Bacher Systems

... Ihr IT-Denkpartner

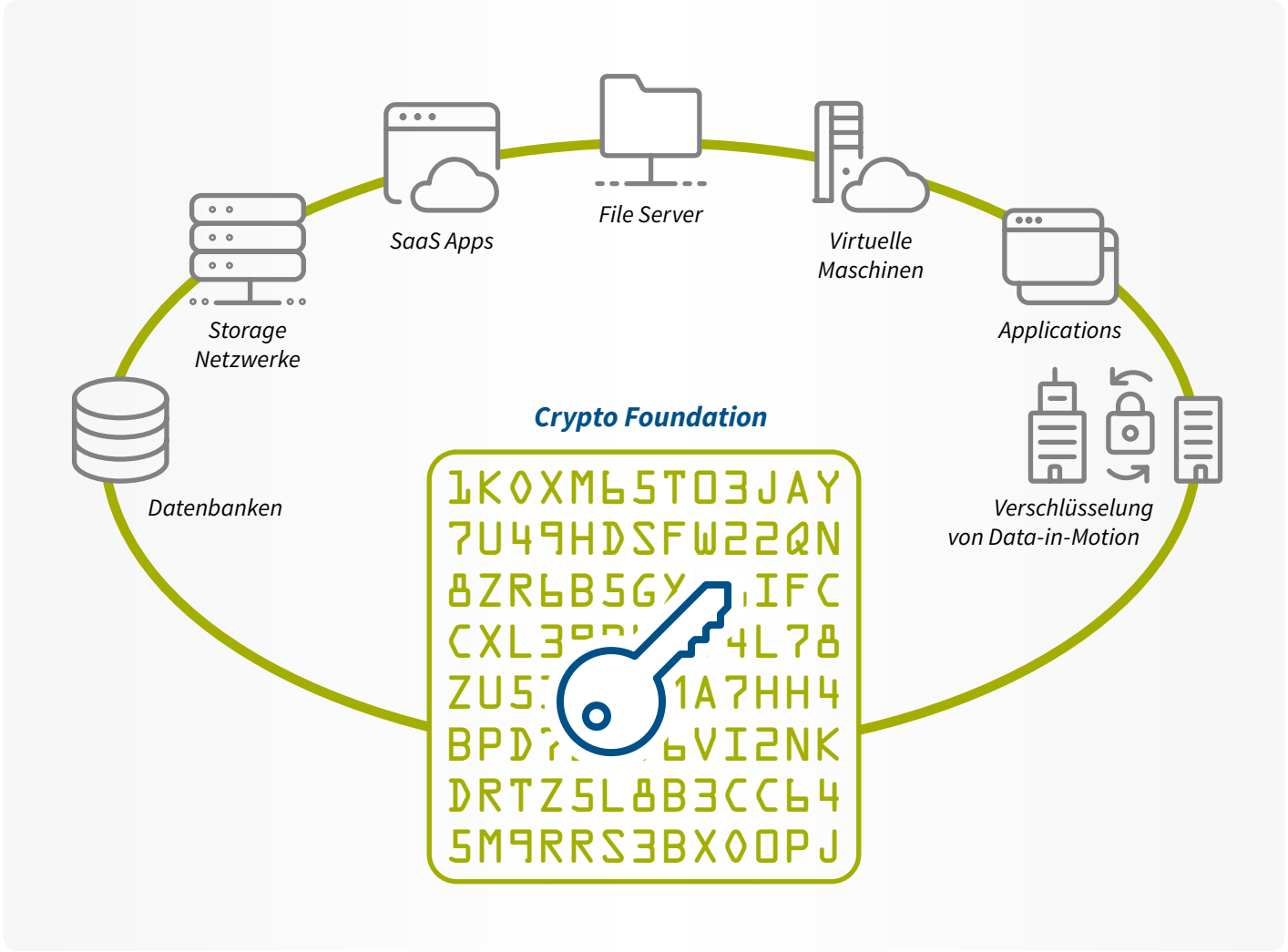
Crypto Management in a Nutshell

Crypto Management

Die Basis für Ihre Crypto-Strategie

Crypto Infrastruktur

Ein essenzieller Bestandteil jeder IT



Warum Encryption?

