MTG **Enterprise Resource Security**
Mastering Cryptographic Key Lifecycles

DARZ
Daten sind wertvoller als Geld

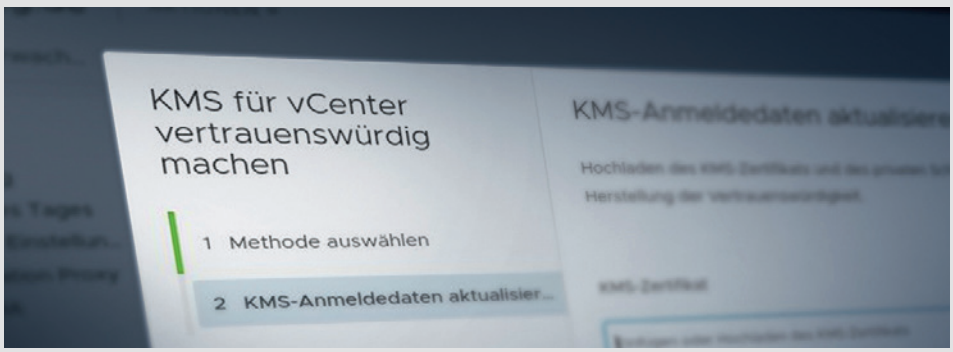
Foto: © MTG

VMware Verschlüsselung – mehr Sicherheit mit wenigen Klicks

Unser Verschlüsselungsservice basiert auf einem auf VMware abgestimmten Key Management System von MTG. Damit erfüllen Sie die wachsenden Sicherheitsanforderungen Ihres Unternehmens schnell und kostengünstig!

Virtuelle Maschinen (VM) sind portabel und daher prinzipiell auf jedem Server lauffähig. Unbefugten internen Personen oder externen Angreifern, die sich Zugang zu den betreffenden Netzwerken verschafft haben, sind die Daten unverschlüsselter VM schutzlos ausgesetzt.

VMware hat auf diese Bedrohung reagiert und ermöglicht die Verschlüsselung für Ihre VM über externe Key Management Systeme (KMS). Der Verschlüsslungsspezialist MTG verfügt über ein VMware-kompatibles KMS-Produkt. Mit dem Infrastructure Solution Provider DARZ konnte so in Kooperation ein kostengünstiges SaaS-Angebot speziell für KMU geschaffen werden.



vmware READY NETWORKING AND SECURITY

Einmal an das vCenter angebunden, können Nutzer mit wenigen Mausklicks ihre VMware VM zuverlässig verschlüsseln.

MTG KMS & DARZ Managed IT Security Services

Effektiver Schutz der Daten

Mehr Sicherheit für Ihre Daten – weniger Sorgen!

Unterstützt NIS 2, DSGVO, ISO 27001 und branchenspezifische Standards

Immer mehr gesetzliche Regularien fordern, den „Stand der Technik" in der Cybersecurity umzusetzen. Dazu gehören die jüngst in Kraft getretenen NIS 2 Verordnung, die DSGVO oder auch Anforderungen der DIN ISO 27001. Hierbei werden auch kleinere Unternehmen und mehr Branchen mit einbezogen.

Bei durchgehender Verschlüsselung aller VMware-VM können Prüfschritte entfallen und Prozessbeschreibungen im Rahmen der Schutzbedarfs- und Risikoanalyse deutlich reduziert werden.

Schutz sensibler Daten

Mit dem Verschlüsselungsservice sind sämtliche sensible Daten auf den VMware-VM geschützt:

> Datenbank, Dateisystem und Source Code Repository werden automatisch verschlüsselt.

> Lokal gespeicherte Zugangsdaten (z. B. für Datenbank Access, SSH Keys etc.) werden geschützt.

> Logdateien (z. B. von Applikationen) sowie personenbezogene Daten bei Anmeldungen am System, Transaktionen und IP-Adressen werden stets mitverschlüsselt.

vSAN Schutz & TPM

Neben der Verschlüsselung von VM bietet VMware noch die Möglichkeit, virtuelle Speicher-Netzwerke, sogenannte vSANs (virtual Storage Attached Network) mit der gleichen Methode zu schützen.

Anwendungen und Betriebssysteme, für die TPM (Trusted Plattform Module) vorausgesetzt werden (z. B. Microsoft Windows 11), lassen sich mit diesem Verfahren problemlos virtualisieren.

