Kai Jendrian, Christoph Schäfer

Verschlüsseln in der Cloud

Visualisiert am Beispiel von Microsoft Azure RMS

IT-Outsourcing in „die Cloud“ liegt im Trend. Die Anbieter locken mit skalierbaren und anpassungsfähigen Anwendungen und Infrastrukturen und versprechen höhere Flexibilität bei geringeren Kosten. Doch Datenschutz- und IT-Sicherheitsbeauftragte sind alarmiert: Wie können personenbezogene Daten und sensible Informationen vor Dritten geschützt werden? Sind die Verschlüsselungsansätze der Cloud-Anbieter eine Lösung? Eine Analyse am Beispiel von Microsoft Azure RMS zeigt, dass die sichere Verwahrung von Schlüsseln nicht genügt.

1 Was ist Azure RMS?

Microsoft Azure ist die Cloud Computing-Plattform von Microsoft. Die Azure Rights Management Services (RMS) dienen dazu, Informationen bei der Verarbeitung mit Microsoft Office 365 Anwendungen vor nicht autorisierter Verwendung zu schützen.

Die Eigentümer von Dokumenten können in Azure RMS festlegen, wer diese öffnen, ändern, drucken, weiterleiten oder andere Aktionen mit ihnen ausführen darf. Der Schutz ist an das jeweilige Dokument gebunden – es ist also unerheblich, wo es gespeichert oder verarbeitet wird.

Die im Verfahren verwendeten Schlüssel und Zertifikate werden im Beitrag jeweils an der Stelle eingeführt, an der sie zum ersten Mal verwendet werden. Die Erzeugung und die Verteilung der Schlüssel sind nicht Gegenstand dieses Beitrags.

2 Verschlüsselung

An einem fiktiven Beispiel stellen wir die Funktionsweise von Azure RMS vor. Dabei stehen nicht die konkreten kryptografischen Bausteine im Vordergrund. Diese können sich jederzeit ändern. Wir wollen die komplexen Abläufe transparent machen.

Kai Jendrian

Security Consultant bei der Secorvo Security Consulting GmbH, lizenzierter Auditor und OWASP-Mitglied. Beratungsschwerpunkte: Information Security Management und Anwendungssicherheit.
E-Mail: kai.jendrian@secorvo.de

Christoph Schäfer

Security Consultant bei der Secorvo Security Consulting GmbH, zertifizierter betrieblicher Datenschutzbeauftragter (GDDcert.), Beratungsschwerpunkte: Datenschutz und Datensicherheit.
E-Mail: christoph.schaefer@secorvo.de

2.1 Berechtigungen

Ein Mitarbeiter erstellt mit einer Office-Anwendung ein Dokument und möchte es mit Azure RMS schützen. In unserem Beispiel legt dieser Mitarbeiter (M) zunächst Berechtigungen für das Dokument fest (Abbildung 1): Alle Mitarbeiter mit der Rolle „Vertrieb“ sollen lesen und schreiben [RW] können. Mitarbeiter mit der Rolle „Support“ sollen nur lesen dürfen [RO].

2.2 Content Key

Durch den Client wird zum Schutz des Dokuments ein zufälliger 128 bit langer AES-Schlüssel erzeugt. Für mobile Geräte wird dieser von Microsoft generiert und dem Endgerät übermittelt.

Dieser symmetrische Schlüssel wird als *Content Key* bezeichnet. Das Dokument wird dann durch die Anwendung mit dem Content Key symmetrisch mit AES 128 verschlüsselt (Abbildung 2).

Der Mitarbeiter M hat nun

- das ungeschützte Dokument,
- den zufälligen 128 bit langen Content Key, der dauerhaft auf seinem Endgerät gespeichert wird,
- die Berechtigungsliste, die er erzeugt hat, und
- eine AES-verschlüsselte Version seines Dokuments.

