ebook

mwt SOLUTIONS | ManageEngine

CLOUD SECURITY V PRAXI

Komplexní ochrana dat a systémů s ManageEngine

e-book

MWT Solutions | ManageEngine

Cloud Security v praxi

Komplexní ochrana dat a systémů s ManageEngine

Obsah

Úvod

Cloud je dnes velmi populární téma — mnoho společností směřuje k migraci své infrastruktury do cloudového prostředí. Mezi výhody, které můžeme zmínit, patří:

- Škálovatelnost,
- Žádná potřeba vlastní infrastruktury,
- Žádné problémy související se sítí,
- Vysoká dostupnost a redundance dat.

Jde o nesporné výhody, které mají reálný dopad na efektivitu naší práce a fungování celé organizace. Jak už to ale bývá, s velkými možnostmi přichází na straně poskytovatele i velká odpovědnost. Jako zákazníci očekáváme nejlepší službu a nejlepší ochranu našich dat, a proto v tomto e-booku představujeme řešení implementovaná společnostmi ManageEngine a Zoho, která zajišťují bezpečnost organizace.

Aplikace

Objevte aplikace, které tvoří cloudová řešení 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.

V současné době se jedná o všechny aplikace, které ManageEngine hostuje jako cloudová řešení.

Základní informace

Umístění data centra

Poskytovatelem cloudu — tedy infrastruktury, na které ManageEngine hostuje své aplikace — je společnost Zoho Corporation, která provozuje data centra po celém světě. Služba je proto hostována v regionu zvoleném při jejím nastavení. Pro zákazníky z Polska je relevantním regionem Evropa, což vyžaduje uchovávání dat v rámci Evropského hospodářského prostoru (EHP). Hlavní data centrum společnosti ZOHO se nachází v Amsterdamu (Nizozemsko), se sekundárním (záložním) centrem v Dublinu (Irsko).

Certifikace a compliance

Používání cloudové infrastruktury s sebou také přináší nutnost splnit specifické požadavky. Níže naleznete všechny certifikace, které se vztahují na cloudové aplikace 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) – Španělsko
- CSA STAR Self-Assessment
- CCPA

Zabezpečení dat

Teorie

Co je šifrování dat?

Šifrování je proces převodu dat do nečitelného kódu za účelem jejich ochrany před neoprávněným přístupem. Jeho hlavním účelem je zajistit, aby zprávu mohl přečíst pouze oprávněný příjemce.

Šifrování využívá algoritmus (veřejně známou metodu, např. AES 256) a tajný klíč, který je potřeba jak k zašifrování dat, tak k jejich opětovnému přečtení (což nazýváme dešifrováním).

Bez správného klíče jsou zachycená data (tzv. šifrovaný text) zcela nepoužitelná a nesrozumitelná, což zaručuje jejich bezpečnost.

Co jsou naše data?

Rozlišujeme dva typy dat:

1. Data zákazníka: Jedná se o informace, které uživatel ukládá ve službách Zoho nebo ManageEngine a které jsou spojeny s jeho účtem.
2. Odvozená data: Jedná se o data, která uživatel neposkytuje přímo, ale která jsou generována na základě jeho dat (např. autentizační tokeny, jedinečné identifikátory, reporty).

Kam data putují?

Šifrování při přenosu chrání vaše data během jejich přenosu přes internet a zabraňuje útoku typu „man-in-the-middle", tedy zachycení dat neoprávněnými stranami.

Ve službách Zoho/ManageEngine se toto šifrování používá ve dvou hlavních situacích:

- Když data putují z vašeho prohlížeče na servery Zoho.
- Když jsou data odesílána ze serverů Zoho ke službám třetích stran (např. během integrací).

GDPR

Co je GDPR?

GDPR (obecné nařízení o ochraně osobních údajů) je legislativa EU, která komplexně upravuje způsob, jakým společnosti chrání osobní údaje obyvatel EU, a zároveň jim dává větší kontrolu nad informacemi, které sdílejí.

Ačkoli je GDPR evropské nařízení, jeho zásady mají globální význam. Proto společnost Zoho přijala standardy GDPR jako základní úroveň ochrany pro veškerý svůj provoz po celém světě. To znamená, že na každého zákazníka, bez ohledu na jeho lokalitu, se vztahují stejné vysoké standardy ochrany dat.

Co jsou osobní údaje?

Jedná se o veškeré informace týkající se identifikované nebo identifikovatelné fyzické osoby. Tato definice je velmi široká a zahrnuje mnohem více než jen jméno nebo e-mailovou adresu. Zahrnuje také data jako:

- Finanční informace,
- Biometrické a genetické údaje,
- IP adresa a údaje o poloze,
- Politické názory nebo sexuální orientace.

