SZYFROWANIE PROGRAMOWE A ZGODNOŚĆ Z PRZEPISAMI: TAŃSZE ROZWIĄZANIE WIĄŻĄCE SIĘ Z POWAŻNYMI ZAGROŻENIAMI DLA BEZPIECZEŃSTWA

WYMOGI PRAWNE I DOTYCZĄCE ZGODNOŚCI Z PRZEPISAMI

Zapewnienie bezpieczeństwa danych było kiedyś wyłącznie domeną działów IT, jednak z powodu ciągłych naruszeń poufności danych klientów rządy na całym świecie nakładają na firmy coraz więcej wymagań dotyczących szyfrowania i ochrony wszystkich danych, które umożliwiają identyfikację osób.

Od regulacji HIPAA w obszarze służby zdrowia po rozporządzenia RODO (GDPR) w regionie EMEA oraz CCPA w stanie Kalifornia – szyfrowanie chronionych klas danych jest obecnie wymagane przepisami. W ciągu ostatnich 3 lat, w następstwie gwałtownego wzrostu liczby przepisów i związanych z nimi kar oraz ryzyka prawnego, liczba organizacji nadzorujących zapewnienie zgodności z przepisami rosła w tempie wykładniczym.

Wskutek tych zmian działy IT mają trudności z nadążaniem za wymogami dotyczącymi zapewnienia bezpieczeństwa i rosnącymi kosztami. W czasach pandemii COVID budżety są wykorzystywane na dodatkowe inwestycje w zasoby sprzętowe i zapory kosztem skupienia się na szyfrowaniu danych.

W rzeczywistości rośnie popularność szyfrowania programowego z wykorzystaniem oprogramowania Microsoft BitLocker® lub oprogramowania do zarządzania punktami końcowymi takich firm, jak Symantec, McAfee itp. Niektóre firmy i użytkownicy korzystają również ze standardowych urządzeń pamięci USB z „niewidoczną" partycją tworzoną przez oprogramowanie oferowane przez niektórych producentów.

SZYFROWANIE A PRZENOSZENIE DANYCH

Pracownicy i konsumenci chcą mieć możliwość zabrania ze sobą potrzebnych danych. W takim przypadku mają do dyspozycji

1. usługi w chmurze, które pozwalają uzyskać dostęp do danych z dowolnego urządzenia połączonego z Internetem. Jednak ta elastyczność ma swoją cenę. Przechowywanie danych w chmurze pozbawia użytkownika lub firmę kontroli nad danymi i wiąże się z potencjalnym ryzykiem, ponieważ zdarzały się przypadki pozostawienia serwerów w chmurze bez zabezpieczeń lub uzyskania do nich nieuprawnionego dostępu.
2. Standardowe pamięci USB: chociaż noszenie przy sobie pamięci USB wydaje się bezpieczniejsze, zachodzi znaczne ryzyko naruszenia danych wskutek utraty takiego nośnika. Krąży wiele historii o zgubionych pamięciach USB zawierających poufne informacje lub o szufladach w pralniach pełnych pozostawionych nośników.
3. Szyfrowane sprzętowo pamięci USB: tego typu pamięci mają niestandardową architekturę, która obejmuje wbudowany kontroler szyfrowania i funkcje kontroli dostępu. Dane są szyfrowane z wykorzystaniem najsilniejszego algorytmu szyfrowania AES zkluczem 256-bitowym w trybie XTS, a także przy użyciu innych dostępnych zabezpieczeń w celu ograniczenia skutków ataków fizycznych i opartych na oprogramowaniu sprzętowym. Pamięci te są produkowane przez firmy specjalizujące się w produkcji urządzeń zabezpieczających i chociaż są droższe niż standardowe pamięci USB, zapewniają większe bezpieczeństwo danych. Pamięci oparte na standardzie FIPS 197 lub FIPS 140-2 poziomu 3 zapewniają wyższy poziom ochrony i poczucie pewności.
4. Standardowe pamięci USB z szyfrowaniem programowym: W celu zapewnienia bezpieczeństwa wymaganego przepisami można zastosować szyfrowanie programowe z wykorzystaniem oprogramowania BitLocker lub innych narzędzi. To dobre rozwiązanie, ponieważ jest stosunkowo niedrogie i opiera się na tym samym algorytmie szyfrowania – AES-256 XTS.