2.3 Public Key

Für den nächsten Schritt besorgt sich die Office-Anwendung des Mitarbeiters den öffentlichen Schlüssel (*Public Key*) des RMS Servers, das sogenannte *Server Licensor Certficate* (SLC). Der Public Key des RMS-Servers ist ein 2048 bit langer RSA-Schlüssel.

Mit dem Public Key des RMS Servers wird der Content Key per RSA-Verfahren verschlüsselt (Abbildung 3).

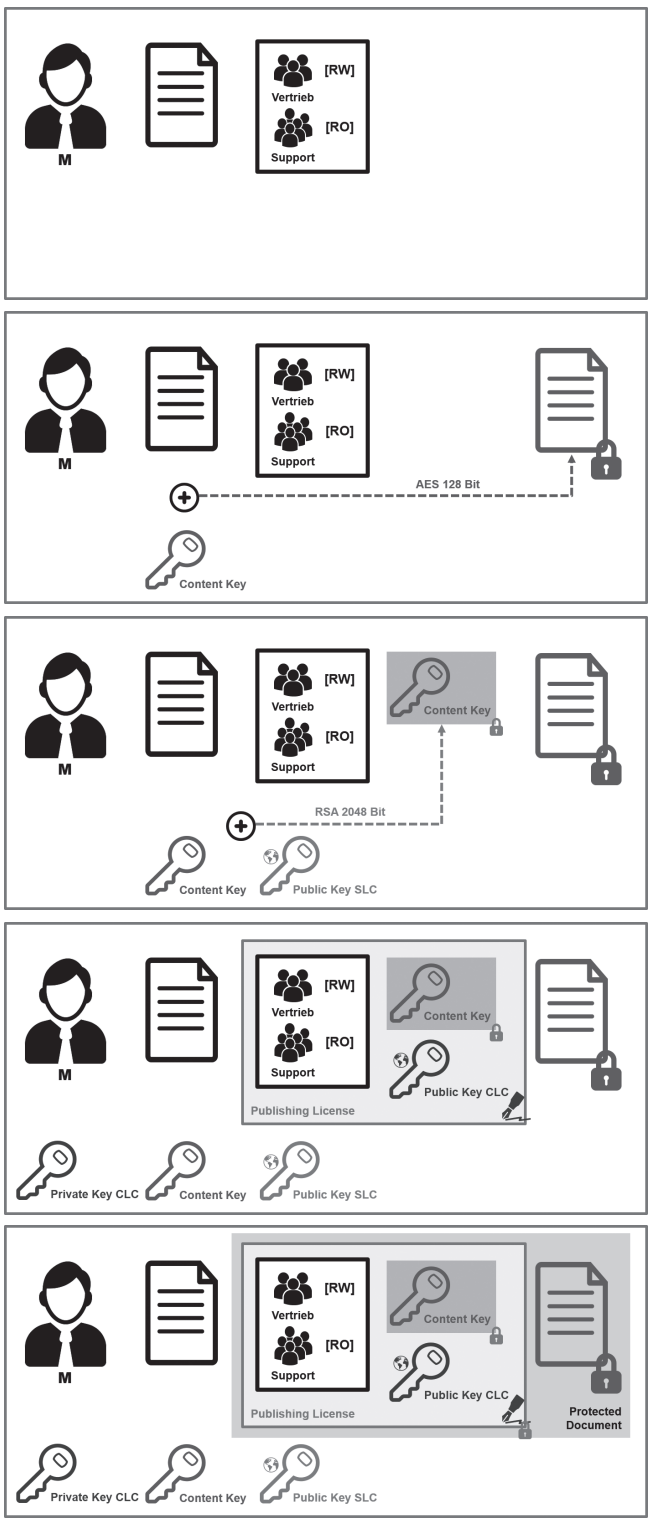
2.4 Publishing License

Für den nächsten Schritt benötigt der Client seinen privaten Schlüssel (Private Key) und den zugehörigen öffentlichen Schlüssel aus dem *Client Licensor Certficate* (CLC).

