



Optymalna ochrona
w punktach końcowych –
opracowanie
przygotowane we
współpracy z firmą
Matrix42

MATRIX42

#KingstonIsWithYou



Optymalna ochrona w punktach końcowych – opracowanie ◀ ◀◀ ▶▶ ▶▶ przygotowane we współpracy z firmą Matrix42

Wprowadzenie

Ochrona danych to podstawowe zadanie firm, instytucji państwowych i osób prywatnych w dzisiejszym świecie.

Naruszenia ochrony danych, ataki hakerskie i „czynniki ludzkie” stale przypominają nam o powszechnie występujących zagrożeniach i ryzyku. Koszty związane z naruszeniem ochrony danych – zarówno finansowe, jak i te dotyczące reputacji – mogą być ogromne. Wymagania zaawansowanego bezpieczeństwa cybernetycznego i strategię ochrony przed utratą danych (DLP) zależą od niezawodnych i skutecznych rozwiązań w zakresie przechowywania i pamięci masowej.

Istotnym krokiem jest zastosowanie szyfrowania i pamięci do szybkiego zapisu i przechowywania danych w połączeniu z najlepszymi praktykami, standardami i zasadami postępowania. Zgubione laptopy i pamięci USB stanowią zagrożenie ujawnienia informacji dotyczących osób prywatnych i firm. Kingston oferuje rozwiązania, które pozwalają zapobiec zagrożeniom i pomagają zmniejszyć ryzyko, jednocześnie uzupełniając istniejące lub dopiero tworzone procedury bezpieczeństwa.



Optymalna ochrona w punktach końcowych – opracowanie ◀ ◀◀ ▶▶ ▶▶ przygotowane we współpracy z firmą Matrix42

Zawartość

W ramach tej krótkiej publikacji przyglądamy się rozwiązaniom dla punktów końcowych i pokazujemy, w jaki sposób szyfrowane pamięci USB firmy Kingston, jej program personalizacji oraz oprogramowanie EgoSecure Data Protection firmy Matrix42 pomogły rozwiązać problemy organizacji w sześciu różnych sektorach, zapewniając rozwiązania dostosowane do ich potrzeb biznesowych.

Dokładnie przyglądając się sytuacji w tych sześciu sektorach, sprawdzamy, w jaki sposób radzą sobie one z wyzwaniami związanymi z ochroną w punktach końcowych.

Spis treści

Rozdział 1	Przykład zastosowania w branży – sektor publiczny	4
Rozdział 2	Przykład zastosowania w branży – opieka zdrowotna	5
Rozdział 3	Przykład zastosowania w branży – finanse	6
Rozdział 4	Przykład zastosowania w branży – motoryzacja	7
Rozdział 5	Przykład zastosowania w branży – telekomunikacja	8
Rozdział 6	Przykład zastosowania w branży – produkcja	9
Rozdział 7	Rozwiązania firm Kingston i Matrix42	10
	Podsumowanie	11
	O firmie Kingston	12



Rozdział 1: Przykład zastosowania w branży sektor publiczny



Sytuacja:

W sektorze publicznym bardzo często korzysta się z urządzeń USB. Na przykład pracownicy instytucji odpowiedzialnych za utrzymanie porządku publicznego kopiują do swoich systemów z aparatów cyfrowych zdjęcia dokumentujące wykroczenia parkingowe i administracyjne, używając przewodów USB. Organy policji otrzymują dane dotyczące dochodzeń na zewnętrznych urządzeniach do przechowywania danych. Dane te wymagają przeniesienia i zabezpieczenia przed nieuprawnionym dostępem.

Wyzwanie:

W związku z dużym zapotrzebowaniem na urządzenia USB pracownicy regularnie proszą o zaopatrzenie w nośniki pamięci USB. Ze względów bezpieczeństwa korzystanie z prywatnych i niezatwierdzonych urządzeń musi być zablokowane. Jeśli pracownik potrzebuje nowego nośnika pamięci USB, dział pomocy technicznej powinien go jak najszybciej dostarczyć, aby nie opóźniać jego pracy. Warto podkreślić, że korzystanie z odpowiednich urządzeń USB nie powoduje żadnych problemów związanych z bezpieczeństwem.

