkiego przesyłania danych, przechowywania, tworzenia kopii zapasowych i zabezpieczeń, które można wykorzystać:

- do zapisywania informacji prawnych, które wymagają osobistego dostarczenia;
- do zapisywania dokumentów prawnych i finansowych, które należy dostarczyć i wydrukować na miejscu lub poza siedzibą firmy;
- w każdym potencjalnie niebezpiecznym środowisku, w którym zagrożenie może stanowić oprogramowanie ransomware;
- do przenoszenia danych do systemów drukowania, w których niedozwolony jest dostęp do sieci.

Wiodący dostawca szyfrowanych pamięci USB, firma Kingston Technology, dotrzymuje kroku rosnącemu zapotrzebowaniu, wprowadzając na rynek takie rozwiązania, jak pamięć Kingston IronKey™ S1000. Ta najlepsza w swojej klasie szyfrowana pamięć USB spełnia najbardziej wymagające standardy, zapewniając ochronę poufnych danych dzięki 256-bitowemu szyfrowaniu XTS-AES oraz oddzielnemu układowi kryptograficznemu z mocnymi zabezpieczeniami przed fizyczną ingerencją. Ponadto urządzenie otrzymało certyfikat FIPS 140-2 Level 3. Oznacza to, że zostało formalnie zatwierdzone przez rząd USA jako urządzenie kryptograficzne, co czyni go idealnym rozwiązaniem dla organizacji potrzebujących pewności skutecznej ochrony danych.

Tego typu szyfrowane sprzętowo pamięci USB oferują scentralizowane rozwiązania do bezpiecznego zarządzania urządzeniami, niezależnie od tego, czy dane są przechowywane w chmurze, czy w siedzibie firmy. Zgodna z przepisami, szyfrowana pamięć masowa, która jest łatwa w użyciu i nie wymaga oprogramowania, pozwala również zaoszczędzić cenny czas specjalistów IT, oferując rozwiązania stworzone z myślą o szybkim i wydajnym wdrożeniu.

# Przenośna pamięć masowa, która odpowiada zmieniającym się potrzebom

Tworzenie kopii zapasowych i archiwizacja to kolejny obszar, w którym pamięć USB może być wykorzystywana do długookresowej ochrony zasobów cyfrowych niezależnie od zewnętrznych usług w chmurze. Chociaż to prawda, że duże transfery danych można łatwo obsługiwać w chmurze, zastrzeżone adresy IP mogą być na tyle wrażliwe, że warto je przechowywać w szyfrowanej, zabezpieczonej pamięci USB, którą można przechowywać w bezpiecznym miejscu z dala od Internetu.

Zawsze będą istniały okoliczności, w których organizacja będzie potrzebować logicznej i fizycznej kontroli nad danymi, zwłaszcza w przypadku korzystania z dysków szyfrowanych. Są także przypadki, kiedy nie można zaszyfrować pamięci na dysku HDD/SSD. Korzystanie z zewnętrznej szyfrowanej pamięci USB, np. Kingston IronKey D300S, rozwiązuje ten problem. To urządzenie pamięci flash USB wykorzystuje 256-bitowe szyfrowanie sprzętowe Advanced Encryption Standard (AES) w trybie XTS, tj. rodzaj szyfru blokowego, który umożliwia szyfrowanie 128-bitowych bloków danych. A gdy zachodzi potrzeba zaszyfrowania danych wykraczających poza ten zakres, technologia AES używa trybu szyfru blokowego XTS, który jest w stanie zapewnić lepszą i silniejszą ochronę danych niż poprzednie tryby.