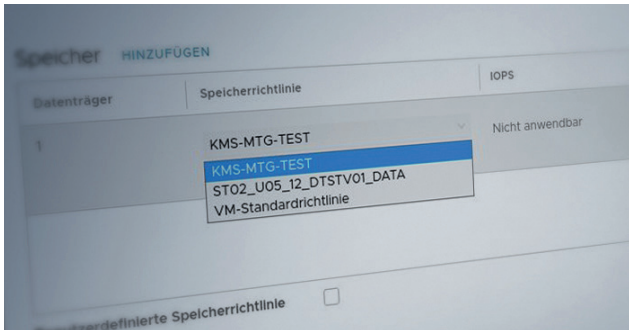
Verschlüsselung der Daten in jedem Betriebsmodus

Während der Speicherung, dem Betrieb und beim Zugriff bleiben die Daten auf der VM verschlüsselt. Das bietet umfassende Sicherheit und spart zusätzliche Kosten für die Verschlüsselung physischer Speichermedien.

> **Security at rest:** Bei Zugriff auf das Speichermedium, auf dem die verschlüsselte VM liegt, sind die Daten nicht lesbar. Das gilt explizit auch für Datenbanken, die auf der VM laufen. Teure Datenbankverschlüsselungen sind nicht mehr notwendig.

> **Security at work:** Der Schutz wird auch während der Laufzeit des Betriebs der VM gewährleistet.

> **Security in transit:** Bei der Übertragung vom Speicherort zum Hypervisor / ESXi Host werden die Daten der VM ebenfalls geschützt.



Hochsichere Schlüsselablage

Der Key-Encryption-Key (KEK) wird pro VM extern in einem KMS gespeichert und über FIPS-zertifizierte Hardware Security Module geschützt. Damit sind die Speicherorte der VM und der Schlüssel logisch getrennt.

Bei Speicherung von VM auf Wechseldatenträgern oder mobilen Datenträgern sind die VM immer verschlüsselt. Ein Verlust der Datenträger ist unkritisch. Die Datenträger können am Ende des Lebenszyklus leichter entsorgt werden.

Gelistet bei VMware Marketplace

Mit wenig Aufwand und Kosten zum Ziel

Einfache Anbindung

Das Angebot zeichnet sich über die Möglichkeit aus, die VM völlig standortunabhängig über den DARZ Service verschlüsseln zu lassen. Die Anbindung des MTG Key Management Systems erfolgt über die KMIP Standard-schnittstelle des vCenters und wird von unseren Experten übernommen.

Einfache Verschlüsselung über das eigene vCenter

Über die gewohnte Nutzeroberfläche zur Verwaltung der VM (vCenters / vCloud Directors) können Benutzer jede angebundene VM mit wenigen Klicks verschlüsseln. Es ist keine zusätzliche Software oder Schulung erforderlich.

Back-up, Redundanz und Hochverfügbarkeit

Das Schlüsselmaterial wird kundenspezifisch und sehr sicher abgelegt. Das ganze System ist hochskalierbar und wird ausfallsicher und geo-redundant betrieben.