Rozwiązanie:

Połączenie kontroli nad urządzeniami, filtrowania i szyfrowania danych pozwala zastosować następujące rozwiązania:

Nieznane urządzenia są standardowo blokowane w punktach końcowych komputerów. Obsługa urządzeń z nośnikami danych, takich jak aparaty cyfrowe, jest dozwolona tylko w zakresie niektórych funkcji, takich jak odczyt plików graficznych. Operacje zapisu są standardowo szyfrowane i dozwolone tylko na zatwierdzonych urządzeniach USB. Wszystkie dane objęte dostępem są rejestrowane. Zarządzanie zatwierdzonymi urządzeniami można uprościć, przydzielając im numery seryjne oraz identyfikatory sprzętu. Oprogramowanie Service Management firmy Matrix42 umożliwia użytkownikowi zamówienie spersonalizowanej pamięci USB firmy Kingston Technology przez samoobsługowy portal. Po zakończeniu procesu zatwierdzenia urządzenie USB zostaje automatycznie dopuszczone do użycia w ramach systemu EgoSecure Data Protection.

“ Nasi pracownicy doceniają to, że mogą łatwo i szybko otrzymać nowe urządzenie USB po krótkim procesie zatwierdzenia. Jesteśmy bardzo zadowoleni z programu personalizacji firmy Kingston Technology i łatwości obsługi rozwiązania Matrix42, łączącego zarządzanie usługami z bezpieczeństwem punktów końcowych. ”

Kierownik działu pomocy technicznej, sektor publiczny

Rozdział 2: Przykład zastosowania w branży opieka zdrowotna

Sytuacja:

Zewnętrzne nośniki danych są nadal często wykorzystywane do wymiany danych między pracownikami i zewnętrznymi instytucjami.

Na przykład szpitale w Niemczech muszą przekazywać do rejestru chorób nowotworowych bieżące informacje o przypadkach zachorowań na raka i postępach ich leczenia. Dla ułatwienia dane te są często przekazywane z wykorzystaniem przenośnych urządzeń do przechowywania danych.

Również lekarze często przenoszą dokumenty, np. dane z badań do prezentacji na wykładzie, korzystając z pamięci USB.

Wyzwanie:

Dane pacjentów mają wrażliwy charakter i nie mogą dostać się w ręce niepowołanych osób. Dlatego należy zwiększyć i wzmocnić ochronę danych. Utrata nośnika z danymi może spowodować poważne problemy, nie tylko ze względu na wymogi RODO, lecz także na dobro pacjentów. Dlatego istotne jest, aby dostęp do urządzeń pamięci USB był kontrolowany, monitorowany i szyfrowany.

Rozwiązanie:

Oprogramowanie EgoSecure Data Protection łączy różne środki ochrony, takie jak kontrola dostępu, audyt danych oraz filtrowanie i szyfrowanie, w jedno rozwiązanie. Administratorzy systemów IT mogą zdecydować, który pracownicy otrzymają uprawnienia dostępu do określonych urządzeń. Możliwe jest np. określanie wyjątków na podstawie numeru seryjnego i identyfikatora sprzętu. Identyfikatory te można zdefiniować w ramach programu personalizacji firmy Kingston Technology, dzięki czemu wystarczy skonfigurować w oprogramowaniu do zarządzania EgoSecure Data Protection tylko jedną wartość, aby możliwe było korzystanie wyłącznie z urządzeń zatwierdzonych przez firmę. Pozwala to ograniczyć do minimum wysiłek administracyjny i zwiększa bezpieczeństwo danych (RODO, CCPA, HIPAA itp.), ponieważ dostęp jest szyfrowany i monitorowany.

“ Korzystaliśmy już szyfrowanych urządzeń pamięci USB firmy Kingston. Teraz, dzięki oprogramowaniu EgoSecure Data Protection, mamy również możliwość śledzenia transferów danych pacjentów zgodnie z wymogami RODO obowiązującymi w UE. ”

**Administrator bezpieczeństwa informacji,
szpital uniwersytecki**



Rozdział 3: Przykład zastosowania w branży finanse



Sytuacja:

Banki podlegają różnym wymogom w zakresie zgodności procedur z prawem. Jednym z nich jest zapewnienie zgodności ze standardem bezpieczeństwa PCI-DSS (Payment Card Industry Data Security Standard). Wymagania standardu PCI-DSS obejmują konieczność szyfrowania danych, analizę podatności na zagrożenia oraz filtrowanie danych. Celem jest ograniczenie do minimum lub całkowite wyeliminowanie zagrożeń i ryzyka naruszenia bezpieczeństwa IT.