> Moim zdaniem urządzenia pamięci flash USB nadal pozostają w użyciu i stanowią integralny element bezpieczeństwa danych. Służą m.in.: do szybkiego przenoszenia informacji między urządzeniami oraz do ich odpowiedniego przechowywania i ochrony.
> - Tomasz Surdyk

# Szyfrowanie sprzętowe i programowe

Patrząc na sposób szyfrowania danych, można stwierdzić, że szyfrowanie sprzętowe jest łatwiejsze w zarządzaniu i bezpieczniejsze niż szyfrowanie programowe. Jest tak, ponieważ proces szyfrowania jest oddzielony od reszty systemu hosta, co znacznie utrudnia jego przechwycenie lub złamanie. Scentralizowane zarządzanie na poziomie urządzeń umożliwia kontrolowanie nośników pamięci za pośrednictwem sieci LAN i Internetu, dzięki czemu może być doskonałym narzędziem do:

- ustanawiania i egzekwowania indywidualnych lub grupowych zasad korzystania z szyfrowanych urządzeń pamięci USB;
- kontrolowania operacji na plikach w celu lepszego śledzenia danych przychodzących i wychodzących z organizacji;
- zdalnego tworzenia kopii zapasowych treści w celu przenoszenia danych o kluczowym znaczeniu;
- zdalnego wyłączania urządzeń pamięci USB w przypadku ich utraty lub naruszenia;
- zdalnego zresetowania hasła w przypadku jego zapomnienia.

Prawidłowe zarządzanie autoryzowanymi urządzeniami pamięci minimalizuje ryzyko kopiowania i udostępniania danych wrażliwych. Ponadto współczesne urządzenia pamięci USB z funkcją szyfrowania sprzętowego oferują wiele dodatkowych funkcji zabezpieczeń, które pomagają zapobiegać dostępowi do plików i wiadomości lub ich odczytaniu przez osoby niebędące ich adresatami.

> **Uważam, że szyfrowanie sprzętowe jest lepsze niż szyfrowanie programowe. Różnice między metodami szyfrowania sprzętowego i programowego są znaczące pod względem podatności na ataki typu brute force. Urządzenia szyfrowane sprzętowo niełatwo im się poddają. - Tomasz Surdyk**

# Szyfrowanie sprzętowe i programowe

Chociaż firmy mogą rozważać zastosowanie szyfrowania opartego na oprogramowaniu ze względu na koszty, może być to nieco krótkowzroczne. Rozwiązania oparte na oprogramowaniu współdzielą zasoby hosta z innymi programami, są więc tak bezpieczne, jak bezpieczny jest komputer, i często wymagają aktualizacji oprogramowania. W przeciwnym razie pozostawiają użytkownika bez ochrony. Szyfrowane programowo urządzenia pamięci USB mogą być przedmiotem nieograniczonych ataków typu brute force w celu odgadnięcia hasła i nie są odporne na ataki słownikowe, oparte na wykorzystaniu oprogramowania, które jest w stanie w krótkim czasie przetestować miliony kombinacji znaków.