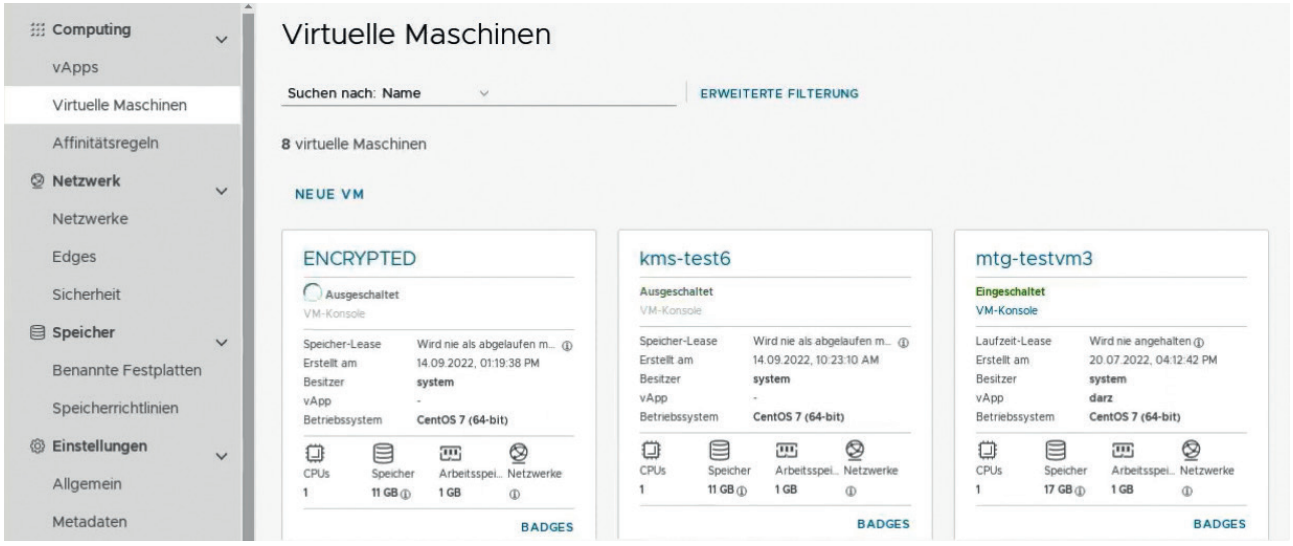
Einheitliche Verschlüsselungsprozesse

> Mit der angebotenen Lösung verfügt der Nutzer über ein einheitliches Verfahren und einen Prozess zur Verschlüsselung aller Daten in den VM. Das spart Zeit, Kosten und reduziert Komplexität.

> Das vCenter sorgt für eine transparente Ver- und Entschlüsselung. Nach einmaliger Konfiguration ist kein weiterer manueller Prozess erforderlich. Die Passwort-Eingabe (Pre-Boot Authentication) ist ebenfalls nicht nötig.

> Alles was auf einer VM läuft, ist automatisch verschlüsselt. Eine Verschlüsselung der VM ist unabhängig vom Gast-Betriebssystemen (Windows, Linux, iOS etc.) möglich. Sie kann insbesondere auch dann durchgesetzt werden, wenn das Gast-OS keine Full Disk Encryption unterstützt.

> Die Verschlüsselung von VM kann per Policy firmenweit durchgesetzt werden. In Audits lässt sich die Verschlüsselung dann ganz leicht zentral überprüfen und nachweisen. Diese Policy gilt dann Plattformübergreifend für alle Gastsysteme.



Demo Video:
Einfache Verschlüsselung über vCloud Director

MTG KMS & DARZ Managed IT Security Services

Unternehmensprofile & Kontakt

Managed Service von erfahrenen Experten

Zusammen mit dem langjährigen Kooperationspartner und Infrastruktur Serviceprovider DARZ GmbH wurde ein neuartiges VMware Encryption-as-a-Service-Angebot geschaffen, mit dem Sie Ihre VMware schnell und einfach verschlüsseln können.

DARZ GmbH

Die DARZ GmbH unterstützt Unternehmen dabei, die Chancen der digitalen Transformation für sich zu nutzen. Die Managed Services Lösungen offerieren neben der Leistungsfähigkeit eine ausgeprägte Modularität, Flexibilität und Skalierbarkeit. Dadurch wird jeder Kunde in die Lage versetzt, die für ihn zum jeweiligen Zeitpunkt relevanten Leistungen in Menge, Qualität und Kombination mit anderen Services selbst zusammenzustellen.

Das Rechenzentrum verfügt über diverse Sicherheitszertifizierungen, wie TÜV ISO EN50600 CAT III, DIN ISO 27001 und BSI TR-03145. Das angebotene System wird ausfallsicher und geo-redundant an zwei deutschen Standorten betrieben.

MTG AG

Die MTG AG wurde 1995 gegründet und ist ein führender Spezialist für anspruchsvolle Verschlüsselungstechnologien „Made in Germany". Das MTG ERS® Produktangebot umfasst Certificate Lifecycle Management, Public Key Infrastrukturen, Key Management Systeme und Hardware Security Module.

Neben der Verschlüsselung von VMware werden zudem Cloud-Lösungen für eine Managed PKI mit Certificate Lifecycle Management angeboten. Alle Unternehmensprozesse bei MTG sind ISO 27001 zertifiziert.

SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

DARZ GmbH · Julius-Reiber-Straße 11 · 64293 Darmstadt
Tel.: +49 6151/8762-777 · vertrieb@da-rz.de

da-rz.de

MTG AG · Dolivostraße 11 · 64293 Darmstadt
Tel.: +49 6151 8000-0 · contact@mtg.de

mtg.de