Die Berechtigungsliste, der verschlüsselte Content Key und der Public Key des Clients (aus dem CLC) werden zusammengestellt. Mit dem Private Key des Clients (CLC) wird diese Zusammenstellung signiert. Microsoft setzt dafür einen SHA-256-Hash ein.

Die signierte Zusammenstellung von Berechtigungen und Schlüsseln heißt *Publishing License* (Abbildung 4).

Abbildung 1 - 5 | Verschlüsseln



2.5 Protected Document

Die Publishing License in einem weiteren Schritt mit dem Public Key des RMS verschlüsselt. Die verschlüsselte Publishing Licence und das verschlüsselte Dokument werden in einer Datei zusammengestellt. Diese Datei wird als *Protected Document* bezeichnet (Abbildung 5).

3 Entschlüsselung

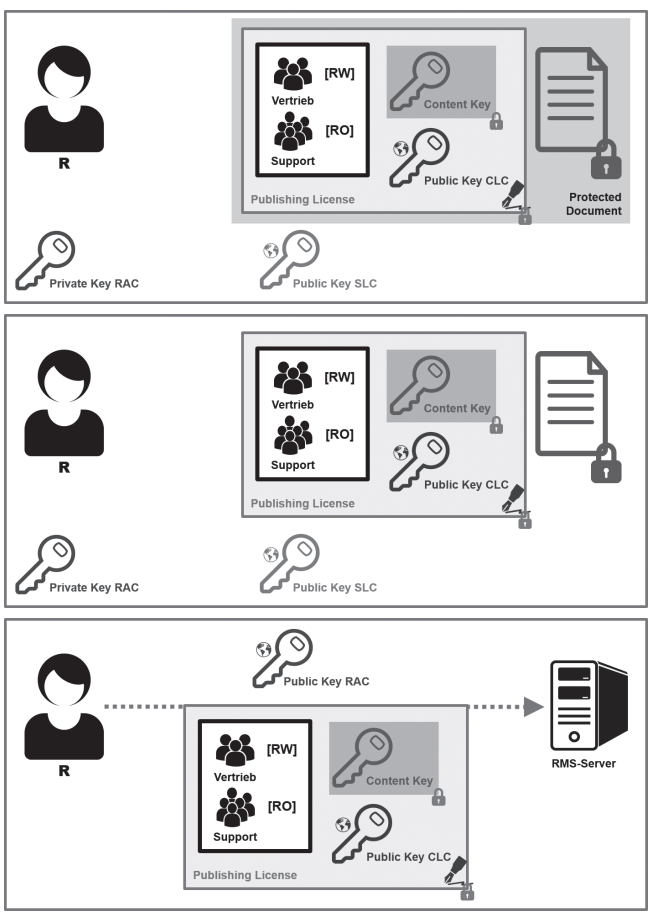
Der Prozess der Entschlüsselung erfordert einige Schritte mehr als die Verschlüsselung.

3.1 Empfang des Dokuments

Ein Empfänger (R) erhält ein Protected Document und will dieses nutzen (Abbildung 6). Er extrahiert die Publishing License und den verschlüsselten Inhalt (Abbildung 7).

Für die weitere Verarbeitung sendet der Empfänger zunächst die Publishing License und den Public Key seines *Rights Account Certificates* (RAC) an den RMS-Server (Abbildung 8). Das Zertifikat hat zwei Funktionen: es enthält seine ID für die Berechtigungsprüfung und seinen Public Key, mit dem später sichergestellt wird, dass nur er das Dokument verwenden kann.