Klíčové kroky Zoho pro zajištění souladu s GDPR

Za účelem zajištění plného souladu s nařízením přijala společnost řadu komplexních opatření, která lze rozdělit do několika klíčových oblastí:

- Interní procesy a organizace
    - Školení a budování povědomí: V celé organizaci proběhla školení, aby zaměstnanci rozuměli zásadám GDPR a věděli, jak nakládat s daty.
    - Hodnocení rizik a inventarizace: Byla provedena podrobná posouzení vlivu na ochranu osobních údajů (DPIA) a byl vytvořen registr informačních aktiv, který přesně mapuje toky dat, účely zpracování a úrovně přístupu v rámci společnosti.
    - Jmenování rolí: Byl jmenován interní pověřenec pro ochranu osobních údajů (DPO) a v jednotlivých týmech byli určeni specializovaní „garanti ochrany soukromí" (privacy champions).
- Produkty a technická opatření
    - „Privacy by Design": Zásada „privacy by design" (ochrana soukromí již od návrhu) byla zavedena do procesu vývoje produktů, což uživatelům dává větší kontrolu nad jejich daty.
    - Posílení zabezpečení: Byly vylepšeny bezpečnostní metody, mimo jiné prostřednictvím šifrování uložených dat v závislosti na jejich citlivosti.
    - Datová hygiena: Databáze byly vyčištěny, byly odstraněny neaktivní účty a nepotřebné informace, aby byla zajištěna jejich přesnost a minimalizace dat.
- Právní záležitosti a spolupráce
    - Ověřování partnerů: U všech externích dodavatelů bylo ověřeno, že rovněž splňují požadavky GDPR.
    - Aktualizace dokumentace: Byly aktualizovány zásady ochrany osobních údajů a byla připravena smlouva o zpracování údajů (DPA) v souladu s GDPR, dostupná zákazníkům na vyžádání.
- Reakce na incidenty
    - Zásady oznamování: Byla zavedena jasná politika reakce na incidenty, která vyžaduje informování zákazníků o narušení bezpečnosti do 72 hodin od jeho zjištění.

Praxe

Komunikace klient – server

Protokol: TLS (Transport Layer Security) verze 1.2/1.3.

Certifikáty: Generovány pomocí SHA 256.

Sada šifer (cipher suite):

- **Šifrování:** AES_CBC / AES_GCM (256/128bitové klíče).
- **Autentizace zpráv:** SHA2.
- **Mechanismus výměny klíčů**: ECDHE_RSA.
- **Další ochranná opatření:** Implementace Perfect Forward Secrecy (PFS) a vynucení HSTS (HTTP Strict Transport Security) na všech stránkách.

Komunikace server – aplikace třetích stran

- Základní protokol: HTTPS.
- Transakce zahrnující citlivá data: Používá se asymetrické šifrování (systém veřejného/soukromého klíče).

Správa klíčů (KMS – Key Management Service):

- Páry klíčů jsou generovány a spravovány v KMS.
- Vygenerované páry klíčů jsou zašifrovány pomocí master key a uloženy v KMS.
- Master key je uložen na samostatném serveru.

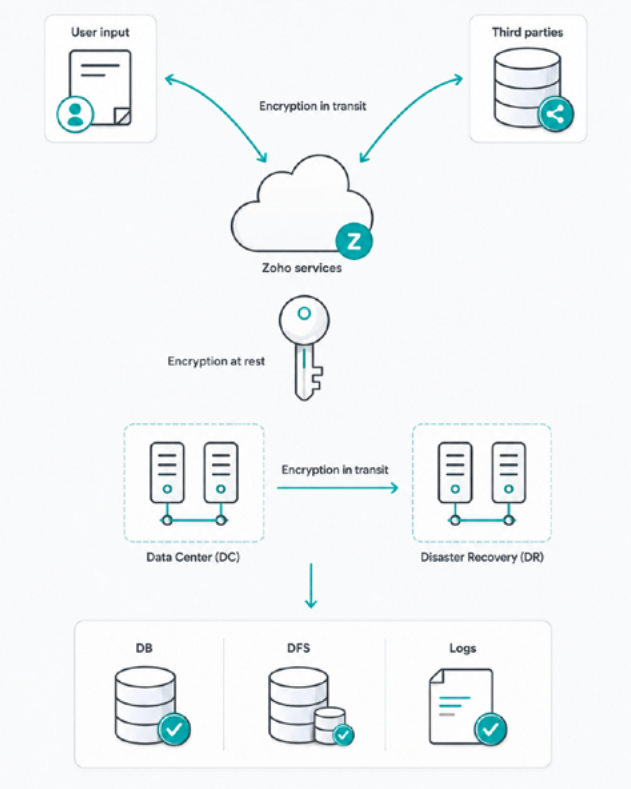
Proces komunikace:

- Veřejné klíče jsou sdíleny s třetími stranami prostřednictvím certifikátů.
- Soukromý klíč je bezpečně uložen v KMS.
- K dešifrování dat dochází v KMS po úspěšné autentizaci.