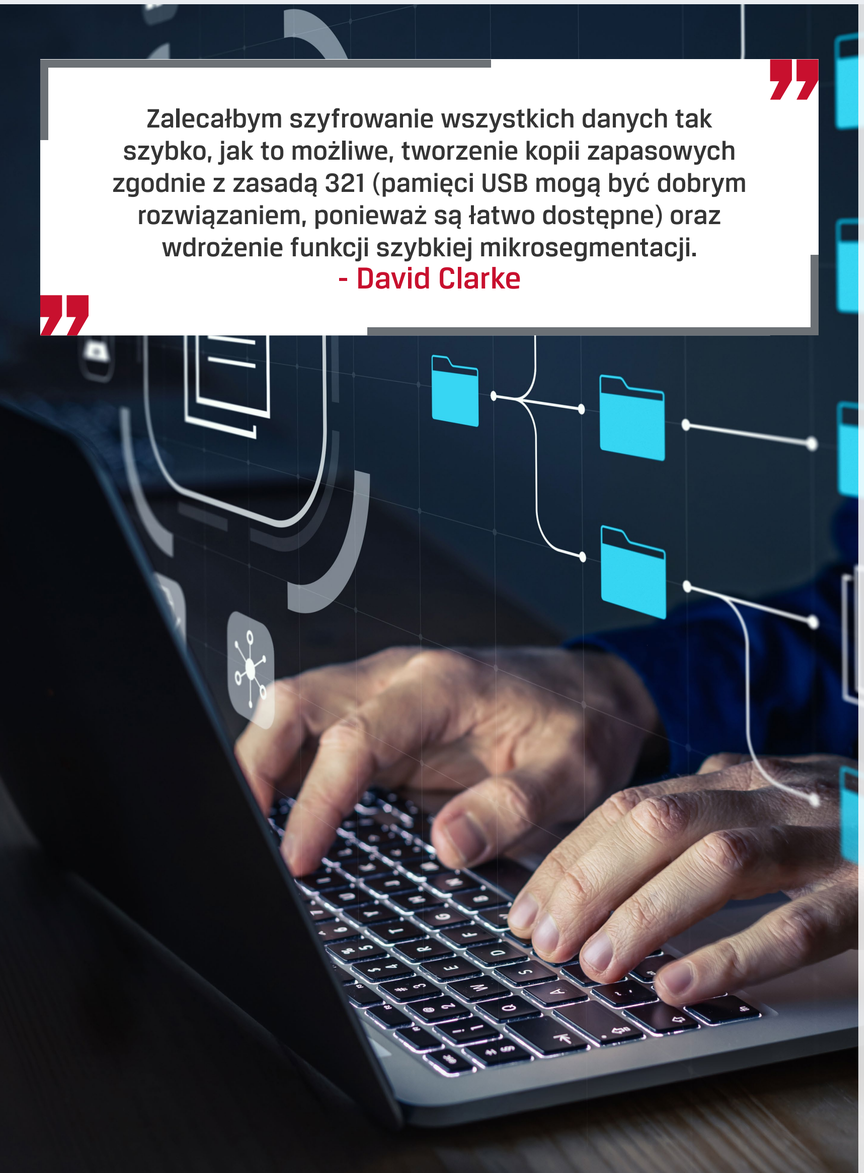
Ponadto szyfrowanie programowe uważa się także za szyfrowanie usuwalne. Każdy pracownik korzystający z pamięci szyfrowanej programowo może skopiować dane i sformatować pamięć USB, aby w ten sposób usunąć szyfrowanie. Następnie może z powrotem skopiować pliki danych i korzystać z pamięci bez utrudnień związanych z uwierzytelnianiem na różnych platformach i systemach operacyjnych.

Jak wspomniano wcześniej, w przypadku szyfrowania sprzętowego fizyczne „szyfrowanie" – a następnie przechowywanie danych – odbywa się niezależnie od systemu hosta. Zapewnia to dodatkową warstwę ochrony, gdyby systemy zostały kiedykolwiek naruszone.

Nie można o tym zapominać, zwłaszcza w takich branżach, jak finanse, ochrona zdrowia czy administracja. Dzieje się tak, ponieważ przepisy takie jak Health Insurance Portability and Accountability Act (HIPAA) oraz Payment Card Industry Data Security Standard (PCI DSS) często narzucają surowe wymagania dotyczące szyfrowania informacji wrażliwych.

Przestrzeganie tych przepisów poprzez stosowanie urządzeń z silnym szyfrowaniem sprzętowym pomaga organizacjom uniknąć kosztownych kar, procesów sądowych i potencjalnie szkodliwego wpływu na reputację. Chociaż pamięci szyfrowane sprzętowo mogą być droższe niż standardowe pamięci USB, koszty związane z naruszeniem przepisów mogą z łatwością dorównać kosztom zakupu setek pamięci – wystarczy zaledwie kilka godzin konsultacji prawnych.