Abbildung 6 - 8 | Entschlüsseln – Empfang



3.2 AD und HSM

Für die weiten Schritte benötigt Azure RMS zusätzlich zum RMS-Server noch zwei weitere Komponenten:

- Ein *Active Directory* (AD) mit Zuordnung von Individuen (IDs) zu Gruppen (Rollen).
- Ein *Hardware Security Module* (HSM), um kritische Entschlüsselungsfunktionen auszuführen. Das HSM hält dazu den privaten Schlüssel des SLC-Schlüsselpaares. Das HSM entschlüsselt alles, was der RMS-Server ihm zur Entschlüsselung vorlegt.

3.3 Berechtigungsprüfung

Um zu prüfen, ob der Empfänger das Dokument verwenden darf, benötigt der RMS-Server die entschlüsselte Publishing Licence.

Der RMS-Server selbst kann das Dokument nicht entschlüsseln, das kann nur das HSM. Der RMS-Server übergibt deshalb die verschlüsselte Publishing License an das HSM zur Entschlüsselung (Abbildung 9). Das HSM gibt dann die entschlüsselte Publishing License an den RMS-Server zurück (Abbildung 10).

Mit Hilfe des AD prüft der RMS-Server die Berechtigungen des Empfängers für das Dokument (Abbildung 11). Der RMS-Server hat nun die tatsächlichen Berechtigungen des Empfängers für das Dokument ermittelt – in unserem Beispiel darf der Empfänger das Dokument nur lesen (Abbildung 12). Falls der Empfänger nicht berechtigt ist, wird die weitere Bearbeitung abgebrochen.

3.4 RMS und HSM arbeiten zusammen

Der RMS-Server übergibt nach erfolgreicher Berechtigungsprüfung den verschlüsselten Content Key aus der Publishing License zur Entschlüsselung an das HSM (Abbildung 13). Das HSM entschlüsselt anschließend den Content Key und gibt ihn unverschlüsselt an den RMS-Server zurück (Abbildung 14).11Der RMS-Server