Šifrování uložených dat

Používají se dvě hlavní úrovně šifrování: šifrování na úrovni aplikace a hardwarové šifrování celého disku. Následující popis se zaměřuje na strategii šifrování na úrovni aplikace, která závisí na způsobu ukládání dat:

- **Databáze (DB): data v tabulkách,**
- **Distribuovaný souborový systém (DFS): data v souborech,**
- **URL adresy,**
- **Zálohy,**
- **Logy,**
- **Cache.**



Šifrování na úrovni aplikace

Každá služba Zoho/ManageEngine zpracovává uživatelská data ve formě souborů nebo polí, která jsou šifrována různými způsoby. Tato část popisuje šifrování uložených dat na úrovni aplikace.

Šifrování na úrovni polí

Citlivá data zadaná do aplikace jsou uložena v databázích a šifrována podle standardu AES 256 v režimu AES/CBC/PKCS5Padding. Šifrování probíhá na aplikační vrstvě, což znamená, že přímý přístup k databázi (např. přes SQL) odhalí pouze zašifrovaná data. Přístup ke klíčům spravuje KMS (Key Management Service).

Typy šifrování podle citlivosti dat

- Typ 1 (výchozí): Každá organizace obdrží v KMS vyhrazený klíč, který slouží k šifrování jejích dat. Tento klíč je následně zašifrován pomocí master key a uchováván na samostatném serveru.
- Typ 2 (pro citlivá data a PII): Používá se pro data, jako jsou čísla bankovních účtů nebo biometrické údaje. V tomto modelu generuje KMS jedinečný klíč pro každý sloupec v tabulce databáze.

Typy šifrování podle možnosti vyhledávání

- Možnost vyhledávání v zašifrovaných datech závisí na použitém inicializačním vektoru (IV) — náhodné hodnotě, která zajišťuje, že stejný nešifrovaný text vždy vygeneruje jiný šifrovaný text.
- Equality-Preserving Encryption: Na jeden klíč se používá pouze jeden IV. To znamená, že stejný nešifrovaný text vždy vytvoří stejný šifrovaný text, což umožňuje vyhledávání v zašifrovaných datech (např. podle e-mailové adresy). Tato varianta se obvykle používá u šifrování typu 1.
- Standardní šifrování: Každý datový záznam obdrží jedinečný, náhodný inicializační vektor (IV). To znemožňuje vyhledávání, ale nabízí vyšší úroveň zabezpečení, protože identická vstupní data generují odlišné šifrované texty. Obvykle se používá u šifrování typu 2.

Šifrování souborů

Soubory uložené v distribuovaném souborovém systému (DFS) jsou šifrovány na úrovni aplikace pomocí standardu AES 256 v režimu CTR nebo GCM. Režim GCM je preferován, protože kromě šifrování zajišťuje také autentizaci a integritu dat prostřednictvím kryptografického kontrolního součtu.

- Typ 1: Každá organizace obdrží jeden klíč. Každý soubor je tímto klíčem zašifrován, avšak s jedinečným, náhodným inicializačním vektorem (IV) uloženým společně se souborem.
- Typ 2: Každý soubor obdrží jedinečný šifrovací klíč. Tento klíč je následně zašifrován pomocí vyhrazeného klíče Key Encryption Key (KEK), jedinečného pro danou organizaci a spravovaného pomocí KMS.

Další oblasti šifrování

- Šifrování URL: Citlivé části URL adres (např. identifikátory dokumentů) jsou šifrovány. Používá se model jednoho klíče na organizaci nebo jednoho klíče na funkci.
- Šifrování záloh: Všechna data v zálohách jsou v klidovém stavu šifrována stejnými standardy jako produkční data.
- Šifrování logů: Logy uložené v HDFS (Hadoop Distributed File System) jsou šifrovány pomocí nativní technologie Hadoop, přičemž správu klíčů zajišťuje KMS.
- Šifrování cache: Data v cache (Redis) obsahující citlivé osobní údaje podléhají šifrování.

Správa klíčů

Operace s kryptografickými klíči provádí interní KMS (Key Management Service). Proces šifrování využívá hierarchickou strukturu klíčů:

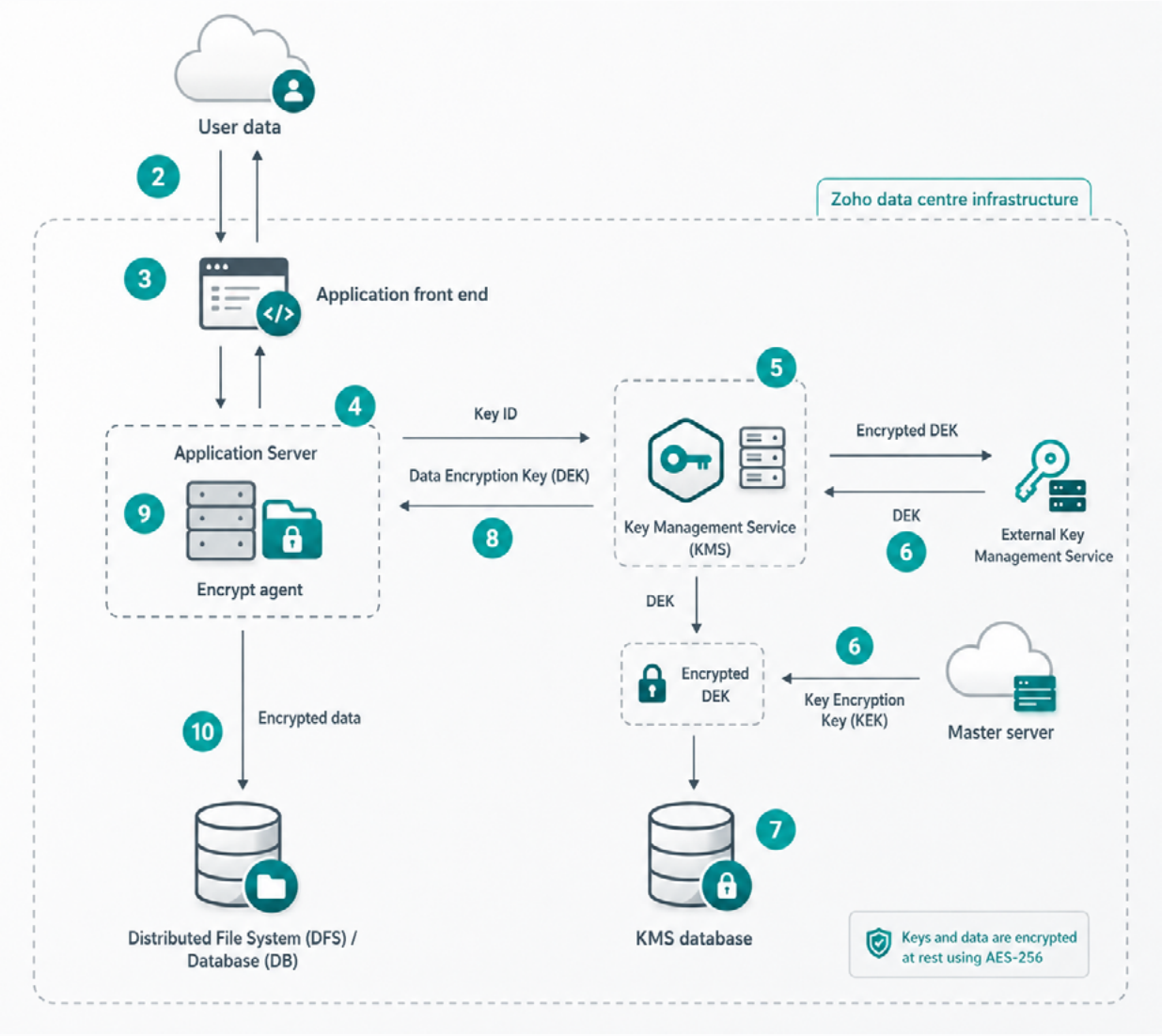
- Data Encryption Key (DEK): Používá se přímo k šifrování a dešifrování dat (převodu nešifrovaného textu na šifrovaný text).
- Key Encryption Key (KEK): Používá se k šifrování klíčů DEK a poskytuje tak další vrstvu ochrany. Je generován na samostatném serveru a ve výchozím nastavení je individuálně přiřazen dané službě Zoho.
- Master Key: Používá se k šifrování klíčů KEK. Z bezpečnostních důvodů je uložen na zcela izolovaném serveru.

Ve výchozím nastavení spravuje celý životní cyklus klíčů Zoho. Zákazníci mohou alternativně využít funkci Bring Your Own Key (BYOK) a používat vlastní klíče KEK, spravované v externích službách nebo poskytnuté manuálně.

Jak funguje KMS?

Všechny šifrovací operace jsou založeny na algoritmu AES 256. Proces využívá tzv. „envelope encryption" (obálkové šifrování), které funguje následovně:

1. Data (v databázi nebo souboru) jsou zašifrována pomocí klíče DEK.
2. Klíč DEK je následně zašifrován pomocí klíče KEK.
3. V závěrečné fázi je klíč KEK zašifrován pomocí master key.