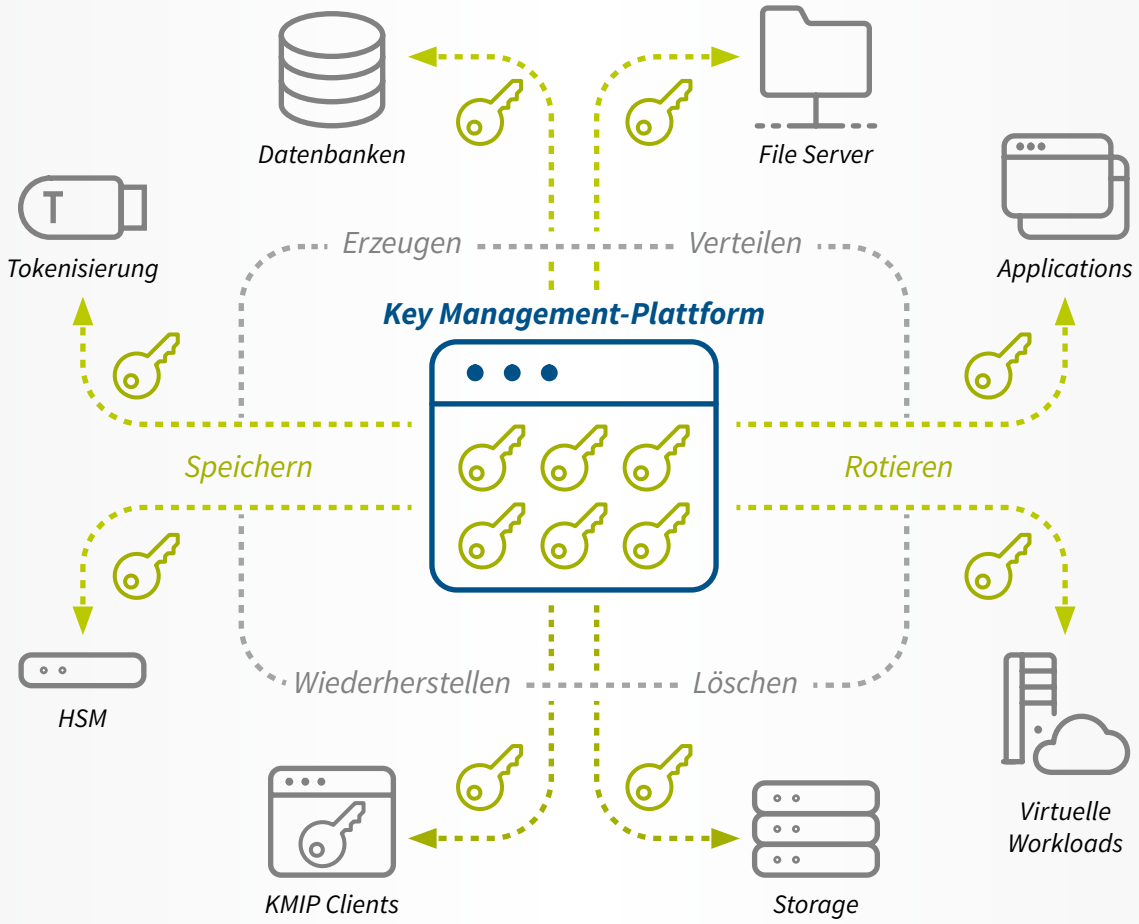
Fast täglich erscheinen Berichte über Diebstahl von Kundendaten. Doch wieso ist es für Angreifer so einfach, Daten zu stehlen? Schützenswerte Daten liegen einerseits an unterschiedlichen Orten – vom eigenen Data Center bis hin zu Cloud-Anwendungen. Andererseits sind sie über mehrere Wege erreichbar, ob nun per App von Mobilgeräten oder per Browser von jedem fremden Gerät aus. Dadurch entsteht ein enormes Risiko für schützenswerte Daten. Ein Mittel, um diese besser zu schützen, ist die Encryption sowohl bei der Übertragung als auch bei der Speicherung. Dabei ist ein zentraler Ansatz sinnvoll, um das Entstehen von „Crypto-Silos“ zu verhindern, bei denen Schlüsselmaterial dezentral abgelegt wird. Dies kann dazu führen, dass schnell die Kontrolle über die Schlüssel und damit auch über die Daten verloren geht.