Wyzwanie:

W punkcie końcowym występuje wiele zagrożeń dla bezpieczeństwa IT. Pracownicy mają na co dzień do czynienia z informacjami o kartach płatniczych osób prywatnych i firm oraz przetwarzają poufne dane z instytucji finansowych. W związku z tym są narażeni na ryzyko, że dane z chmury, poczty e-mail, pamięci USB lub sieci, jeśli nie będą odpowiednio chronione, mogą zostać naruszone przez złośliwe oprogramowanie lub przypadkowo wpaść w ręce niepowołanych osób. Taki incydent stwarzałby ryzyko poniesienia przez bank konsekwencji finansowych na podstawie regulacji RODO, PCI-DSS, a także ustawy Sarbanes-Oxley Act. Ponadto cyberprzestępcy próbują na różne sposoby uzyskać wpływ na systemy bankowe,

manipulować nimi i stają się w tym coraz bardziej kreatywni. Na przykład niedawno doszło do cyberprzestępstwa, którego obiektem stały się bankomaty. W celu kradzieży pieniędzy po odcięciu zasilania ich system uruchamiano z rozruchowego urządzenia USB.

Rozwiązanie:

Systemy IT wymagają zabezpieczenia z wykorzystaniem wielowarstwowej struktury środków ochronnych. Można to osiągnąć poprzez kontrolę aplikacji, kontrolę urządzeń, wykrywanie anomalii, wykorzystanie narzędzi analizy zachowań użytkowników i urządzeń (UEBA) oraz monitorowanie i pełne szyfrowanie dysków z uwierzytelnianiem przed uruchomieniem systemu. Firma Matrix42 może wdrożyć takie rozwiązanie w zautomatyzowanym i zintegrowanym środowisku, aby możliwe było użycie tylko zatwierdzonych aplikacji i zaszyfrowanych urządzeń USB. System wykrywa także podejrzaną lub złośliwą aktywność i automatycznie inicjuje dalsze działania. Jeśli chodzi o korzystanie z pamięci USB, zastosowanie spersonalizowanych pamięci USB firmy Kingston Technology pozwala łatwo umieścić je na liście zatwierdzonych urządzeń i szyfrować dane w sposób umożliwiający ich śledzenie. Ułatwia to znacząco, bez dodatkowego wysiłku, zapewnienie zgodności z obowiązującymi przepisami.



„Dzięki oprogramowaniu EgoSecure Data Protection i funkcji „białej listy” możliwe jest zatwierdzenie do użycia wyłącznie szyfrowanych urządzeń pamięci USB firmy Kingston. Lista zawiera szyfrowane pamięci USB Kingston ze spersonalizowanym identyfikatorem sprzętu – inne urządzenia są niedozwolone. Pozwala to znacząco zmniejszyć wysiłek administracyjny, a jednocześnie zwiększyć bezpieczeństwo!”

Kierownik działu IT, firma finansowa

Rozdział 4: Przykład zastosowania w branży motoryzacja



Sytuacja:

W branży motoryzacyjnej urządzenia pamięci USB są wykorzystywane w różnych obszarach. Na przykład dane badawcze są zapisywane na zewnętrznych urządzeniach pamięci masowej i przekazywane sobie przez inżynierów pracujących w firmie. W podobny sposób przenoszone są również ze środowiska IT do środowiska OT pliki do konfiguracji maszyn produkcyjnych. Tego typu dane mają wrażliwy charakter i powinny być chronione przed szpiegostwem przemysłowym i kradzieżą. W przeciwnym razie zgromadzone „know-how” mogłoby trafić w niepowołane ręce.

Wyzwanie:

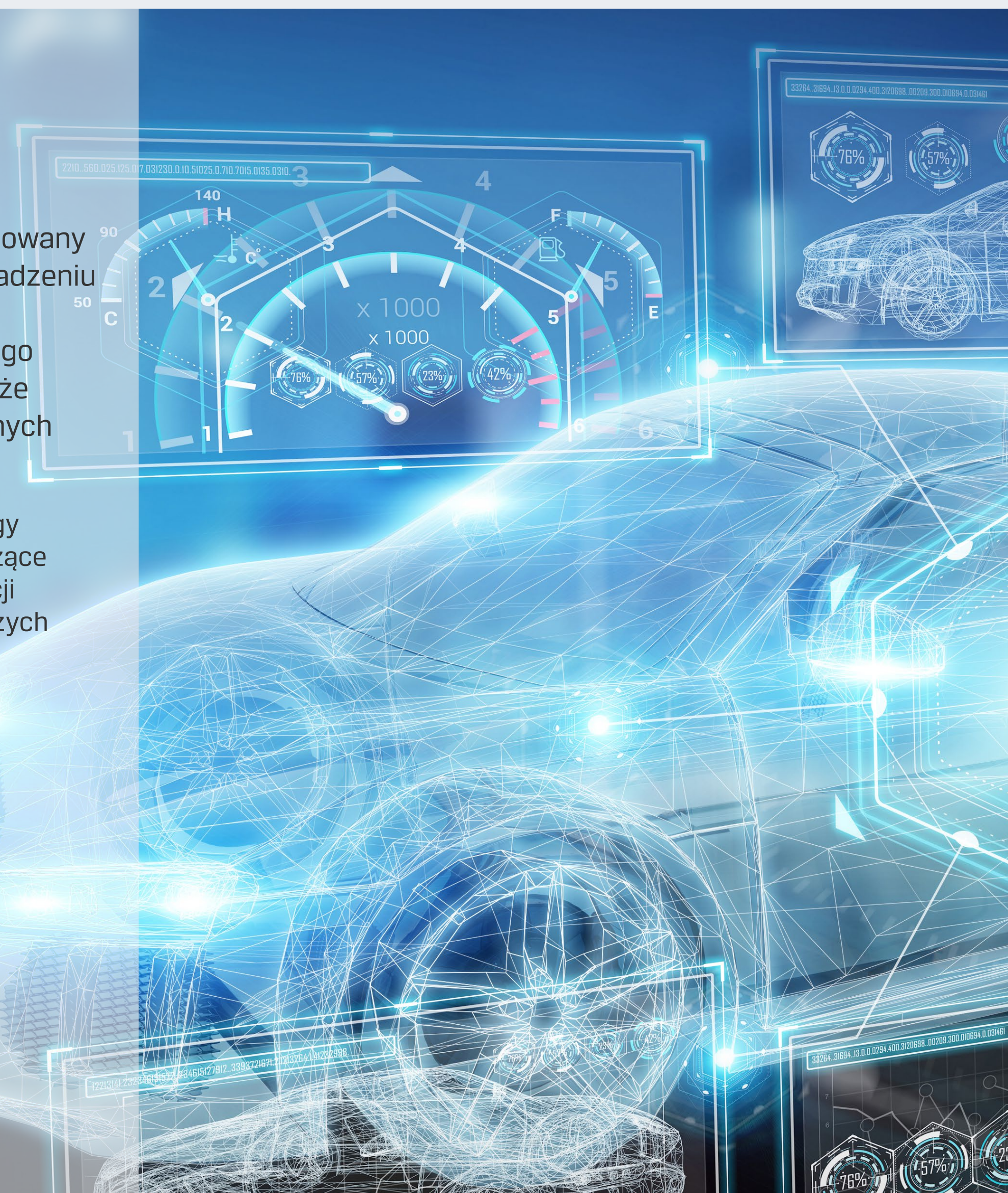
Branża motoryzacyjna podlega wymogom zapewnienia zgodności z regulacjami TISAX, dotyczącymi ochrony prototypów, ENX, ISO27001, dotyczącymi „powiązania z podmiotami zewnętrznymi” oraz RODO. Zgodnie ze standardem TISAX (punkty 9.1, 9.5 i 10.1 dotyczące kontroli) dostęp do danych musi podlegać kontroli, monitorowaniu, filtrowaniu i szyfrowaniu. Środki te muszą być również stosowane zgodnie z wymogami innych regulacji, takich jak RODO czy ISO27001, we wszystkich obszarach działalności firm motoryzacyjnych.

Rozwiązanie:

Szyfrowane urządzenia pamięci USB firmy Kingston Technology zabezpieczają dane poprzez szyfrowanie sprzętowe. Urządzenia te mogą otrzymać spersonalizowany numer seryjny i identyfikator sprzętu, które po wprowadzeniu do systemu EgoSecure Data Protection umożliwiają automatyczne przyznawanie uprawnień do określonego wykorzystania danych. Ponadto przepływ danych może być monitorowany i analizowany pod kątem podejrzanych działań.

