ebook

mwt SOLUTIONS | ManageEngine

CLOUD SECURITY W PRAKTYCE.

Kompleksowa ochrona danych i systemów z ManageEngine

Spis treści

WSTĘP

Chmura to obecnie bardzo popularny temat – wiele firm dąży do migracji swojej infrastruktury do środowiska cloudowego. Wśród zalet można wskazać m.in.:

- Skalowalność,
- Brak własnej infrastruktury,
- Brak problemów sieciowych,
- Wysoka dostępność i redundancja danych.

To niewątpliwe korzyści, które realnie wpływają na efektywność naszej pracy i funkcjonowanie całej organizacji. Jednak, jak to często bywa, z wielkimi możliwościami wiąże się duża odpowiedzialność po stronie producenta. Jako klienci wymagamy najlepszej obsługi oraz bezpieczeństwa naszych danych, dlatego w naszym e-booku przedstawimy wdrożone rozwiązania zapewniające bezpieczeństwo organizacji, oferowane przez firmę ManageEngine oraz Zoho.

Aplikacje

Poznaj aplikacje, które wchodzą w skład chmurowych rozwiązań ManageEngine:

- Analytics Plus Cloud,
- Cloud Security Plus,
- Endpoint Central Cloud,
- Identity360,
- Logs360 Cloud,
- MDM Cloud (Mobile Device Management),
- MSP Central,
- Patch Manager Plus Cloud,
- Remote Access Plus Cloud,
- SaaS Manager Plus,
- ServiceDesk Plus Cloud,
- Site24x7,
- Vulnerability Manager Plus Cloud.

Na chwilę obecną są to wszystkie aplikacje hostowane przez ManageEngine jako rozwiązania chmurowe.

Podstawowe Informacje

Lokalizacja Centrum Danych

Dostawcą chmury, czyli infrastruktury, na której ManageEngine hostuje swoje aplikacje, jest firma Zoho Corporation, która posiada centra danych na całym świecie. Usługa jest więc hostowana w regionie wybranym podczas jej zakładania. Dla klientów z Polski istotny jest obszar europejski, który wymusza przechowywanie danych na terenie Europejskiego Obszaru Gospodarczego (EOG). W przypadku ZOHO główne centrum danych znajduje się w Amsterdamie (Holandia), a zapasowe w Dublinie (Irlandia).

Certyfikaty oraz Zgodności

Korzystanie z infrastruktury chmurowej wiąże się również z koniecznością spełnienia konkretnych wymagań. Poniżej znajdziesz wszystkie certyfikaty, które dotyczą aplikacji chmurowych ManageEngine:

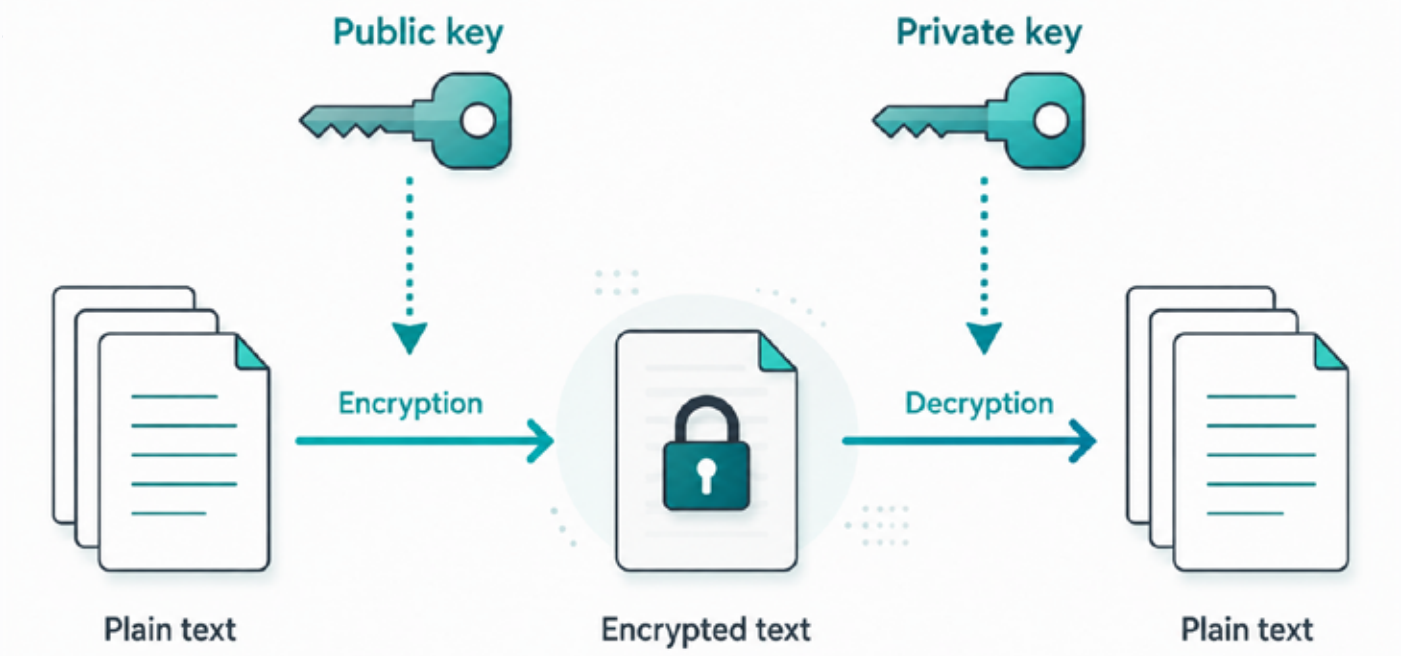
- GDPR
- ISO/IEC 27001
- ISO/IEC 27701
- ISO/IEC 27017
- ISO/IEC 27018
- ISO 9001:2015
- ISO 22301:2019
- ISO 45001
- ISO 50001
- PCI DSS
- SOC 1 Type 1
- SOC 2 Type 2
- SOC 2 + HIPAA
- Cyber Essentials Plus
- TX-RAMP (Texas Risk and Authorization Management Program)
- ESQUEMA NACIONAL DE SEGURIDAD (ENS) – Spain
- CSA STAR Self-Assessment
- CCPA

Bezpieczeństwo Danych

Teoria

Co to jest szyfrowanie danych?