# Rosnąca potrzeba ochrony danych wrażliwych



> Zalecałbym szyfrowanie wszystkich danych tak szybko, jak to możliwe, tworzenie kopii zapasowych zgodnie z zasadą 321 (pamięci USB mogą być dobrym rozwiązaniem, ponieważ są łatwo dostępne) oraz wdrożenie funkcji szybkiej mikrosegmentacji.
> - David Clarke

Jeśli chodzi o ochronę danych wrażliwych przed utratą i kradzieżą, każda organizacja ma obowiązek zadbać o to, aby jej urządzenia posiadały odpowiednie zabezpieczenia. Należy również pamiętać, że choć istnieje niezliczona ilość stale ewoluujących zagrożeń cybernetycznych, istotnymi czynnikami ryzyka pozostają – o ile nie podjęto odpowiednich działań zaradczych – poziom dojrzałości cyfrowej i umiejętności użytkowników w zakresie zarządzania danymi w punktach końcowych. Zagrożenie wewnętrzne, które obejmuje utratę kontroli nad danymi lub urządzeniami pamięci USB, przesyłanie danych poza bezpieczne środowisko, korzystanie z nieszyfrowanych pamięci USB oraz udostępnianie haseł może być efektem braku należytej staranności użytkownika końcowego. Wszystkiego tego można uniknąć dzięki szkoleniom, edukacji i zastosowaniu odpowiednich urządzeń pamięci USB.

Kluczową rolę w radzeniu sobie z potencjalnym zagrożeniem odgrywa również wstępne planowanie i dobrze przetestowana struktura komunikacji. Współczesne cyberzagrożenia mają na celu uderzenie w słabe punkty organizacji.

Plan dotyczący zastosowania szyfrowanych pamięci USB najlepiej opracować zanim jeszcze pojawi się potrzeba jego użycia, poprzez włączenie tych urządzeń i zasad ich użycia do ogólnej strategii bezpieczeństwa organizacji. Brak planu użycia szyfrowanych pamięci USB i odpowiednich wytycznych sprawia, że nie ma się na czym oprzeć, a organizacja jest narażona na ryzyko na każdym poziomie – w tym m.in. na nieprzestrzeganie przepisów, takich jak Ogólne rozporządzenie o ochronie danych (RODO), którego artykuł 32 wyraźnie stanowi, że dane wrażliwe powinny być szyfrowane.

> Organizacja powinna mieć przejrzystą „mapę" swoich danych, w tym m.in. określony poziom ważności i/lub wrażliwości swoich wszystkich zbiorów danych, z planem postępowania w pierwszej kolejności z najważniejszymi danymi poprzez fizyczne usunięcie połączenia lub wyłączenie źródła danych. Możliwość szybkiego odizolowania dotkniętych systemów jest kluczowa, dlatego absolutnie niezbędne jest posiadanie odpowiednio udokumentowanego i przetestowanego planu. - Rafael Bloom

> Użytkownicy przetwarzają dane wrażliwe. Ich utrata zwiększa odpowiedzialność i może znacząco wpłynąć na wizerunek i bezpieczeństwo firmy. W celu ochrony danych wrażliwych należy stosować rozmaite rozwiązania zabezpieczające, w tym szyfrowanie danych. - Tomasz Surdyk

# Ochrona wrażliwych danych finansowych

Oprócz implikacji związanych z bezpieczeństwem istnieją również standardy zgodności, które muszą być spełniane przez rozwiązania do przechowywania danych i tworzenia kopii zapasowych. Niektóre z tych praktyk, takie jak konieczność zarządzania harmonogramami przechowywania danych i egzekwowania ich, są wspólne dla różnych branż, podczas gdy inne, takie jak migracja danych przedsiębiorstwa do chmury, są traktowane w bardzo różny sposób.

W wielu branżach, takich jak sektor usług finansowych, weszły w życie regulacje, które wprowadziły obowiązek odpowiedniego zarządzania danymi. Zwłaszcza banki początkowo niechętnie korzystały z usług podmiotów trzecich w zakresie przechowywania danych i tworzenia kopii zapasowych, a wiele z nich nadal woli pozostawać w posiadaniu całej infrastruktury danych.