Zentrales Key Management

Verschließen Sie Ihre Haustüre, die Garage, den Briefkasten und legen den Schlüssel dann in den Blumentopf? Vermutlich benutzen Sie einen Schlüsselbund, an dem Sie Ihre Schlüssel zentral aufbewahren. In IT-Umgebungen wird dieses Vorgehen leider oft nur unzureichend umgesetzt. Private Keys, die am Webserver liegen, Root-Zertifikate direkt am Server oder ähnliche Szenarien sind häufig anzutreffen. Um eine missbräuchliche Verwendung zu unterbinden, ist die zentrale Kontrolle und Verwaltung der Schlüssel durch ein zentrales Key Management essenziell. Es regelt die sichere Erzeugung, kontrolliert den Life-Cycle während der Verwendung und das zentrale, sichere Löschen von Schlüsseln innerhalb des Unternehmens. Selbst dann, wenn Applikationen, Services und Systeme aus der kontrollierten On-Premises-Umgebung an Cloud-Dienstleister ausgelagert werden.

Crypto Management

Ein zentraler Bestandteil moderner IT-Infrastrukturen



Vorteile

Zentrale Verwaltung von Verschlüsselungs-Keys

Manipulations- und diebstahlsichere Aufbewahrung

Eliminieren von Crypto-Silos

Interaktion mit Vielzahl an Systemen und Services

Sicheres Löschen von Schlüsseln

Cloud-Anbindung (Bring Your Own Key)

Für welche Use Cases ist Crypto Management sinnvoll?

Verschlüsselung bei Data Infrastructure und IT-Security

Sichere Nutzung von Cloud Services

Transparente Datenbank-verschlüsselung

Verschlüsselung zentraler File Shares und Dateien

Anonymisierung personenbezogener Daten

Anforderungen:

- *Verschlüsseln von Systemen in IaaS-Umgebungen*
- *Verschlüsseln von Daten in SaaS-Anwendungen*
- *Sichere Ablage von Backups in der Cloud*
- *Sicheres Löschen/Unbrauchbarmachen von Daten in der Cloud*

Vorteile:

- *Ohne Schlüssel sind die Daten nicht verwendbar*
- *Gestohlene Daten sind dadurch wertlos*
- *Zentrale Kontrolle über Daten in der Cloud*
- *Sicheres Löschen/Unbrauchbarmachen von Daten durch permanentes Löschen der Schlüssel*

Compliance sicherstellen

Sichere Kommunikation (Mail, Webservices)

Absichern von Public Key Infrastructure (PKI)

Verschlüsselung von Storage und Backup

Anforderungen:

- *Schutz der Root Certificate Authority (CA) vor Manipulation und Diebstahl*
- *Schutz von Private Keys einer PKI*
- *Manipulations- und diebstahlsichere Ablage der Keys in Hardware Security Modulen (HSM)*
- *Digitale Signaturen für DNS, Smart Grids, Codes, elektronische Rechnungen, Dokumente*

Vorteile:

- *Gefälschte Keys und Zertifikate sind ausgeschlossen*
- *Root-CA müssen nicht mehr weggesperrt werden*
- *Kopien von Root-CA sind ohne zugehörigen Schlüssel wertlos*

Warum Crypto Management mit Bacher Systems?