Szyfrowanie to proces zamiany danych w niezrozumiały kod, aby chronić je przed nieautoryzowanym dostępem. Jego głównym celem jest zapewnienie, że tylko upoważniony odbiorca może odczytać wiadomość.



Czym są nasze dane?

Wyróżniamy dwa rodzaje danych:

1. **Dane klienta:** Są to informacje, które użytkownik przechowuje w usługach Zoho lub ManageEngine i które są powiązane z jego kontem.
2. **Dane pochodne**: To dane, których użytkownik nie podaje bezpośrednio, ale które są generowane na podstawie jego danych (np. tokeny uwierzytelniające, unikalne identyfikatory, raporty).

Gdzie wędrują dane?

Szyfrowanie podczas przesyłania chroni Twoje dane, gdy są przesyłane przez Internet, uniemożliwiając atak typu „man-in-the-middle", czyli przechwycenie przez osoby nieupoważnione.

W usługach Zoho/ManageEngine szyfrowanie to jest stosowane w dwóch głównych sytuacjach:

- Gdy dane przemieszczają się z Twojej przeglądarki na serwery Zoho.
- Gdy dane są wysyłane z serwerów Zoho do usług firm trzecich (np. podczas korzystania z integracji).

GDPR

Czym jest RODO (GDPR)?

RODO (Rozporządzenie o Ochronie Danych Osobowych) to unijne prawo, które kompleksowo reguluje sposób, w jaki firmy chronią dane osobowe mieszkańców UE, zapewniając im jednocześnie większą

kontrolę nad udostępnianymi informacjami.

Chociaż RODO to rozporządzenie europejskie, jego zasady mają globalne znaczenie. Dlatego Zoho przyjęło standardy RODO jako **bazowy poziom ochrony dla wszystkich swoich operacji na całym świecie.** Oznacza to, że każdy klient, niezależnie od lokalizacji, jest objęty tymi samymi, wysokimi standardami ochrony danych.

Czym są dane osobowe?

To **wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.** Definicja ta jest bardzo szeroka i wykracza daleko poza imię, nazwisko czy adres e-mail. Obejmuje również takie dane jak:

- Informacje finansowe,
- Dane biometryczne i genetyczne,
- Adres IP i dane lokalizacyjne,
- Poglądy polityczne czy orientacja seksualna.

Kluczowe działania Zoho w zakresie zgodności z RODO

Aby zapewnić pełną zgodność z rozporządzeniem, firma podjęła szereg kompleksowych działań, które można podzielić na kilka kluczowych obszarów:

- **Procesy wewnętrzne i organizacja**

  Szkolenia i budowanie świadomości: W całej organizacji przeprowadzono szkolenia, aby upewnić się, że pracownicy rozumieją zasady RODO i potrafią rozporządzać danymi.

  Ocena ryzyka i inwentaryzacja: Przeprowadzono szczegółowe **oceny skutków dla ochrony danych (DPIA)** oraz stworzono rejestr zasobów informacyjnych, aby precyzyjnie zmapować przepływ danych, cele ich przetwarzania i poziom dostępu w firmie.

  Powołanie ról: Wyznaczono wewnętrznego **Inspektora Ochrony Danych (DPO)** oraz specjalnych „opiekunów prywatności" w poszczególnych zespołach.

- **Produkty i środki techniczne**

  „Privacy by Design": Zasada „prywatności w fazie projektowania" została wdrożona w procesie rozwoju produktów, co dało użytkownikom większą kontrolę nad ich danymi.

  Wzmocnienie bezpieczeństwa: Ulepszono metody zabezpieczeń, m.in. poprzez szyfrowanie danych w spoczynku, w zależności od ich wrażliwości.

  Higiena danych: Przeprowadzono czyszczenie baz danych, usuwając nieaktywne konta i niepotrzebne informacje, aby zagwarantować ich aktualność i minimalizację.

- **Kwestie prawne i współpraca**

  Weryfikacja partnerów: Sprawdzono wszystkich dostawców zewnętrznych, aby upewnić się, że również oni spełniają wymogi RODO.

  Aktualizacja dokumentacji: Zaktualizowano Politykę Prywatności oraz przygotowano zgodną z RODO Umowę Powierzenia Przetwarzania Danych (DPA), dostępną dla klientów na życzenie.

- **Reagowanie na incydenty**

  Polityka powiadomień: Wdrożono jasną politykę reagowania na incydenty, która zakłada **powiadomienie klientów o naruszeniu w ciągu 72 godzin** od momentu jego wykrycia.

Praktyka

Komunikacja klient – serwer

Protokół: TLS (Transport Layer Security) w wersjach 1.2/1.3.

Certyfikaty: Generowane z użyciem SHA 256.

Zestaw szyfrów (Ciphers):

- **Szyfrowanie:** AES_CBC / AES_GCM (klucze 256/128-bit).
- **Uwierzytelnianie wiadomości:** SHA2.
- **Mechanizm wymiany kluczy:** ECDHE_RSA.
- **Dodatkowe zabezpieczenia**: Implementacja Perfect Forward Secrecy (PFS) oraz wymuszanie HSTS (HTTPS Strict Transport Security) na wszystkich witrynach.

Komunikacja serwer – aplikacje firm trzecich

- Protokół podstawowy: HTTPS.
- **Transakcje z danymi wrażliwymi:** Stosowane jest szyfrowanie asymetryczne (system kluczy publicznych i prywatnych).

Zarządzanie kluczami (KMS - Key Management Service):

- Pary kluczy są generowane i zarządzane w KMS.
- Wygenerowane pary kluczy są szyfrowane za pomocą klucza głównego (master key) i przechowywane w KMS.
- Klucz główny jest przechowywany na osobnym serwerze.