Instytucje finansowe są również zobowiązane do przestrzegania coraz dłuższej listy przepisów i norm dotyczących bezpieczeństwa danych, takich jak ustawa Sarbanes-Oxley Act (SOX) czy Ogólne rozporządzenie o ochronie danych (RODO). Jednak wraz ze wzrostem liczby pracowników mobilnych i kontrahentów rośnie ryzyko wycieku danych i niespełniania wymogów narzucanych przez te regulacje.

Prawda jest taka, że wysiłki związane z zapewnieniem zgodności z przepisami mogą zaskakująco łatwo zostać zniweczone, jeśli pracownicy mobilni nie zabezpieczą swoich cyfrowych tożsamości, przenośnych miejsc pracy, dokumentacji klientów i danych finansowych, którymi dysponują. Dlatego coraz więcej organizacji wybiera rozwiązania z zakresu bezpieczeństwa mobilnego, takie jak szyfrowane pamięci USB Kingston IronKey, aby chronić cyfrowe tożsamości i aplikacje bez względu na to, gdzie korzystają z nich pracownicy.

> **Biorąc pod uwagę ogólne przesunięcie trendu w kierunku bardziej rozproszonego zakresu działalności IT i samą skalowalność infrastruktury chmury, łatwo jest zauważyć, że większość branż i MŚP nie zaprząta już sobie głowy zarządzaniem klimatyzowanymi serwerowniami. - Rafael Bloom**

# Bezpieczny dostęp do danych medycznych pacjentów

Opieka zdrowotna to kolejna branża, w której bezpieczeństwo danych jest ważniejsze niż kiedykolwiek dotąd. Informacje o pacjentach są jeszcze bardziej narażone na ryzyko kradzieży, a naruszenia w 2021 r. spowodowały ujawnienie 45,67 mln rekordów danych pacjentów, co stanowi największą roczną liczbę od 2015 r.[2] Jeśli chodzi o przechowywanie danych i tworzenie kopii zapasowych, dane pacjentów to kluczowe i kompleksowe informacje medyczne, które umożliwiają placówkom służby zdrowia bezpieczne leczenie pacjentów.

Może to obejmować wszystko, od plików elektronicznych kartotek zdrowotnych (EHR), zawierających historie zdrowia, wyniki badań, zdjęcia i obrazy radiologiczne, po pliki administracyjne, w tym kartoteki płac, ubezpieczenia pacjentów i rozliczenia finansowe. Nic zatem dziwnego, że w obliczu rosnącej liczby pracowników mobilnych i globalizacji rynku opieki zdrowotnej, który przechodzi poważne wstrząsy i transformacje, podmioty świadczące usługi opieki zdrowotnej troszczą się o bezpieczeństwo danych.

> **W związku z tym, że coraz częściej dochodzi do ataków z wykorzystaniem oprogramowania ransomware, każda organizacja, która ma do czynienia z danymi wrażliwymi, musi zastanowić się, jak działać w warunkach skrajnego zagrożenia. - Rafael Bloom**

Ponadto zlekceważenie zagrożeń i niespełnienie rygorystycznych wymogów, takich jak Health Insurance Portability and Accountability Act (HIPAA) czy Health Information Technology for Economic and Clinical Health Act (HITECH), może skutkować kosztownym naruszeniem danych medycznych, co mogłoby jeszcze bardziej zachwiać zaufaniem pacjentów, partnerów i organów nadzorczych.