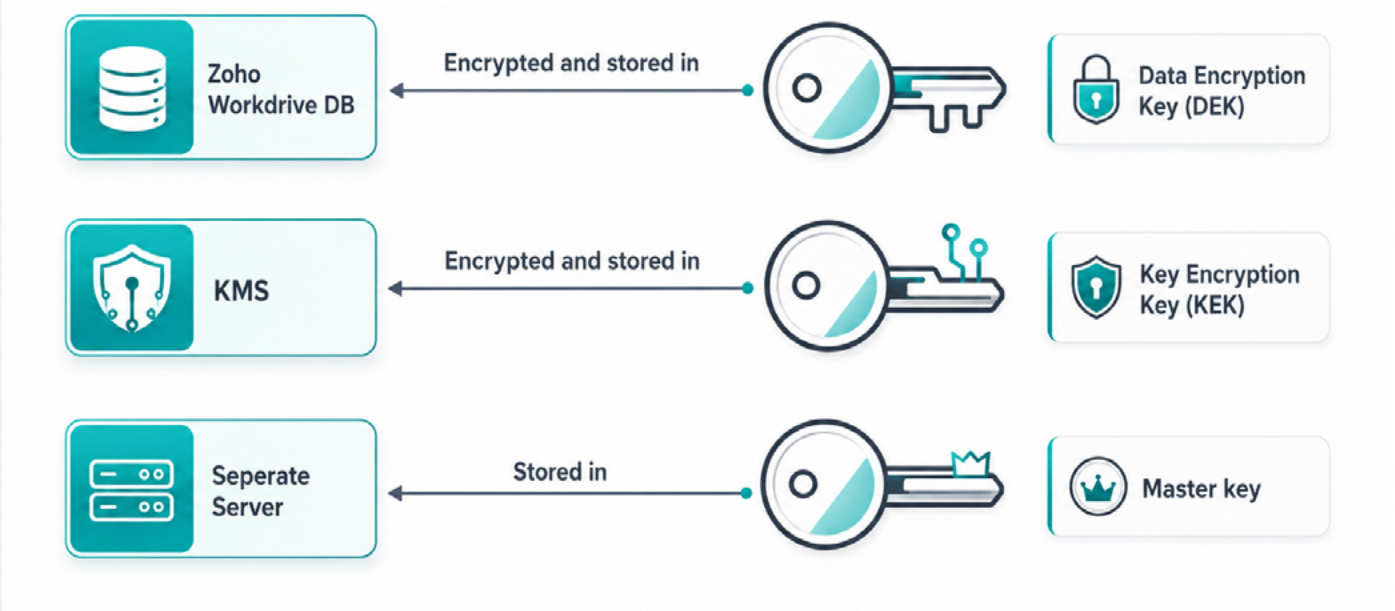


Tento přístup zajišťuje, že přístup k zašifrovaným datům vyžaduje hierarchické odemykání jednotlivých klíčů.

Generování a ukládání klíčů

- KMS generuje 256bitové klíče (v souladu s AES 256) společně s inicializačním vektorem (IV) pomocí knihovny Java Security a generátoru SecureRandom.

- Zašifrované klíče DEK jsou uloženy v databázi KMS. Master key je fyzicky oddělen a umístěn na jiném, zabezpečeném serveru, což útočníkovi znemožňuje získat přístup ke všem klíčům najednou.