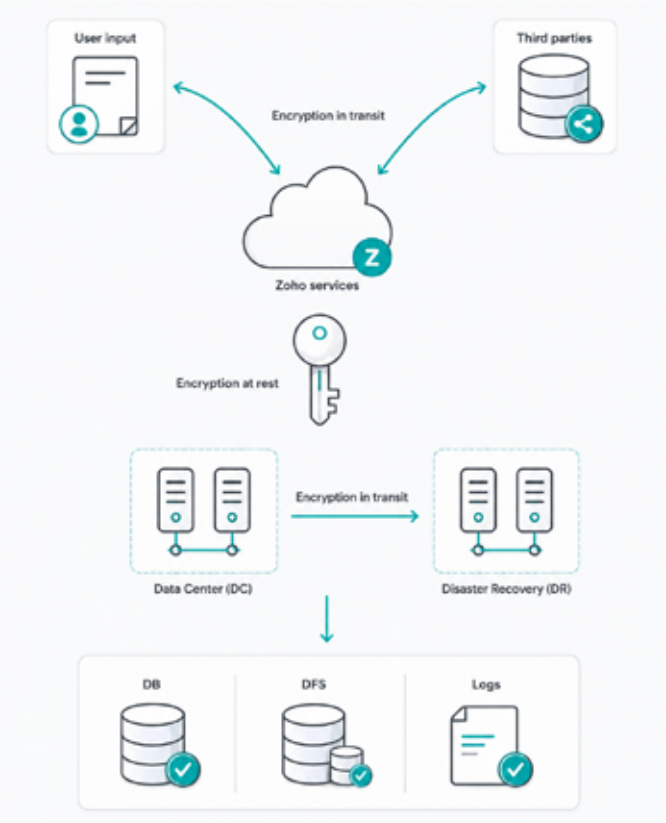
Proces komunikacji:

- Klucze publiczne są udostępniane stronom trzecim przez certyfikaty.
- Klucz prywatny jest bezpiecznie przechowywany w KMS.
- Deszyfrowanie danych odbywa się w KMS po pomyślnym uwierzytelnieniu.

Szyfrowanie danych w spoczynku (Encryption at Rest)

Stosowane są dwa główne poziomy szyfrowania: na poziomie aplikacji oraz sprzętowe szyfrowanie całego dysku. Poniższy opis koncentruje się na strategii szyfrowania na poziomie aplikacji, która zależy od sposobu przechowywania danych:

- **Bazy danych (DB): dane w tabelach,**
- **Rozproszony system plików (DFS): dane w plikach,**
- **Adresy URL,**
- **Kopie zapasowe (Backup),**
- **Logi,**
- **Pamięć podręczna (Cache).**



Szyfrowanie na poziomie aplikacji

Każda usługa Zoho/ManageEngine przetwarza dane użytkownika w formie plików lub pól, które są szyfrowane w odmienny sposób. Ta sekcja opisuje szyfrowanie danych w spoczynku na poziomie aplikacji.

Szyfrowanie na poziomie pola (Field Level Encryption)

Wrażliwe dane wprowadzane do aplikacji są przechowywane w bazach danych i szyfrowane zgodnie ze standardem AES 256 w trybie AES/CBC/PKCS5Padding. Szyfrowanie odbywa się w warstwie aplikacji, co oznacza, że bezpośredni dostęp do bazy danych (np. przez SQL) ujawnia jedynie zaszyfrowane dane. Dostęp do kluczy jest zarządzany przez KMS (Key Management Service).

Rodzaje szyfrowania w zależności od wrażliwości danych

- **Typ 1 (Domyślny):** Każda organizacja otrzymuje dedykowany klucz w KMS, którym szyfrowane są jej dane. Klucz ten jest następnie szyfrowany kluczem głównym (master key) i trzymany na osobnym serwerze.
- **Typ 2 (Dla danych wrażliwych i PII):** Stosowany dla danych takich jak numery kont bankowych czy dane biometryczne. W tym modelu KMS generuje unikalny klucz dla każdej kolumny w tabeli bazy danych.

Rodzaje szyfrowania w zależności od funkcjonalności wyszukiwania

- Funkcjonalność wyszukiwania w zaszyfrowanych danych zależy od użytego wektora inicjującego (IV) – losowej wartości, która zapewnia, że ten sam tekst jawny za każdym razem generuje inny szyfrogram.
- Szyfrowanie z zachowaniem równości (Equality Preserving): Używany jest tylko jeden IV na klucz. Oznacza to, że ten sam tekst jawny zawsze generuje ten sam szyfrogram, co umożliwia przeszukiwanie zaszyfrowanych danych (np. po adresie e-mail). Jest to wariant stosowany zazwyczaj z szyfrowaniem Typu 1.
- Szyfrowanie standardowe: Każdy wpis danych otrzymuje unikalny, losowy wektor inicjujący IV. Uniemożliwia to wyszukiwanie, ale oferuje wyższy poziom bezpieczeństwa, ponieważ identyczne dane wejściowe generują różne szyfrogramy. Zazwyczaj stosowane z szyfrowaniem Typu 2.

Szyfrowanie plików

Pliki przechowywane w rozproszonym systemie plików (DFS) są szyfrowane na poziomie aplikacji przy użyciu standardu AES 256 w trybie CTR lub GCM. Preferowany jest tryb GCM, ponieważ oprócz szyfrowania zapewnia również uwierzytelnianie i integralność danych za pomocą kryptograficznej sumy kontrolnej.

- **Typ 1:** Każda organizacja otrzymuje jeden klucz. Każdy plik jest szyfrowany tym kluczem, ale z unikalnym, losowym wektorem inicjującym IV przechowywanym razem z plikiem.
- **Typ 2:** Każdy plik otrzymuje unikalny klucz szyfrujący. Klucz ten jest następnie szyfrowany za pomocą dedykowanego klucza KEK (Key Encryption Key), unikalnego dla danej organizacji i zarządzanego przez KMS.