Dzięki takim rozwiązaniom jak szyfrowane pamięci USB z serii IronKey firmy Kingston, organizacje opieki zdrowotnej mogą ustanowić zasady dotyczące haseł, korzystania z aplikacji, odzyskiwania danych itp. – w odniesieniu do kilku lub kilku tysięcy nośników – z poziomu jednej konsoli. Dzięki rozwiązaniom przyjaznym dla użytkownika, które eliminują konieczność instalowania sterowników lub innego oprogramowania w celu uzyskania bezpiecznego dostępu do przechowywanych danych, pracownicy mobilni i pracownicy pierwszej linii mogą udzielić pomocy większej liczbie pacjentów. Jednocześnie użytkownicy i administratorzy są w stanie łatwo i szybko zablokować dostęp do danych, bez względu na to, gdzie się znajdują.

# Przyszłość pamięci USB w erze przechowywania danych w chmurze

> **Przechowywanie danych w chmurze to teraźniejszość i przyszłość. Nadal twierdzę, że najbezpieczniejsze jest fizyczne zabezpieczanie danych, np. przy użyciu szyfrowanej pamięci USB. Użytkownicy nie mają pełnej kontroli nad tym, co dzieje się w chmurze. Tymczasem mamy kontrolę nad danymi przechowywanymi na szyfrowanych urządzeniach pamięci USB, które sami zabezpieczamy i przechowujemy. Poza nami nikt nie ma dostępu do tych nośników. - Tomasz Surdyk**

**Jeśli zalety urządzeń pamięci USB są oczywiste, jaka będzie ich rola w przyszłości, w erze przechowywania danych w chmurze?**

Dziesięć lat temu pamięć USB cieszyła się ogromnym zainteresowaniem jako podstawowe narzędzie do wygodnego przechowywania i przenoszenia danych. Jednak wraz z pojawieniem się nowych hybrydowych modeli pracy i coraz bardziej rozproszonych zespołów chmura zapewnia obecnie szybki i łatwy dostęp z wielu urządzeń do przechowywanych informacji. Kiedyś pamięć USB była niezwykle popularna ze względu na wyjątkową wygodę przenoszenia plików. Obecnie jeszcze większą wygodę zapewniają usługi przechowywania danych w chmurze.

Mimo to nadal istnieje wiele ograniczeń dla tej technologii. Niezbędna jest łączność sieciowa, która nie tylko decyduje o tym, jak i kiedy można tworzyć kopie zapasowe lub przesyłać pliki, ale także stanowi dodatkowy problem w kontekście bezpieczeństwa. Gdy firma nakazuje pracownikom korzystanie z chmury, nie zawsze jest w stanie kontrolować, skąd udostępniane są dane. Dlatego prosta czynność uzyskania dostępu do VPN za pośrednictwem prywatnego lub publicznego połączenia Wi-Fi niesie ze sobą ryzyko włamania do sieci. Ponadto usługi w chmurze są bardzo atrakcyjne dla cyberprzestępców, ponieważ większość złośliwego oprogramowania (61%) jest obecnie dostarczana za pośrednictwem aplikacji w chmurze[3].

> **Być może rozsądnie byłoby rozważyć, co się stanie, gdy chmura będzie niedostępna, scenariusze, w których dane muszą być w pełni dostępne, a także w jaki sposób długookresowe przechowywanie danych może zwiększyć podatność na atak. - David Clarke**

# Przyszłość pamięci USB w erze przechowywania danych w chmurze


Z drugiej strony szyfrowanie pamięci USB może być realizowane przez warstwę sprzętową lub oprogramowanie urządzenia. Szyfrowanie sprzętowe, wolne od oprogramowania, to najskuteczniejszy sposób na zapewnienie ochrony przed cyberatakami. Jest to doskonałe, proste rozwiązanie do ochrony przed naruszeniem danych, które spełnia surowe wymogi zgodności z przepisami i zapewnia najwyższy poziom bezpieczeństwa danych, pomagając organizacjom sprawnie zarządzać zagrożeniami i ograniczać ryzyko.