“ Dzięki rozwiązaniom firm Matrix42 i Kingston Technology mogliśmy wdrożyć wymagania standardu TISAX dotyczące kontroli, określone w punktach 9.5 (dostęp do informacji i aplikacji) i 10.1 (szyfrowanie), bez konieczności większych zmian w procedurach dotyczących postępowania użytkowników. ”

**Dyrektor ds. technologii,
firma z branży motoryzacyjnej**



Rozdział 5: Przykład zastosowania w branży telekomunikacja



Sytuacja:

Dostawcy usług telekomunikacyjnych gromadzą duże ilości informacji o klientach. Są to dane wrażliwe, zwłaszcza w kontekście RODO. Dlatego konieczne jest stosowanie odpowiednich środków, aby zapobiec utracie i kradzieży danych.

Wyzwanie:

Pracownicy firm telekomunikacyjnych codziennie mają do czynienia z danymi klientów. Większość danych jest przechowywana w aplikacjach biznesowych. Istnieje jednak ryzyko, że umowy z klientami, a nawet wyeksportowane pliki z bazy danych, będą przechowywane w punkcie końcowym i podłączonych do niego urządzeniach zewnętrznych. Użytkownicy często wykorzystują do wymiany danych zewnętrzne urządzenia pamięci. Dlatego bardzo ważne jest wykrywanie i korygowanie albo zapobieganie niewłaściwym praktykom związanym z przechowywaniem danych.

Rozwiązanie:

Aby uprościć proces zaopatrzenia, szyfrowane urządzenia pamięci USB firmy Kingston Technology ze spersonalizowanym identyfikatorem produktu można szybko zakupić z poziomu wstępnie zdefiniowanej białej listy w aplikacji EgoSecure Data Protection, aby zostały dostarczone w ramach katalogu

usług firmy Matrix42. Czynności przechowywania i eksportu danych, które mogą zawierać poufne informacje, mogą być automatycznie identyfikowane i korygowane poprzez dogłębną kontrolę treści w oparciu o funkcje skanowania „danych w użyciu” i „danych w spoczynku”. Przepływ danych podlega scentralizowanej rejestracji. Dzięki temu pracownik może szybko otrzymać nowe urządzenie do przechowywania danych po jego zamówieniu i zatwierdzeniu. Daje to gwarancję zgodności z wymogami RODO.

“ Dzięki samoobsługowemu portalowi Matrix42 nasi użytkownicy mogą sami zamawiać potrzebne nośniki do przechowywania danych. Po zatwierdzeniu i dostarczeniu zamówienia, urządzenie jest następnie dopuszczane przez system kontroli urządzeń EgoSecure. Rozwiązania oferowane przez Matrix42 i produkty Kingston Technology zwiększają wydajność i bezpieczeństwo naszej firmy. ”

**Dyrektor ds. technologii,
firma z branży telekomunikacyjnej**



Rozdział 6: Przykład zastosowania w branży

Branża produkcyjna



Sytuacja:

Dane cyfrowe są „złotem” przyszłości. Te cenne dane w branży produkcyjnej obejmują plany produkcji, informacje o klientach i dostawcach oraz know-how firmy. Ich utrata może skutkować nie tylko bardzo surowymi karami przewidzianymi przez RODO, ale także problemami na znacznie szerszą skalę, w tym może także wpłynąć na reputację firmy. Niestety, zgubione pamięci USB można znaleźć na co dzień w taksówkach, pralniach, na lotniskach, dworcach kolejowych i parkingach.

Wyzwanie:

Urządzenia pamięci masowej często zawierają wrażliwe dane, które niestety często nie są zaszyfrowane. Zdarza się również, że technicy serwisowi używają zewnętrznych nośników danych do instalowania aktualizacji maszyn produkcyjnych. Takie postępowanie grozi wprowadzeniem do sieci złośliwego oprogramowania.

Rozwiązanie:

Szyfrowane urządzenia pamięci USB firmy Kingston Technology zabezpieczają dane poprzez szyfrowanie sprzętowe. Urządzenia te mogą zostać dostarczone ze spersonalizowanym numerem seryjnym i identyfikatorem sprzętu, które można następnie wprowadzić do systemu EgoSecure Data Protection w celu automatycznego przyznania uprawnień do określonego wykorzystania danych. Ponadto przepływ danych może być monitorowany i analizowany pod kątem podejrzanych działań.