Pozostałe obszary szyfrowania

- **Szyfrowanie URL:** Wrażliwe fragmenty adresów URL (np. identyfikatory dokumentów) są szyfrowane. Stosowany jest model jednego klucza na organizację lub jednego klucza na daną funkcję.
- **Szyfrowanie kopii zapasowych:** Wszystkie dane w kopiach zapasowych są szyfrowane w spoczynku przy użyciu tych samych standardów co dane produkcyjne.
- **Szyfrowanie logów:** Logi przechowywane w HDFS (Hadoop Distributed File System) są szyfrowane przy użyciu natywnej technologii Hadoop, podczas gdy zarządzanie kluczami odbywa się przez KMS.
- **Szyfrowanie pamięci podręcznej (Cache):** Dane w pamięci podręcznej (Redis), które zawierają wrażliwe informacje osobiste, podlegają szyfrowaniu.

Zarządzanie kluczami (Key Management)

Operacje na kluczach kryptograficznych realizowane są przez autorską usługę KMS (Key Management Service). W procesie szyfrowania wykorzystywana jest hierarchiczna struktura kluczy:

- **Klucz szyfrujący dane (DEK – Data Encryption Key):** Bezpośrednio używany do szyfrowania i deszyfrowania danych (konwersji tekstu jawnego na szyfrogram).
- **Klucz szyfrujący klucze (KEK – Key Encryption Key):** Używany do szyfrowania kluczy DEK, co stanowi dodatkową warstwę zabezpieczeń. Jest generowany na osobnym serwerze i domyślnie jest indywidualnie dopasowany do danej usługi Zoho.
- **Klucz główny (Master Key):** Używany do szyfrowania kluczy KEK. Ze względów bezpieczeństwa jest przechowywany na całkowicie odizolowanym serwerze.

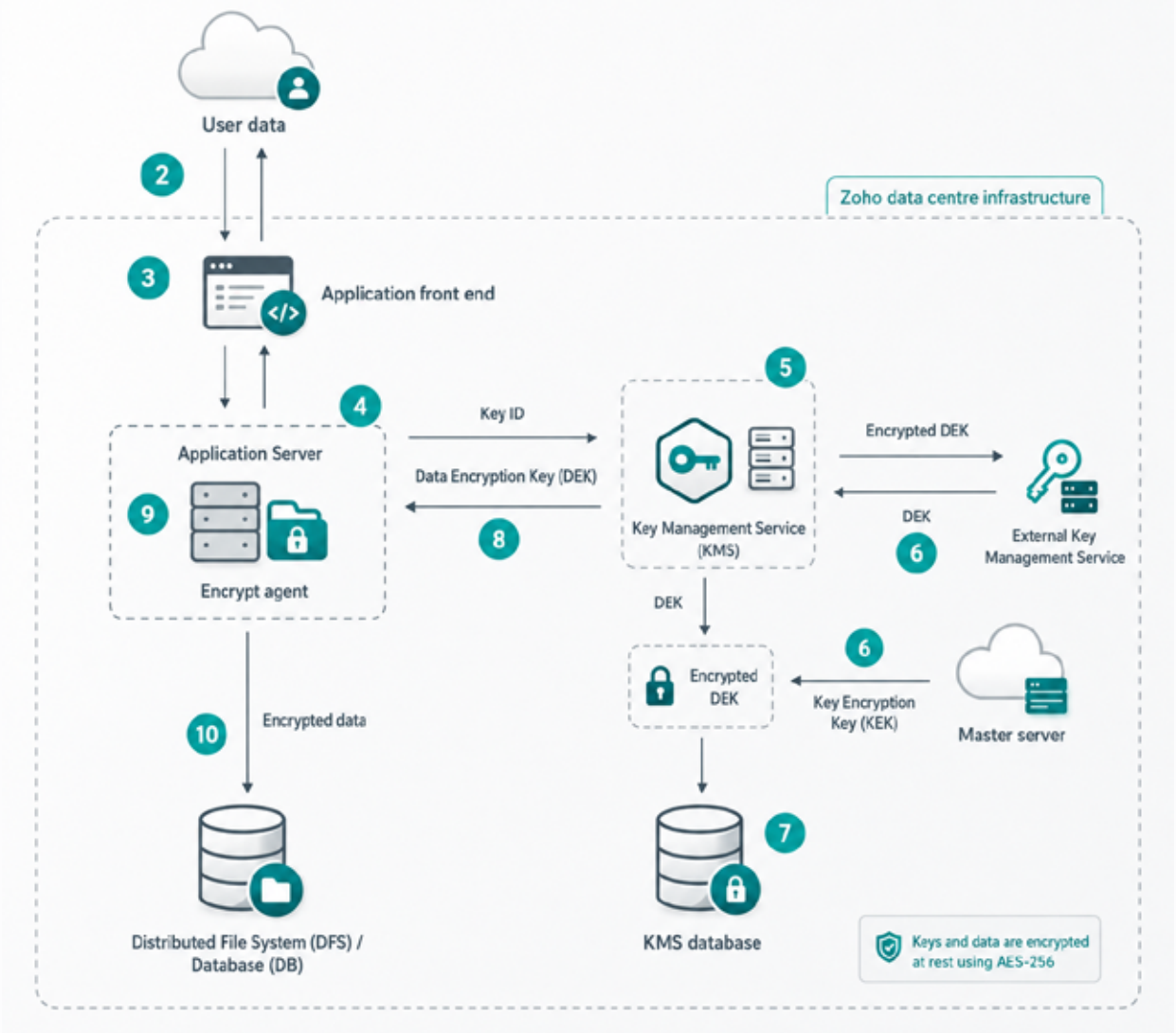
Domyślnie Zoho zarządza całym cyklem życia kluczy. Alternatywnie, klienci mogą skorzystać z funkcji Bring Your Own Key (BYOK), aby używać własnych kluczy KEK, zarządzanych w zewnętrznych usługach lub dostarczonych manualnie.