Abbildung 9 - 12 | Entschlüsseln – Berechtigungsprüfung

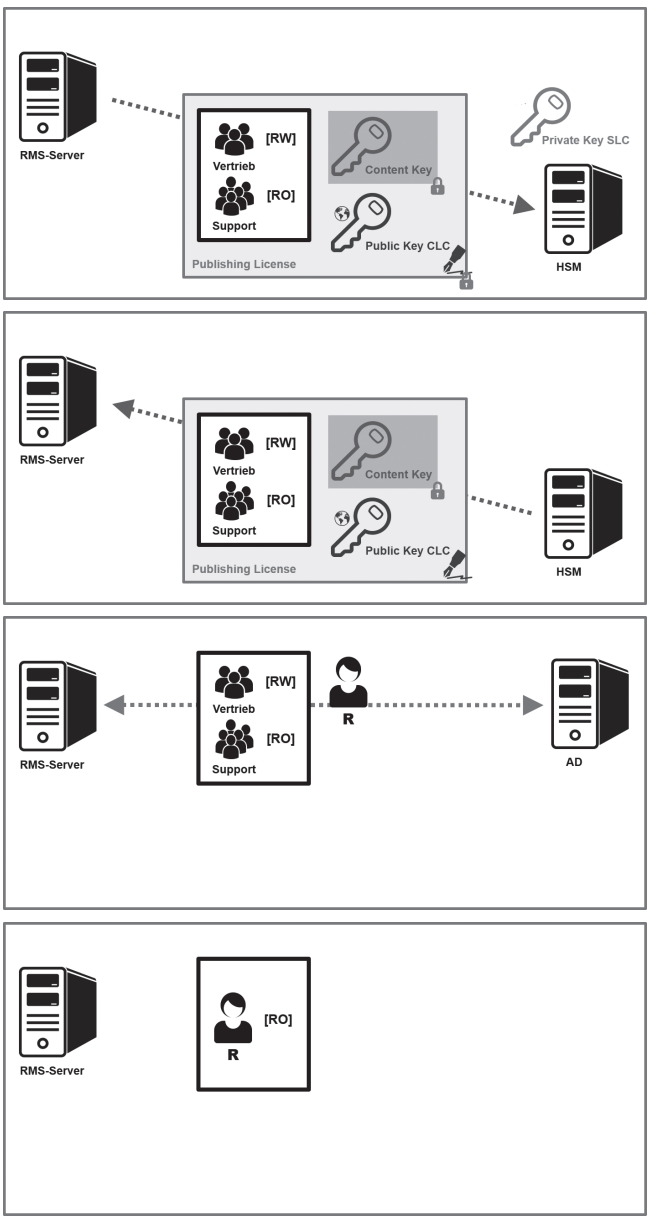


Abbildung 13 - 16 | Entschlüsseln – RSM, HSM

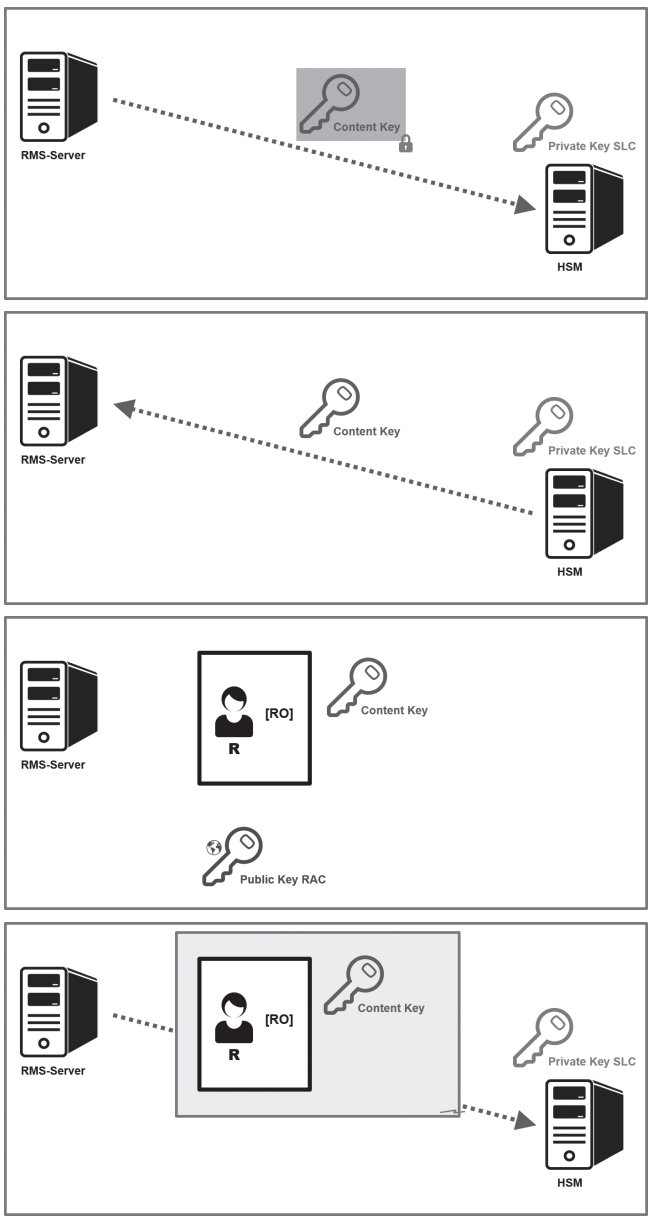
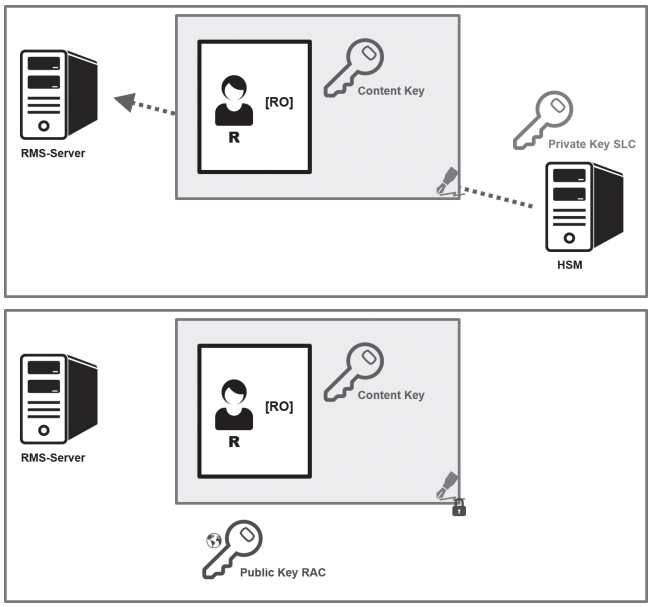