Nie zaskakuje fakt, że w większości przypadków firmy i branże wybierają opcję nr 4, tj. korzystanie ze standardowych urządzeń pamięci USB z szyfrowaniem programowym. Dzieje się tak głównie dlatego, że rozwiązania do szyfrowania programowego, takie jak oprogramowanie BitLocker lub inne narzędzia do przechowywania danych, są „darmowe".

SZYFROWANIE PROGRAMOWE JEST NIEZGODNE Z PRZEPISAMI

Dla specjalistów ds. zapewnienia bezpieczeństwa firmy szyfrowanie programowe może oferować dokładnie takie same możliwości jak droższe urządzenia pamięci USB z funkcją szyfrowania sprzętowego. Ale czy jest to właściwa droga? Budżety są napięte, dlatego firmy, aby zapewnić zgodność z przepisami, przechodzą na szyfrowanie programowe. Są jednak nieświadome istotnych wad tego rozwiązania.

Na czym polega problem z urządzeniami pamięci USB szyfrowanymi programowo? Czy przechowywane i przenoszone dane nie są szyfrowane w systemie AES-256 XTS? Ogólnie rzecz biorąc, są. Problem polega na tym, że szyfrowanie programowe uważa się za „szyfrowanie usuwalne".

W jakim sensie „usuwalne"? Czy to oznacza, że użytkownik pamięci USB szyfrowanej programowo może wyłączyć szyfrowanie?

Odpowiedź brzmi: tak. Użytkownicy mogą usunąć funkcję szyfrowania programowego z pamięci USB. Ale dlaczego mieliby to robić? Ponieważ mogą i chcą uzyskiwać dostęp do plików bez użycia hasła lub po prostu je zapomnieli, ale muszą skorzystać z pamięci USB.

JAK USUNĄĆ FUNKCJĘ SZYFROWANIA PROGRAMOWEGO Z SZYFROWANEJ PAMIĘCI USB

Dla użytkownika, który nie chce tracić czasu na wprowadzanie skomplikowanych haseł dostępu do danych, proces jest prosty:

1. Podłączenie szyfrowanej programowo pamięci do komputera
2. Sformatowanie pamięci
3. Formatowanie powoduje całkowite usunięcie funkcji szyfrowania
4. Skopiowanie plików zawierających tajne lub poufne dane do pamięci w celu uzyskania łatwego dostępu

Użytkownik może łatwo to zrobić na komputerze, który nie jest objęty ograniczeniami. Działy IT ograniczyły możliwość używania poleceń formatowania na komputerach firmowych, ale można to zrobić na każdym innym komputerze nienależącym do firmy.

W kontekście zgodności z przepisami łatwość usunięcia funkcji szyfrowania danych oznacza, że pamięć udostępniona przez firmę staje się nieszyfrowana, chociaż po usunięciu szyfrowania opisaną metodą dane, które zostały zaszyfrowane w pamięci, można uznać za bezpowrotnie utracone (klucze szyfrowania są powiązane z danymi). Wszystkie dane skopiowane na urządzenie po usunięciu funkcji szyfrowania uważa się za niezabezpieczone, co jest potencjalnie niezgodne z przepisami i może być uznane za naruszenie regulacji HIPAA, RODO, CCPA itp.