Jak działa KMS?

Wszystkie operacje szyfrowania opierają się na algorytmie AES 256. Proces wykorzystuje technikę „envelope encryption", która przebiega następująco:

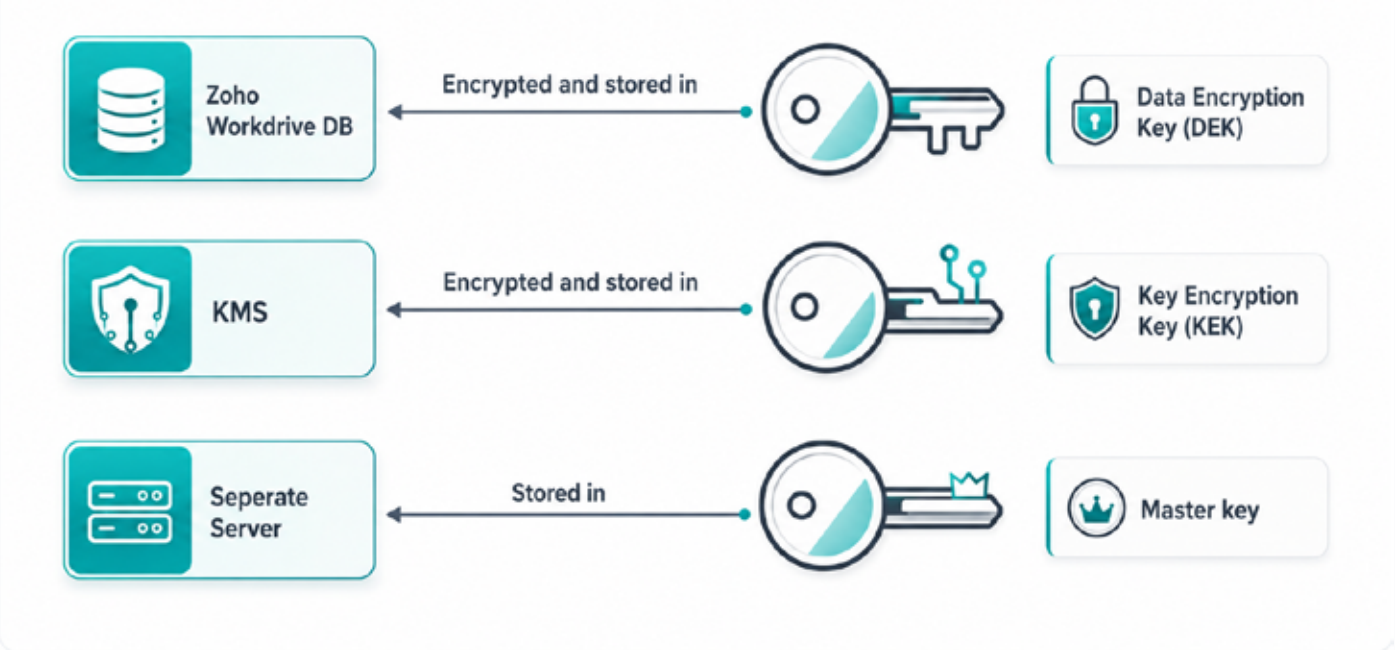
1. Dane (w bazie lub pliku) są szyfrowane za pomocą klucza DEK.
2. Klucz DEK jest następnie szyfrowany za pomocą klucza KEK.
3. W fazie końcowej klucz KEK jest szyfrowany za pomocą klucza głównego.

To podejście zapewnia, że dostęp do zaszyfrowanych danych wymaga hierarchicznego odblokowania kolejnych kluczy.



Generowanie i przechowywanie kluczy

- KMS generuje 256-bitowe klucze (zgodne z AES 256) wraz z wektorem inicjującym (IV) przy użyciu biblioteki Java Security i generatora SecureRandom.
- Zaszyfrowane klucze DEK są przechowywane w bazie danych KMS. Klucz główny jest fizycznie odseparowany i znajduje się na innym, bezpiecznym serwerze, co uniemożliwia jednoczesne przejęcie wszystkich kluczy przez atakującego.