Abbildung 17 - 18 | Entschlüsseln – RSM, HSM



hat nun die tatsächlichen Berechtigungen des Empfängers und den unverschlüsselten Content Key sowie den Public Key des RAC des Empfängers vorliegen (Abbildung 15). Der Server stellt diese Berechtigungen und den unverschlüsselten Content Key zur sogenannten *Use License* zusammen und lässt diese durch das HSM mit dem Private Key des SLC signieren (Abbildung 16).

Das HSM liefert jetzt die signierte Use License an den RMS-Server zurück (Abbildung 17) und der der RMS-Server verschlüsselt die Use License mit dem Public Key aus dem RAC des Empfängers (Abbildung 18).

3.5 Zurück zum Empfänger

Nach diesen Prozessschritten übermittelt der RMS-Server die verschlüsselte Use License an den Empfänger (Abbildung 19), der nun das verschlüsselte Dokument sowie die verschlüsselte Use License vorliegen hat (Abbildung 20). Die Anwendung des Empfängers entschlüsselt die Use License anschließend mit dem Private Key aus dem Schlüsselpaar zum RAC des Empfängers (Abbildung 21).

Die Anwendung prüft die Berechtigungen aus der Use Licence. Ihr liegt jetzt die Berechtigungsliste und der unverschlüsselte Content Key vor (Abbildung 22).

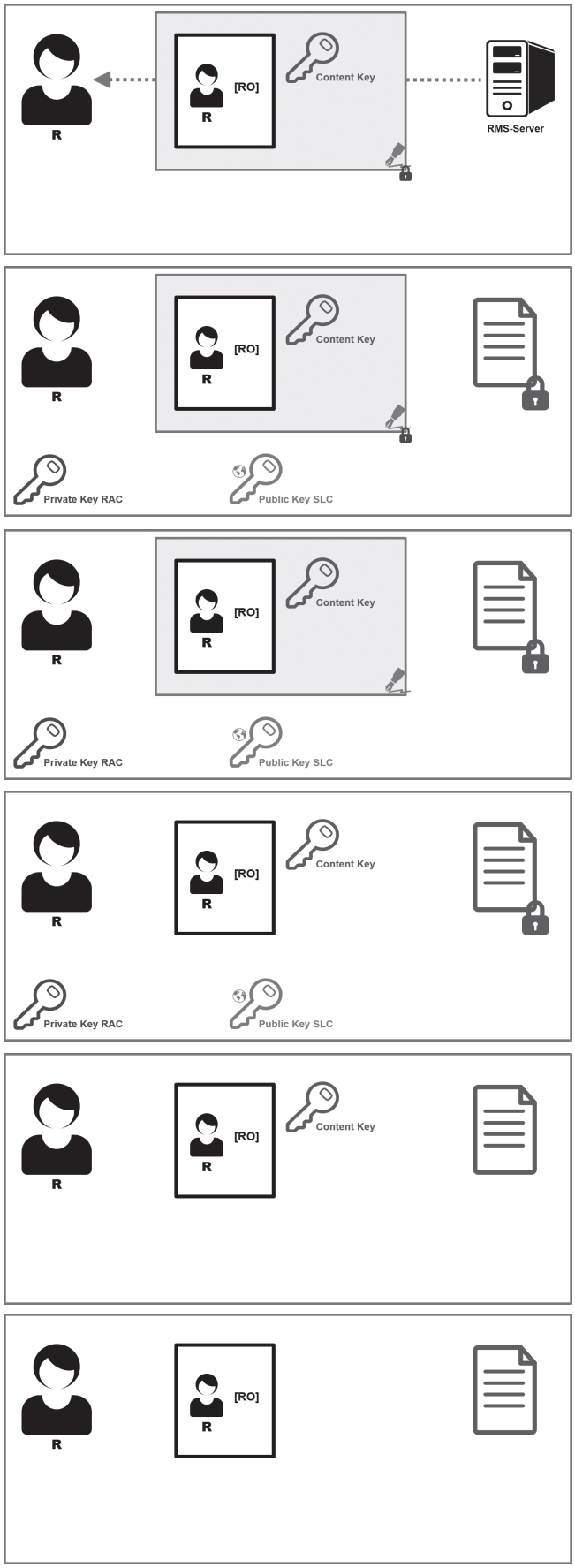
Mit dem Content Key kann die Anwendung des Empfängers nun das Dokument entschlüsseln (Abbildung 23). Die Anwendung beschränkt die Nutzung des Dokuments nach den Vorgaben der Berechtigungsliste (Abbildung 24).