“ Szyfrowanie danych produkcyjnych jest dla nas bardzo ważne z punktu widzenia ochrony przed kradzieżą danych. Te wysoce wrażliwe dane mogą być zapisywane wyłącznie na zatwierdzonych szyfrowanych urządzeniach pamięci USB firmy Kingston z wykorzystaniem funkcji filtrowania plików aplikacji EgoSecure Data Protection. Zapis danych produkcyjnych na innych urządzeniach USB jest blokowany, a dostęp do zapisu w pamięci zewnętrznej jest zabezpieczony przez działające na bieżąco funkcje szyfrowania i rejestracji EgoSecure. ”

Specjalista ds. bezpieczeństwa IT, branża produkcyjna



Istotnym krokiem jest zastosowanie szyfrowania i pamięci do szybkiego zapisu i przechowywania danych w połączeniu z najlepszymi praktykami, standardami i zasadami postępowania. Zgubione laptopy i pamięci USB stanowią zagrożenie ujawnienia informacji dotyczących osób prywatnych i firm. Firma Kingston Technology oferuje rozwiązania, które pozwalają zapobiec zagrożeniom i pomagają zmniejszyć ryzyko, jednocześnie uzupełniając istniejące lub dopiero tworzone procedury bezpieczeństwa.

Szyfrowane urządzenia pamięci USB firmy Kingston Technology

Szyfrowane sprzętowo urządzenia pamięci USB firmy Kingston Technology to rozwiązanie zapewniające ochronę przenoszonych danych, które sprawdza się po obu stronach zapory sieciowej organizacji. Pamięć stworzona z myślą o skutecznej ochronie danych wrażliwych ułatwia spełnienie wymogów odpowiednich standardów branżowych, dyrektyw i innych przepisów. Nasze produkty są zgodne z przepisami TAA, posiadają certyfikat FIPS i oferują pojemność do 128 GB, co czyni je doskonałym rozwiązaniem zarówno dla firm, jak i instytucji administracji publicznej.



Program bezpiecznej personalizacji

Szyfrowane urządzenia pamięci USB firmy Kingston Technology można na wiele sposobów dostosowywać do indywidualnych potrzeb organizacji. Dodając wybrane funkcje, można stworzyć unikalne i istotne dla codziennego funkcjonowania pamięci. Firma Kingston Technology oferuje łatwy i wygodny sposób zamawiania spersonalizowanych, szyfrowanych pamięci USB za pośrednictwem wyselekcjonowanych sprzedawców. Linia szyfrowanych produktów USB firmy Kingston Technology obejmuje modele z serii DTP30, DT4000G2 i IKD300. W ramach programu oferowane są najczęściej wybierane przez klientów opcje, takie jak numeracja seryjna, zabezpieczenie podwójnym hasłem czy umieszczenie na urządzeniu logo klienta. Przy zamówieniu minimum 50 sztuk lub kolejnym zamówieniu co najmniej 25 sztuk program zapewnia dokładnie to, czego potrzebuje dana organizacja.

Oprogramowanie EgoSecure Data Protection firmy Matrix42

Oprogramowanie EgoSecure Data Protection firmy Matrix42 umożliwia firmom kompleksowe zarządzanie bezpieczeństwem w celu ochrony urządzeń, systemów i danych. Rozwiązanie automatyzuje cały proces, poczynając od zapobiegania zagrożeniom i wykrywania ich, a kończąc na działaniach zaradczych w przypadku wystąpienia szkód – a wszystko to bez utraty wydajności.

Ochrona danych i dbałość o cyberbezpieczeństwo mogą wydawać się uciążliwym obowiązkiem. Wymagania dotyczące pracy w środowisku cyfrowym znacząco zmieniły się w sytuacji, gdy pracownicy mogą samodzielnie decydować, kiedy, gdzie i z jakich urządzeń korzystają. Odpowiednie połączenie szyfrowanych sprzętowo pamięci USB i oprogramowania do zarządzania punktami końcowymi może pomóc organizacjom przejąć kontrolę nad wykorzystywanymi przez nie urządzeniami. Pozwoli to ograniczyć ryzyko naruszenia danych i wspomóc realizację bieżącej strategii zapewnienia zgodności z RODO.





O firmie Kingston

Dzięki ponad 30-letniemu doświadczeniu firma Kingston Technology dysponuje wiedzą umożliwiającą identyfikację i rozwiązanie problemów bezpieczeństwa punktów końcowych bez zakłóceń w działaniu organizacji.

©2021 Kingston Technology Europe Co LLP i Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, England.

Tel: +44 (0) 1932 738888 Faks: +44 (0) 1932 785469. Wszelkie prawa zastrzeżone. Wszelkie znaki towarowe i zastrzeżone znaki towarowe są własnością odpowiednich właścicieli.

#KingstonIsWithYou