KONSEKWENCJE UTRATY NIESZYFROWANYCH URZĄDZEŃ PAMIĘCI

W przypadku zgubienia i znalezienia urządzenia pamięci USB należącego do firmy, nawet jeśli początkowo nie była ona tego świadoma i dowiedziała się o tym po fakcie z mediów społecznościowych, zgodnie z przepisami firma musi spełnić specjalne wymagania, które mogą obejmować:

1. Przeprowadzenie dochodzenia kryminalistycznego w celu ustalenia, jakie dane zostały utracone
2. Ustalenie w porozumieniu z działem prawnym, czy doszło do naruszenia prawa
3. Określenie, czy konieczne jest powiadomienie klientów

W takim przypadku utrata pojedynczego urządzenia pamięci USB może stać się bardzo kosztowna. Przy stawkach za usługi prawne przekraczających setki dolarów za godzinę, proces zapewnienia zgodności może skutkować wydatkami rzędu tysięcy dolarów, a także potencjalnymi grzywnami, pozwami klientów i innych podmiotów oraz utratą reputacji wynikającą z ujawnienia danych.

Gdy rozważa się szyfrowanie programowe ze względu na niskie koszty wdrożenia, nie bierze się pod uwagę tego ryzyka i jego poważnych konsekwencji finansowych.

Zezwolenie na korzystanie z nieszyfrowanych urządzeń pamięci USB w sieci firmowej wiąże się z jeszcze jednym niebezpieczeństwem. Powszechnie określa się je mianem „BadUSB". BadUSB to klasa złośliwego oprogramowania, które jest wykorzystywane przez hakerów do naruszania zapór sieciowych i wprowadzania złośliwego oprogramowania do firmowych systemów cyberbezpieczeństwa za pośrednictwem urządzeń pamięci USB.

BadUSB

Po podłączeniu pamięci USB do komputera, kontroler chipsetu komputera rozpoczyna proces uzgadniania z kontrolerem pamięci USB za pośrednictwem oprogramowania układowego. Odbywa się to, zanim system operacyjny, taki jak Windows/macOS/Linux, „zorientuje się", że podłączono pamięć USB. Każda pamięć USB ma oprogramowanie sprzętowe, które działa, gdy jest ona podłączona do portu USB.

Hakerzy odkryli, że mogą wprowadzić złośliwe oprogramowanie za pomocą tego mechanizmu uzgadniania, zastępując oprogramowanie sprzętowe urządzenia pamięci USB innym, złośliwym oprogramowaniem sprzętowym, które wprowadza złośliwe oprogramowanie do docelowego systemu komputerowego, gdy komunikuje się on z pamięcią USB. Standardowa pamięć USB nie ma zabezpieczenia w wewnętrznym oprogramowaniu sprzętowym, którego instrukcje są wykonywane przez kontroler. Stąd wzięła się nazwa BadUSB, ponieważ „dobre" napędy USB zaczęły być wykorzystywane do przenikania przez zapory sieciowe i łamania zabezpieczeń cybernetycznych.

Wiele firm próbuje zakazać używania pamięci USB w swoich systemach, a nawet posuwa się do wypełniania portów USB żywicą epoksydową. Jednak część pracowników musi przenosić dane, korzystając z pamięci USB. Na przykład zarządzający firmą mogą chcieć zabrać ze sobą dane, aby wykorzystać je do pracy lub przekazać zewnętrznym doradcom prawnym lub finansowym, którzy nie mają dostępu do firmowej chmury. Mogą być to również kontrahenci firmy, którzy potrzebują danych do pracy, ale mają ograniczony dostęp do firmowych baz danych, bądź analitycy finansowi, którzy spieszą się, aby ukończyć miesięczne raporty i muszą pracować na arkuszach kalkulacyjnych w domu.

Jak wspomniano wyżej, korzystanie ze standardowej pamięci USB z funkcją szyfrowania programowego wiąże się ze znacznym ryzykiem. Na pierwszy rzut oka rozwiązanie, które wydaje się tańsze, może okazać się potencjalnie bardzo szkodliwe i znacznie droższe. Już sam koszt 2-3-godzinnej konsultacji z prawnikiem w sprawie potencjalnego naruszenia ochrony danych pochłania wszelkie oszczędności uzyskane na tańszym rozwiązaniu.