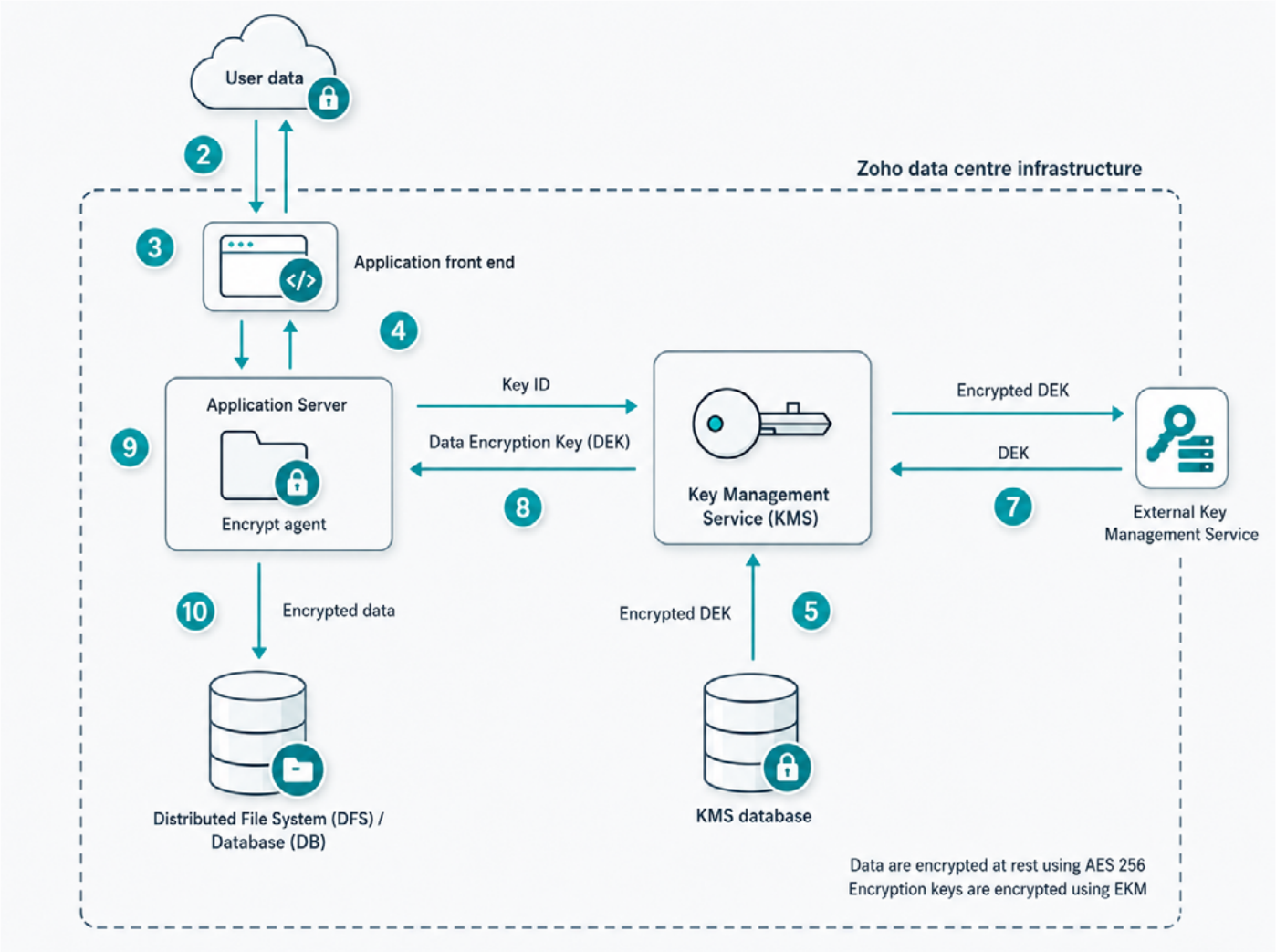


Zabezpečení klíčů

- Řízení přístupu: Přístup ke klíčům je přísně regulován pomocí seznamů řízení přístupu (ACL), které umožňují používat konkrétní klíče pouze vybraným službám. Každý přístup je autentizován a zaznamenáván a logy procházejí pravidelnými audity. Přístup pro zaměstnance Zoho je omezený a vyžaduje schválení vedením.
- Rotace klíčů: Master key prochází rotací. Proces výměny zahrnuje dešifrování všech klíčů KEK pomocí starého master key a jejich opětovné zašifrování novým klíčem. V současné době je tento proces spouštěn v případě kompromitace klíče.
- Dostupnost klíčů: Infrastruktura klíčů je replikována napříč data centry (master, slave, sekundární slave), což zaručuje vysokou dostupnost v případě výpadku hlavní lokality.

Bring Your Own Key (BYOK)

- Funkce BYOK umožňuje organizacím převzít plnou kontrolu nad vlastními šifrovacími klíči (KEK), místo aby se spoléhaly na klíče generované Zoho. To poskytuje možnost nezávisle spravovat přístup k datům a jejich dešifrování.
- BYOK lze nakonfigurovat prostřednictvím Zoho Directory, přidáním klíče z externího správce klíčů (EKM) nebo jeho ručním nahráním. V současné době jsou podporovány následující služby EKM:
    - AWS KMS,
    - Google KMS,
    - Thales CTM,
    - Fortanix DSM.



Šifrování celého disku

K implementaci hardwarového šifrování celého disku se používají samošifrovací disky (Self-Encrypting Drives, SED). Jedná se o disky HDD nebo SSD s vestavěným kryptografickým čipem, který automaticky šifruje všechna data zapsaná na disk a při čtení je dešifruje.

Jak to funguje a správa klíčů

Proces je založen na dvou typech klíčů:

1. Data Encryption Key (DEK): Uložen přímo na disku a používán k šifrování dat. Výchozí klíč od výrobce je námi během konfigurace serveru přegenerován, aby byly zachovány vyso ké bezpečnostní standardy.
2. Authentication Key (AK): Používán k šifrování klíče DEK a k uzamčení/odemčení celého disku, čímž poskytuje další vrstvu ochrany. Klíče AK jsou spravovány lokálním systémem správy klíčů (LKMS).

V případě krádeže nebo neoprávněného fyzického přístupu k disku zůstávají data nepřístupná, protože bez klíče AK — který je uložen odděleně — nelze klíč DEK dešifrovat.

Organizační zabezpečení

Zabezpečení ve společnosti Zoho je založeno na formálním systému řízení bezpečnosti informací (ISMS), který definuje cíle, rizika a metody jejich zmírňování. Tento systém je realizován prostřednictvím přísných politik a postupů, které zaručují bezpečnost, dostupnost, integritu a důvěrnost dat zákazníků.

Níže jsou uvedeny 4 klíčové pilíře bezpečnostního systému:

1. Lidé a bezpečnostní kultura

Prověřování zaměstnanců: Před nástupem do práce prochází každý zaměstnanec podrobnou prověrkou (trestní rejstřík, historie zaměstnání, vzdělání), kterou provádějí externí specializované agentury. Dokud není výsledek ověření pozitivní, není zaměstnanci udělen přístup k citlivým systémům.

Školení a budování povědomí: Proces onboardingu nových zaměstnanců zahrnuje podpis dohody o mlčenlivosti a školení v oblasti bezpečnosti informací a ochrany soukromí. Znalosti jsou pravidelně ověřovány a vzdělávací programy pokračují po celou dobu zaměstnání prostřednictvím interních platforem a akcí, aby si všichni udrželi přehled o nejlepších postupech.