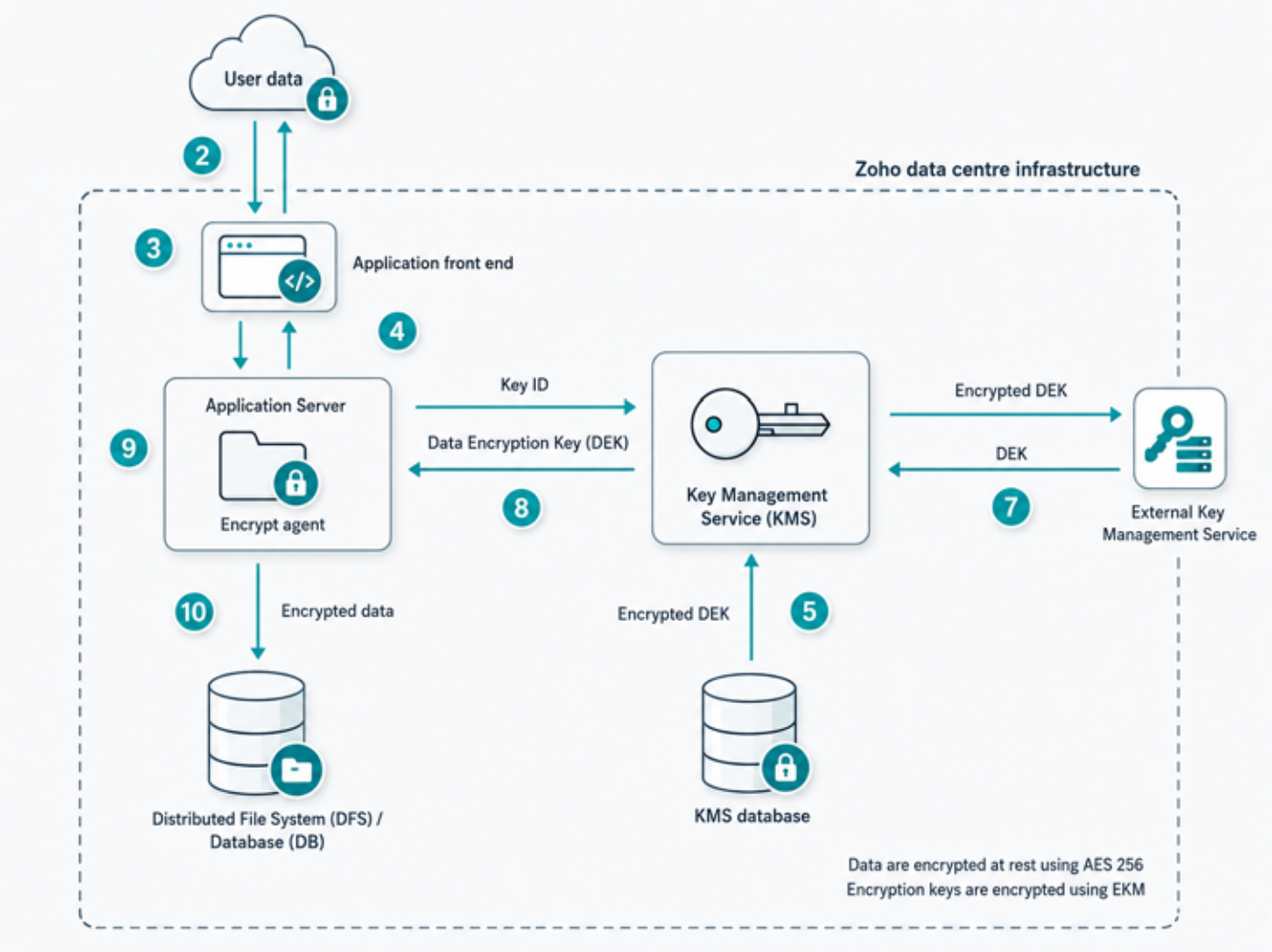


Bezpieczeństwo kluczy

- **Kontrola dostępu:** Dostęp do kluczy jest ściśle regulowany przez listy kontroli dostępu (ACL), które pozwalają tylko wybranym usługom na korzystanie z określonych kluczy. Każdy dostęp jest uwierzytelniany i logowany, a logi podlegają regularnym audytom. Dostęp dla personelu Zoho jest limitowany i wymaga zatwierdzenia przez zarząd.
- **Rotacja kluczy:** Klucz główny podlega rotacji. Wymiana polega na deszyfracji wszystkich kluczy KEK starym kluczem głównym i ponownym zaszyfrowaniu ich nowym. Obecnie proces ten jest uruchamiany w przypadku kompromitacji klucza.
- **Dostępność kluczy:** Infrastruktura kluczy jest replikowana w centrach danych (master, slave, secondary slave), co gwarantuje wysoką dostępność (High Availability) w przypadku awarii głównego ośrodka.

Bring Your Own Key (BYOK)

- Funkcja BYOK pozwala organizacjom na przejęcie pełnej kontroli nad własnymi kluczami szyfrującymi (KEK), zamiast polegać na kluczach generowanych przez Zoho. Daje to możliwość samodzielnego zarządzania dostępem do danych i ich deszyfracją.
- BYOK można skonfigurować przez Zoho Directory, dodając klucz z zewnętrznego menedżera kluczy (EKM) lub wgrywając go manualnie. Obecnie wspierane są następujące usługi EKM:
  - AWS KMS,
  - Google KMS,
  - Thales CTM,
  - Fortanix DSM.



Szyfrowanie Warstwy Fizycznej (Full-Disk Encryption)

Do realizacji sprzętowego szyfrowania całego dysku wykorzystywane są dyski samoszyfrujące (SED – Self-Encrypting Drives). Są to dyski HDD lub SSD z wbudowanym układem kryptograficznym, który automatycznie szyfruje wszystkie zapisywane dane i deszyfruje je podczas odczytu.

Zasada działania i zarządzanie kluczami

Proces opiera się na dwóch rodzajach kluczy:

1. **Klucz szyfrujący dane (DEK – Data Encryption Key):** Jest przechowywany bezpośrednio na dysku i służy do szyfrowania danych. Domyślny klucz producenta jest przez nas regenerowany podczas konfiguracji serwera, aby zachować wysokie standardy bezpieczeństwa.
2. **Klucz uwierzytelniający (AK –Authentication Key):** Służy do szyfrowania klucza DEK oraz do blokowania/odblokowywania całego dysku, stanowiąc dodatkową warstwę zabezpieczeń. Klucze AK są zarządzane przez lokalny system zarządzania kluczami (LKMS).

W przypadku kradzieży lub nieautoryzowanego dostępu fizycznego do dysku, dane pozostają niedostępne, ponieważ bez klucza AK, który jest przechowywany osobno, nie można odszyfrować klucza DEK.

Bezpieczeństwo Organizacyjne

Bezpieczeństwo w Zoho opiera się na formalnym Systemie Zarządzania Bezpieczeństwem Informacji (SZBI/ISMS), który definiuje cele, ryzyka i metody ich ograniczania. System ten jest realizowany poprzez rygorystyczne polityki i procedury, które gwarantują bezpieczeństwo, dostępność, integralność i poufność danych klientów.

Poniżej znajdują się 4 kluczowe filary systemu bezpieczeństwa:

1. **Personel i Kultura Bezpieczeństwa**

   Weryfikacja pracowników: Każdy pracownik przed rozpoczęciem pracy przechodzi szczegółową weryfikację przeszłości (niekaralność, historia zatrudnienia, wykształcenie), przeprowadzaną przez zewnętrzne, wyspecjalizowane agencje. Do czasu pozytywnego wyniku weryfikacji pracownik nie otrzymuje dostępu do wrażliwych systemów.