4 Thesen

These I

Wenn in einer Organisation kooperativ in der Cloud gearbeitet werden soll, ist Verschlüsselung eine Herausforderung. Im Hintergrund laufen bei Azure RMS komplexe Schritte ab. Gleichwohl bietet Microsoft damit eine funktionierende und dem Stand der Technik entsprechende Lösung an.

Abbildung 19 - 24 | Entschlüsseln – Zurück zum Empfänger



These II

Cloud-Outsourcing setzt Vertrauen in den Dienstleister voraus. Mit Diensten wie Azure RMS kann ein hohes Schutzniveau von Informationen gewährleistet und die Durchsetzung einer Infoklassifizierung effektiv unterstützt werden.

Die Cloud-Anbieter können ein hohes technisches und organisatorisches Schutzniveau bieten und dabei auch den alleinigen Zugriff ihrer Mitarbeiter ausschließen, insbesondere auch der Administratoren. Dennoch besteht weiterhin das Risiko des missbräuchlichen Zugriffs auf Daten seitens des Cloud-Anbieters als Organisation, solange keine Ende-zu-Ende-Verschlüsselung eingesetzt wird.

These III

Um auch sensible Informationen in der Cloud speichern zu können, muss der Auftraggeber sowohl die Ver- als auch die Entschlüsselung alleine beherrschen und dabei auch die Schlüssel kontrollieren. Da Cloud-Verschlüsselungen für Kollaboration in der Regel auf Berechtigungslisten aufbauen, genügt die Schlüsselhoheit allein nicht, wie das Beispiel Azure RMS zeigt.

Entweder muss man das System zur Ver- und Entschlüsselung selbst betreiben oder aber auf eine Lösung eines Drittanbieters setzen – mit allen damit verbundenen Vor- und Nachteilen.

These IV

Wenn der Zugriff des Dienstleisters nicht vollständig ausgeschlossen werden kann, benötigt man trotz einer Verschlüsselung wie bei Azure RMS einen Auftragsdatenverarbeitungsvertrag gemäß § 11 des Bundesdatenschutzgesetzes (BDSG) mit dem Dienstleister.

Azure RMS dient primär dem Berechtigungsmanagement und gerade nicht dem Schutz von Daten oder Berufsgeheimnissen vor dem Dienstleister. Es ist daher ungeeignet, einen Zugriff vollständig auszuschließen.