2. Specializované týmy pro bezpečnost a ochranu soukromí

Společnost udržuje specializované týmy odpovědné za zavádění a řízení bezpečnostních programů. Ty odpovídají za návrh obranných systémů, nepřetržité sledování sítě z hlediska hrozeb a poskytování poradenství vývojářským týmům během vývoje produktů.

3. Interní audit a compliance

Samostatný tým pro compliance zajišťuje, aby interní postupy a politiky odpovídaly mezinárodním standardům a předpisům. Tento tým provádí pravidelné interní audity a koordinuje nezávislé audity prováděné externími firmami.

4. Zabezpečení koncových zařízení

Všechna zařízení používaná zaměstnanci podléhají přísným bezpečnostním pravidlům:

Pracovní stanice: Každý počítač má nainstalovaný aktuální software a antivirový software a je centrálně spravován prostřednictvím řešení pro monitoring koncových zařízení.

Výchozí ochrany: Zařízení jsou ve výchozím nastavení nakonfigurována tak, aby vynucovala šifrování disku, silná hesla a automatické uzamčení obrazovky po určité době nečinnosti.

Mobilní zařízení: Telefony a tablety používané k pracovním účelům jsou registrovány v systému MDM (Mobile Device Management), který vynucuje bezpečnostní standardy společnosti.

Zabezpečení infrastruktury

Ochrana infrastruktury je založena na vícevrstvém přístupu, který kombinuje pokročilé síťové technologie, hardwarovou redundanci a proaktivní sledování hrozeb.

Zabezpečení sítě

Síťová architektura byla navržena s ohledem na koncept „defense in depth" (hloubkové obrany). **Mezi klíčové prvky patří:**

Segmentace: Produkční prostředí (kde běží služby a jsou uložena data zákazníků) jsou na síťové úrovni důsledně oddělena od testovacích a vývojových prostředí.

Firewally: Veškerý provoz je filtrován, aby se zabránilo neoprávněnému přístupu. Konfigurace firewallu je denně kontrolována síťovými inženýry.

Nepřetržité sledování: Specializovaný tým Network Operations Center (NOC) nepřetržitě sleduje infrastrukturu a aplikace, zda nedochází k anomáliím nebo podezřelé aktivitě, přičemž využívá vlastní pokročilé nástroje.

Redundance a odolnost vůči chybám

Platforma je postavena na distribuované architektuře, která zajišťuje vysokou dostupnost služeb. To znamená, že výpadek jednoho serveru neovlivní provoz systému ani přístup uživatelů k jejich datům. Redundance se vztahuje také na klíčové síťové komponenty (jako jsou switche, routery a bezpečnostní brány), čímž se eliminuje riziko tzv. single points of failure (jednotlivých bodů selhání).

Ochrana před útoky DDoS

Na ochranu před útoky DDoS (Distributed Denial of Service) se používají technologie od předních specializovaných poskytovatelů. Tyto systémy přesně filtrují škodlivý provoz a zároveň zaručují neomezený průchod pro legitimní uživatele, čímž zajišťují kontinuitu služby a vysoký výkon.

Hardening systému

Všechny servery procházejí před nasazením do produkčního prostředí důkladným procesem hardeningu. Tento proces mimo jiné zahrnuje deaktivaci všech nepotřebných portů a služeb, odstranění výchozích účtů a zpevnění konfigurací. Proces je automatizovaný a zabudovaný do základního obrazu operačního systému (OS), což zaručuje konzistenci a vysoký bezpečnostní standard pro každý stroj.

Detekce a prevence průniků (IDS/IPS)

Používá se vícevrstvý systém detekce průniků:

Úroveň serveru a sítě: Systém sleduje signály z jednotlivých zařízení a analyzuje provoz v rámci celé sítě. Všechny administrativní akce a použití privilegovaných příkazů jsou podrobně zaznamenávány.

Analýza hrozeb: Pokročilá pravidla a mechanismy strojového učení analyzují shromážděná data a upozorňují bezpečnostní inženýry na potenciální incidenty.

Úroveň aplikace: Vlastní Web Application Firewall (WAF) filtruje provoz na základě definovaných bezpečnostních pravidel.

Úroveň poskytovatele internetových služeb (ISP): Uplatňuje se další vrstva ochrany (včetně filtrování provozu a rate-limitingu), která chrání před útoky na různých síťových vrstvách.

Provozní zabezpečení

Logování a monitoring

Systémy nepřetržitě monitorují a analyzují informace ze služeb, interního síťového provozu a aktivity zařízení — tyto události jsou zaznamenávány v různých typech logů (např. auditní události, kritické chyby a administrativní akce). Logy jsou automaticky analyzovány za účelem detekce anomálií, jako je neobvyklá aktivita na účtech zaměstnanců nebo pokusy o přístup k datům zákazníků.