   Szkolenia i budowanie świadomości: Proces wdrażania nowego pracownika obejmuje podpisanie umowy o poufności oraz szkolenia z zakresu bezpieczeństwa informacji i prywatności. Wiedza jest regularnie weryfikowana, a programy edukacyjne są kontynuowane przez cały okres zatrudnienia poprzez wewnętrzne platformy i wydarzenia, aby zapewnić, że wszyscy są na bieżąco z najlepszymi praktykami.

2. **Dedykowane Zespoły ds. Bezpieczeństwa i Prywatności**

   Firma utrzymuje wyspecjalizowane zespoły, których zadaniem jest wdrażanie i zarządzanie programami bezpieczeństwa. Odpowiadają one za projektowanie systemów obronnych, stałe monitorowanie sieci w poszukiwaniu zagrożeń oraz doradztwo dla zespołów inżynieryjnych w trakcie tworzenia produktów.

3. **Audyt Wewnętrzny i Zgodność (Compliance)**

   Odrębny zespół ds. zgodności dba o to, by wewnętrzne procedury i polityki były zgodne z międzynarodowymi standardami i regulacjami. Zespół ten przeprowadza okresowe audyty wewnętrzne oraz koordynuje niezależne audyty realizowane przez firmy zewnętrzne.

4. **Bezpieczeństwo Punktów Końcowych (Endpoint Security)**

   Wszystkie urządzenia wykorzystywane przez pracowników podlegają ścisłym zasadom bezpieczeństwa:

   Stacje robocze: Każdy komputer ma zainstalowane aktualne oprogramowanie, system antywirusowy i jest centralnie zarządzany przez rozwiązania do monitorowania punktów końcowych.

   Domyślne zabezpieczenia: Urządzenia są domyślnie skonfigurowane tak, aby wymuszać szyfrowanie dysku, stosowanie silnych haseł oraz automatyczną blokadę ekranu po okresie bezczynności.

   Urządzenia mobilne: Telefony i tablety używane do celów służbowych są zarejestrowane w systemie MDM (Mobile Device Management), który egzekwuje firmowe standardy bezpieczeństwa.

Bezpieczeństwo Infrastruktury

Ochrona infrastruktury opiera się na wielowarstwowym podejściu, łączącym zaawansowane technologie sieciowe, redundancję sprzętową oraz proaktywne monitorowanie zagrożeń.

Bezpieczeństwo Sieci

Architektura sieciowa została zaprojektowana z myślą o głębokiej ochronie. Kluczowe elementy to:

Segmentacja: Środowiska produkcyjne (gdzie działają usługi i przechowywane są dane klientów) są krytycznie odseparowane sieciowo od środowisk testowych i deweloperskich.

Zapory sieciowe (Firewalls): Cały ruch jest filtrowany, aby zapobiegać nieautoryzowanemu dostępowi. Konfiguracja zapór jest codziennie weryfikowana przez inżynierów sieci.

Ciągłe monitorowanie: Dedykowany zespół Network Operations Center (NOC) przez całą dobę monitoruje infrastrukturę i aplikacje pod kątem wszelkich anomalii lub podejrzanych aktywności, wykorzystując do tego autorskie, zaawansowane narzędzia.

Redundancja i Odporność na Awarie

Platforma została zbudowana w architekturze rozproszonej, co zapewnia wysoką dostępność usług. Oznacza to, że awaria pojedynczego serwera nie wpływa na działanie systemu ani na dostęp użytkowników do ich danych. Redundancja obejmuje również kluczowe komponenty sieciowe (takie jak przełączniki, routery i bramy bezpieczeństwa), co eliminuje ryzyko tzw. pojedynczych punktów awarii (Single Points of Failure).

Ochrona przed Atakami DDoS

W celu ochrony przed atakami typu DDoS (Distributed Denial of Service), wykorzystywane są technologie od wiodących, wyspecjalizowanych dostawców. Systemy te precyzyjnie filtrują złośliwy ruch, jednocześnie gwarantując swobodny przepływ legalnym użytkownikom, co zapewnia ciągłość działania i wysoką wydajność usług.

Utwardzanie (Hardening) Systemów

Wszystkie serwery przechodzą rygorystyczny proces utwardzania, zanim zostaną włączone do środowiska produkcyjnego. Proces ten polega m.in. na wyłączaniu wszystkich zbędnych portów i usług, usuwaniu domyślnych kont oraz wzmacnianiu konfiguracji. Proces ten jest zautomatyzowany i wbudowany w bazowy obraz systemu operacyjnego (OS), co gwarantuje spójność i wysoki standard bezpieczeństwa każdej maszyny.

Wykrywanie i Zapobieganie Włamaniom (IDS/IPS)

Stosowany jest wielopoziomowy system wykrywania intruzów:

- **Poziom serwera i sieci:** System monitoruje sygnały z pojedynczych urządzeń oraz analizuje ruch w całej sieci. Wszelkie czynności administracyjne i użycie uprzywilejowanych poleceń są szczegółowo logowane.
- **Analiza zagrożeń:** Zaawansowane reguły i mechanizmy uczenia maszynowego analizują zebrane dane, ostrzegając inżynierów bezpieczeństwa o potencjalnych incydentach.
- **Poziom aplikacji:** Działa autorska zapora WAF (Web Application Firewall), która filtruje ruch na podstawie zdefiniowanych reguł bezpieczeństwa.
- **Poziom dostawcy internetu (ISP):** Stosowana jest dodatkowa warstwa zabezpieczeń (obejmująca m.in. filtrowanie i ograniczanie ruchu), która chroni przed atakami na różnych warstwach sieci.

Bezpieczeństwo Operacyjne

Rejestrowanie (Logging) i Monitorowanie

Systemy stale monitorują i analizują informacje z usług, wewnętrzny ruch sieciowy oraz aktywność na urządzeniach – zdarzenia te są rejestrowane w formie różnych logów (np. zdarzeń audytowych, nagłych błędów i działań administracyjnych). Logi są automatycznie analizowane w celu wykrywania anomalii, takich jak nietypowa aktywność na kontach pracowników czy próby dostępu do danych klientów.