Szyfrowane sprzętowo urządzenia pamięci USB nie wymagają oprogramowania na komputerze, ponieważ są samowystarczalne. Brak luk w oprogramowaniu eliminuje również możliwość ataków siłowych, sniffingu i haszowania pamięci. W przypadku pamięci USB szyfrowanej programowo zachodzi również ryzyko, że użytkownik wyłączy szyfrowanie, formatując pamięć na dowolnym komputerze i używając jej do przechowywania poufnych danych w niebezpieczny sposób.

Urządzenia pamięci USB z szyfrowaniem sprzętowym oferują również wyjątkowe fizyczne środki ochrony danych. Umożliwiają one ustanowienie kryteriów dostępu do informacji przez użytkownika lub administratora i mogą być zintegrowane z istniejącymi rozwiązaniami lokalnych punktów końcowych. Dzięki temu są wygodnym i ekonomicznym rozwiązaniem w wielu sytuacjach, w których przechowywanie danych w chmurze nie sprawdziłoby się lub nie byłoby tak skuteczne. Może to dotyczyć sytuacji, w których dane muszą być przechowywane w urządzeniach niepodłączonych do sieci, pozostawać poufne lub wymagają możliwości dostępu w trybie offline.

> **Jeśli pomyślimy o danych jako o „gorących" lub „zimnych" w zależności od poziomu ich codziennej użyteczności dla organizacji, wówczas bardziej efektywne może być umieszczanie „zimnych" danych w chmurze i opieranie się w większym stopniu na lokalnej pamięci USB w przypadku danych „gorących" – o ile dla organizacji lub określonej krytycznej funkcji lub procesu biznesowego priorytetowa jest ciągłość operacyjna i wysoka wydajność. - Rafael Bloom**

# Podsumowanie

Chociaż nie jesteśmy w stanie przewidzieć przyszłych innowacji, możemy zaoferować szereg wielokrotnie nagradzanych urządzeń pamięci USB, które oferują szeroki wybór rozwiązań szyfrowania dla wszystkich poziomów wymagań w zakresie ochrony danych mobilnych. Od urządzeń pamięci USB wyposażonych w klawiaturę alfanumeryczną, zapewniającą łatwą w użyciu ochronę kodem PIN, poprzez certyfikat FIPS 140-2-Level 3, gwarantujący najwyższy poziom szyfrowania wraz z zabezpieczeniami przed fizyczną ingerencją, po technologię SuperSpeed USB 3.1, która nie wpływa na obniżenie poziomu bezpieczeństwa, produkty Kingston IronKey zostały zaprojektowane w taki sposób, aby sprostać wyzwaniom związanym ochroną danych na urządzeniach pamięci USB, które gwarantują wydajne i bezpieczne przenoszenie i przechowywanie danych.

Nasz wyspecjalizowany zespół ekspertów jest gotowy udzielić Ci wsparcia na każdym etapie procesu związanego z przechowywaniem danych, oferując pomoc w znalezieniu odpowiedniego rozwiązania pamięci masowej, które spełni Twoje potrzeby.

Mamy umiejętności i możliwości techniczne, aby pomóc Ci zachować bezpieczeństwo poufnych informacji i przestrzegać nowych przepisów – niezależnie od tego, czy chcesz stworzyć plan wdrożenia szyfrowanej pamięci USB, wybrać najlepsze urządzenia pamięci USB dla swojej firmy, czy wprowadzić i egzekwować określone zasady bezpieczeństwa. Oferując wysoce spersonalizowaną usługę, dostarczamy produkty, które są zgodne z priorytetami przechowywania danych naszych klientów i umożliwiają dotrzymanie kroku niezwykle szybkim zmianom, jakim podlega świat biznesu.

## O firmie Kingston

Dzięki 35-letniemu doświadczeniu firma Kingston dysponuje wiedzą pozwalającą na identyfikację i rozwiązywanie problemów związanych z danymi mobilnymi, aby ułatwić pracownikom bezpieczną pracę bez uszczerbku dla firmy.


1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers




**#KingstonIsWithYou**