NAJLEPSZYM SPOSOBEM NA ZAPEWNIENIE ZGODNOŚCI Z PRZEPISAMI JEST WYKORZYSTANIE URZĄDZEŃ PAMIĘCI USB SZYFROWANYCH SPRZĘTOWO

Oto, co sprawia, że pamięć USB szyfrowana sprzętowo to najlepszy wybór w kontekście wymogów regulacyjnych:

1. Pamięć USB szyfrowana sprzętowo ma funkcję szyfrowania, która jest zawsze WŁĄCZONA: użytkownicy nie mają możliwości wyłączenia szyfrowania, zresetowania zasad dotyczących haseł (minimalna długość, złożoność) ani wyłączenia automatycznego ponawiania żądania wpisania hasła. W odróżnieniu od funkcji szyfrowania programowego, które nie zapobiega wielokrotnym próbom odgadnięcia hasła poprzez ataki słownikowe, funkcja szyfrowania sprzętowego ogranicza liczbę prób ponownego wprowadzenia hasła i blokuje dostęp do danych po dziesięciu, a czasem nawet mniejszej liczbie prób wprowadzenia nieprawidłowego hasła. To bardzo bezpieczne rozwiązanie w dobie superkomputerów.
2. Urządzenia pamięci szyfrowanej sprzętowo korzystają z najlepszych kontrolerów szyfrowania i mają wiele funkcji zabezpieczeń: chociaż nie zawsze ujawniamy wszystkie środki zaradcze w dziedzinie bezpieczeństwa, istnieje taki, który chroni przed atakiem przez lukę BadUSB. W zakładzie produkcyjnym, podczas instalacji oprogramowania sprzętowego w urządzeniu pamięci szyfrowanej sprzętowo, oprogramowanie jest podpisywane cyfrowo. Oznacza to, że po podłączeniu takiego szyfrowanego urządzenia USB kontroler szyfrowania najpierw sprawdza integralność oprogramowania sprzętowego za pomocą podpisu cyfrowego i wczytuje je tylko wtedy, gdy przejdzie weryfikację. Każda próba wymiany oprogramowania sprzętowego powoduje uszkodzenie urządzenia pamięci, które przestaje działać i tym samym nie stanowi już zagrożenia.
3. Urządzenia pamięci USB szyfrowane sprzętowo mogą mieć niestandardowe identyfikatory produktu (PID) skonfigurowane dla danej firmy: te urządzenia klasy premium mogą mieć zaprogramowany identyfikator cyfrowy, dzięki czemu po ich podłączeniu do wewnętrznej lub zewnętrznej zapory firmy można je zidentyfikować jako urządzenia należące do danej firmy. Jeśli np. pracownik zgubi firmowe urządzenie pamięci i kupi ten sam model w sklepie, nowo zakupiona pamięć nie zostanie zatwierdzona w sieci firmowej. Taka personalizacja zapewnia dodatkową warstwę bezpieczeństwa podczas korzystania z pamięci USB.
4. Urządzenia pamięci szyfrowanej sprzętowo pozwalają bardzo szybko zaoszczędzić pieniądze: samo zmniejszenie i wyeliminowanie ryzyka sprawia, że cykl zwrotu jest bardzo krótki.

Firma Kingston jest największym na świecie producentem szyfrowanych urządzeń pamięci USB i oferuje rodziny produktów o różnych funkcjach i w różnych przedziałach cenowych. Skontaktuj się bezpośrednio z firmą Kingston, aby dowiedzieć się, w jaki sposób możemy pomóc Ci zachować zgodność z przepisami dzięki rozwiązaniom szyfrowanej pamięci USB dla kadry kierowniczej, pracowników, kontrahentów i nie tylko.