Za účelem zajištění integrity a dostupnosti jsou logy uloženy na zabezpečených, izolovaných serverech a chráněny proti neoprávněným zásahům. Zákazníci mají také přístup k podrobným auditním logům operací (jako jsou aktualizace nebo smazání) provedených na jejich datech.

Správa zranitelností

Společnost uplatňuje specializovaný proces správy zranitelností, který zahrnuje aktivní

skenování systémů pomocí vlastních i externích nástrojů, jakož i pravidelné penetrační testování. Bezpečnostní tým rovněž proaktivně sleduje veřejné zdroje threat intelligence.

Každá identifikovaná zranitelnost je okamžitě zaznamenána, je jí přiřazena priorita na základě její závažnosti a je sledována, dokud není zcela opravena nebo dokud nejsou zavedena vhodná nápravná opatření.

Ochrana před malwarem a spamem

Všechny soubory nahrané uživateli jsou automaticky skenovány vlastním antimalwarovým systémem. Tento engine je pravidelně aktualizován o nové signatury hrozeb a k ochraně dat využívá techniky strojového učení (ML).

Za účelem prevence spamu služby podporují standard DMARC (založený na SPF a DKIM). Kromě toho specializovaný antispamový tým, podporovaný vlastními detekčními enginy, sleduje systémy z hlediska zneužití (např. phishingu) a reaguje na nahlášení.

Zálohy

Provádějí se denní přírůstkové zálohy a týdenní úplné zálohy databází. Tato data jsou šifrována (AES-256) a ukládána na serverech pomocí polí RAID, což zajišťuje jejich bezpečnost a redundanci.

Zálohy jsou uchovávány po dobu tří měsíců, během níž mohou zákazníci požádat o obnovu dat. Proces vytváření záloh je automaticky monitorován a jeho integrita je ověřována. Zoho také doporučuje zákazníkům, aby si pravidelně exportovali a vytvářeli vlastní lokální záložní kopie.

Obnova po havárii a kontinuita provozu

Data aplikací jsou replikována téměř v reálném čase mezi primárním a záložním data centrem (DC). V případě výpadku hlavní lokality okamžitě přebírá jeho funkce záložní centrum, čímž je zajištěna kontinuita služby s minimálním výpadkem.

Obě centra disponují redundantním internetovým připojením (od více poskytovatelů ISP) a kompletními fyzickými bezpečnostními opatřeními (záložní napájení, klimatizace, hasicí systémy). Společnost má formalizovaný plán kontinuity provozu (Business Continuity Plan, BCP), jehož účinnost je pravidelně ověřována prostřednictvím testů obnovy po havárii.

Řízení incidentů

Společnost má specializovaný tým pro řízení incidentů, který odpovídá za komplexní řešení bezpečnostních událostí.

Hlášení a reakce

Zákazníci mohou nahlásit jakékoli incidenty související s bezpečností nebo ochranou soukromí na vyhrazenou e-mailovou adresu: incidents@zohocorp.com. Tato hlášení jsou vždy považována za nejvyšší prioritu.

V případě, že je incident zjištěn interně:

- Informujeme zákazníky dotčené danou událostí a zároveň poskytujeme doporučení ohledně kroků, které by měli podniknout.
- Každý incident je sledován až do jeho úplného vyřešení, včetně zavedení nápravných opatření a mechanismů, které zabrání opakování podobné situace.
- Tam, kde je to relevantní, identifikujeme a uchováváme potřebné důkazy (např. systémové logy)

související s danou událostí.
- Způsob oznámení je přizpůsoben rozsahu incidentu: obecné události jsou komunikovány veřejně (blogy, fóra), zatímco incidenty týkající se konkrétní organizace jsou hlášeny přímo na registrovanou e-mailovou adresu administrátora dané organizace.

Oznamování úniků dat

Postupy oznamování přísně vycházejí z platných právních požadavků (jako je GDPR) a závisí na roli společnosti:

V roli správce údajů oznamujeme narušení bezpečnosti příslušnému dozorovému úřadu (např. předsedovi Úřadu pro ochranu osobních údajů, UODO) ve lhůtě stanovené zákonem.

V roli zpracovatele údajů neprodleně informujeme správce údajů (tedy zákazníka) dotčeného danou událostí.

Odpovědné zveřejňování zranitelností

Provozujeme program „Bug Bounty" zaměřený na aktivní zapojení komunity bezpečnostních výzkumníků. Prostřednictvím tohoto programu oceňujeme a odměňujeme práci jednotlivců, kteří nám pomáhají identifikovat potenciální zranitelnosti.

Zavazujeme se úzce spolupracovat s komunitou při ověřování, reprodukci a implementaci vhodných oprav nahlášených zranitelností.

Pokud jste nalezli bezpečnostní zranitelnost, můžete ji nahlásit dvěma způsoby:

1. Prostřednictvím naší oficiální platformy programu: https://bugbounty.zohocorp.com/
2. Přímo našemu bezpečnostnímu týmu na: security@zohocorp.com

Bibliografie

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)