Aby zapewnić integralność i dostępność, logi są przechowywane na bezpiecznych, izolowanych serwerach i chronione przed manipulacją. Klienci mają również dostęp do szczegółowych logów audytowych operacji (jak aktualizacje czy usuwanie) wykonywanych na ich danych.

Zarządzanie Podatnościami

Firma stosuje dedykowany proces zarządzania podatnościami, który obejmuje aktywne skanowanie systemów przy użyciu narzędzi własnych i zewnętrznych oraz regularne testy penetracyjne. Zespół bezpieczeństwa proaktywnie monitoruje również publiczne źródła informujące o zagrożeniach.

Każda zidentyfikowana podatność jest natychmiast rejestrowana, otrzymuje priorytet w zależności od jej wagi, a następnie jest śledzona aż do pełnego załatania lub wdrożenia odpowiednich środków zaradczych.

Ochrona przed Złośliwym Oprogramowaniem i Spamem

Wszystkie pliki przesyłane przez użytkowników są automatycznie skanowane przez autorski system antymalware. Silnik ten jest regularnie aktualizowany o nowe sygnatury zagrożeń i wykorzystuje techniki uczenia maszynowego (ML) do ochrony danych.

W celu zapobiegania spamowi, usługi wspierają standard DMARC (oparty na SPF i DKIM). Ponadto, dedykowany zespół antyspamowy, wspierany przez własne silniki detekcji, monitoruje systemy pod kątem nadużyć (np. phishingu) i reaguje na zgłoszenia.

Kopie Zapasowe (Backup)

Wykonywane są codzienne kopie przyrostowe oraz cotygodniowe pełne kopie zapasowe baz danych. Dane te są szyfrowane (AES-256) i przechowywane na serwerach wykorzystujących macierze RAID, co zapewnia ich bezpieczeństwo i redundancję.

Kopie są przechowywane przez okres trzech miesięcy, a klienci mogą w tym czasie wnioskować o odzyskanie danych. Proces ich tworzenia jest automatycznie monitorowany i walidowany pod kątem integralności. Zoho zaleca również klientom regularne eksportowanie i tworzenie własnych, lokalnych kopii zapasowych.

Odtwarzanie po Awarii i Ciągłość Działania

Dane aplikacji są replikowane w czasie niemal rzeczywistym pomiędzy głównym a zapasowym centrum danych (DC). W przypadku awarii głównego ośrodka, zapasowe centrum natychmiast przejmuje jego funkcje, zapewniając ciągłość usług przy minimalnej przerwie w działaniu.

Oba centra posiadają redundantne łącza internetowe (wielu dostawców ISP) oraz pełne zabezpieczenia fizyczne (zasilanie awaryjne, kontrola klimatu, systemy przeciwpożarowe). Firma posiada sformalizowany plan ciągłości działania (BCP), którego skuteczność jest okresowo weryfikowana poprzez testy odtwarzania po awarii

Zarządzanie Incydentami

Firma posiada dedykowany zespół ds. zarządzania incydentami, który odpowiada za kompleksową obsługę zdarzeń bezpieczeństwa.

Zgłaszanie i Reagowanie

Klienci mogą zgłaszać wszelkie incydenty związane z bezpieczeństwem lub prywatnością na dedykowany adres e-mail incidents@zohocorp.com. Zgłoszenia te są zawsze traktowane z najwyższym priorytetem.

W przypadku wykrycia incydentu wewnętrznie:

- Powiadamiamy klientów, których dotyczy zdarzenie, przekazując jednocześnie zalecenia dotyczące ewentualnych działań, jakie powinni podjąć.
- Każdy incydent jest monitorowany aż do pełnego rozwiązania, łącznie z wdrożeniem działań naprawczych oraz mechanizmów zapobiegających powtórzeniu się podobnej sytuacji w przyszłości.
- W stosownych przypadkach identyfikujemy i zabezpieczamy niezbędne dowody (np. logi systemowe) dotyczące zdarzenia.
- Sposób powiadamiania jest dostosowany do skali incydentu: zdarzenia ogólne są komunikowane publicznie (blogi, fora), natomiast incydenty dotyczące konkretnej organizacji są zgłaszane bezpośrednio na zarejestrowany adres e-mail jej administratora.

Powiadomienia o Naruszeniu Ochrony Danych

Procedury powiadamiania są ściśle dostosowane do obowiązujących przepisów prawa (takich jak RODO) i zależą od roli firmy:

Działając jako administrator danych, powiadamiamy odpowiedni organ nadzoru (np. Prezesa UODO) o

naruszeniu w wymaganym prawnie terminie.

Działając jako podmiot przetwarzający (procesor), bezzwłocznie informujemy o naruszeniu administratora danych (czyli klienta), którego dotyczy zdarzenie.

Odpowiedzialne Ujawnianie Podatności (Responsible Disclosure)

Prowadzimy program „Bug Bounty", który ma na celu aktywne angażowanie społeczności badaczy bezpieczeństwa. W ramach tego programu doceniamy i nagradzamy pracę osób, które pomagają nam identyfikować potencjalne luki.

Zobowiązujemy się do ścisłej współpracy ze społecznością w celu weryfikacji, reprodukcji i wdrożenia odpowiednich rozwiązań dla zgłoszonych podatności.

Jeśli znalazłeś lukę w bezpieczeństwie, możesz ją zgłosić na dwa sposoby:

1. Poprzez naszą oficjalną platformę programu: https://bugbounty.zohocorp.com/
2. Bezpośrednio do naszego zespołu bezpieczeństwa na adres e-mail: security@zohocorp.com

Bibliografia

Security Whitepaper - Zoho

Compliance at Zoho

Encryption at Zoho

Zoho - Anti Spam Policy

EU ManageEngine On-Demand Service Status

Zoho security Frequently Asked Questions (FAQ)