Nur durch den Einsatz von Verschlüsselungstechnologien können IT-Verantwortliche die Hoheit über ihre Daten in der Cloud behalten. Der sicheren Erzeugung des Schlüsselmaterials und dessen Verwaltung kommt dabei große Bedeutung zu.

Peter Bauer, Account Manager bei Bacher Systems

PKI-erzeugte Zertifikate spielen eine wesentliche Rolle in der Absicherung von Endgeräten. Um das Risiko des Verlustes der PKI-Schlüssel auszuschließen, müssen sie in Hardware erzeugt und abgelegt werden.

Markus Malits, IT-Security Consultant bei Bacher Systems

Wir machen den Schutz Ihrer Daten für Sie einfach!

- Status erheben: Wir identifizieren mit Ihnen alle schützenswerten Daten Ihres Unternehmens.
- Lösung erkennen: Wir entwickeln ein ganzheitliches Konzept für den umfassenden Schutz Ihrer Daten.
- Live erleben: Wir zeigen Ihnen Anwendungsbeispiele von HSM- und Key Management-Lösungen.
- Daten schützen: Professionell begleiteter Proof of Value durch Wissens- und Erfahrungsvorsprung.
- Kontrolle aufrechterhalten: Wir integrieren Crypto Management in Ihre IT-Umgebung.

Bacher Systems – Ihr IT-Denkpartner für Technologie in Ihren Geschäftsprozessen

Kontaktieren Sie uns doch einfach:
+43 1 60 126-0 oder info@bacher.at

Bacher Systems

Sechs Mythen über Encryption

Mythos: Encryption schränkt den Benutzer ein.

Wahrheit

Encryption ist für den Benutzer oft transparent. Im täglichen Betrieb ist davon meist nichts zu bemerken, da diese im Hintergrund passiert. Die Rechte dazu werden zentral vergeben, auch davon bemerkt der Benutzer nichts.

Mythos: Encryption ist teuer.

Wahrheit

Encryption ist eines der zentralen Mittel, um Daten vor Missbrauch oder Verlust zu schützen. Dieser Missbrauch kann weitreichende finanzielle Folgen durch Reputationsverlust, Strafzahlungen u.ä. haben, die die Anschaffungskosten einer Crypto-Managementlösung um ein Vielfaches übersteigen. Ein zentrales Key Management bringt auch erhöhte Effizienz und verringert die operativen Kosten.

Mythos: In der Cloud ist man bei Encryption auf den Cloud-Anbieter angewiesen.

Wahrheit

Viele Cloud-Anbieter sowohl im IaaS/PaaS als auch SaaS-Bereich bieten bereits Bring Your Own Key (BYOK). Der Cloud-Anbieter hat somit keine Möglichkeit auf Daten zuzugreifen, wenn diese mit dem mitgebrachten Schlüssel gesichert sind.

Mythos: Encryption braucht 3rd-Party Software.

Wahrheit

In vielen Lösungen und Services ist Encryption bereits inkludiert, dadurch wird 3rd-Party Software meist nicht benötigt. Für die Verwaltung der Schlüssel ist lediglich die Verbindung zum zentralen Encryption Management erforderlich – der Rest funktioniert out of the box.

Mythos: Encryption ist kompliziert.

Wahrheit

Ein zentrales Management vereinfacht Crypto-Operationen im Unternehmen. Der Überblick über die im Unternehmen verwendeten Schlüssel ist jederzeit gegeben.

Mythos: Encryption kostet Performance.

Wahrheit

Encryption ist in vielen Lösungen bereits bei der Entwicklung mitgeplant und daher optimal und mit geringstmöglichem Overhead integriert. Performance-Einbußen sind im Praxisbetrieb für den Benutzer nicht bemerkbar.

Bacher Systems EDV GmbH
Wienerbergstraße 11/B9
1100 Wien
E-Mail: info@bacher.at
Tel: +43 1 60 126-0
www.bacher.at

Bacher Systems