Die hier vorgestellte Verschlüsselung ist dennoch aus Datenschutzsicht eine Bereicherung. Insbesondere für Interessensabwägungen – beispielweise als Grundlage für Datenübermittlungen – kann sie ein wichtiger Aspekt sein. Gleichzeitig stellt sie generell eine Maßnahme zur Verbesserung der Datensicherheit dar.

5 Fazit

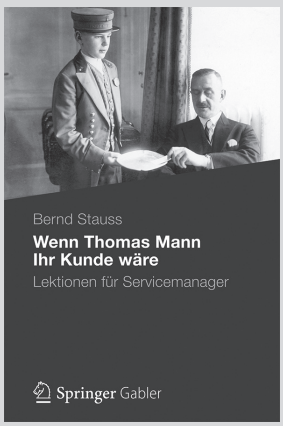
Ist Kryptographie also das Allheilmittel der Cloud? Diese Frage muss man klar mit „Jein" beantworten. Die Verschlüsselungs-Lösung eines Cloud-Anbieters einzusetzen, setzt Vertrauen in diesen voraus. Drittanbieter-Lösungen sind zwar erhältlich, scheitern aber im täglichen Betrieb oft an geringer Performance.

Nach einer Risikoabwägung wird man daher derzeit vermutlich zu einer Mischlösung kommen: Die allgemeine Datenverarbeitung kann möglicherweise unter Beachtung aller rechtlichen und technischen Rahmenbedingungen in die Cloud ausgelagert werden. Für besonders schützenswerte Informationen, wie beispielsweise dem Berufsgeheimnis unterliegende Daten, Gesundheitsdaten oder die „Kronjuwelen" des Unternehmens, wird man vielleicht eher eine klassische interne Rechenzentrumslösung wählen.

In jedem Fall muss der Auftraggeber die jeweilige Verschlüsselungslösung genau prüfen. Anbieter wären gut beraten, ihre Lösungen umfänglich und verständlich zu dokumentieren, um potenziellen Kunden eine solide Entscheidungsgrundlage zu bieten.

Von Thomas Mann Service lernen

springer-gabler.de



Bernd Stauss
Wenn Thomas Mann Ihr Kunde wäre
Lektionen für Servicemanager
2012. V, 210 S. mit 9 Abb. Geb. € (D) 24,95
ISBN 978-3-8349-4030-8

Wenn Servicemanager exzellenten Service liefern wollen, dann sollten sie ihr Handeln weniger an abstrakten Zahlenwerten und Modellen orientieren, sondern lieber Thomas Mann lesen. Die in diesem Buch präsentierten Textpassagen aus seinen Novellen und Romanen zeigen, wie präzise er Dienstleistungssituationen erfasst, die von bleibender Aktualität sind. Denn bei allem technischen Wandel hat sich nichts daran geändert, wie Menschen andere Menschen im Servicekontakt erleben und wie sie als Menschen behandelt werden wollen. Thomas Mann beschreibt meisterhaft das Denken, Empfinden und Handeln von Dienstleistungskunden. Daher eignen sich die geschilderten Episoden hervorragend dazu, zentrale Lektionen für heutige Servicemanager abzuleiten. Auf diese Weise führt uns der große deutsche Schriftsteller und Nobelpreisträger vor Augen, was modernes wissenschaftliches und praktisches Dienstleistungsmanagement ausmacht. „Wie seine literarischen Geschöpfe war Thomas Mann ein bürgerlicher, wohlhabender Mann mit sehr hohen Ansprüchen an Komfort und Servicequalität [...] Was er seinen Erzähler in der Novelle ‚Das Eisenbahnunglück' sagen lässt, gilt absolut auch für ihn selbst: ‚Ich reise gern mit Komfort.'"

Einfach bestellen:
SpringerDE-service@springer.com
Telefon +49 (0)6221 / 3 45 – 4301

Springer Gabler

Änderungen vorbehalten. Erhältlich im Buchhandel oder beim Verlag.