Ei des Kolumbus – oder Kuckucksei?
Microsoft Office 365 und Datenschutz

Christoph Schäfer
Secorvo Security Consulting GmbH

Als Christoph Kolumbus 1493 von seiner ersten Reise nach Amerika zurückgekehrt war, soll er zu einem Festmahl bei Kardinal Mendoza eingeladen worden sein. Auf seinen Reisebericht erwiderten einige Gäste, dass seine Entdeckung nicht außergewöhnlich gewesen sei – jeder andere hätte das auch gekonnt. Daraufhin soll Kolumbus die anwesenden Zweifler gebeten haben, ein hartgekochtes Ei auf eine der Spitzen zu stellen. Niemandem gelang es. Kolumbus schlug das Ei mit der Spitze auf den Tisch und stellte es hin. Empört wurde ihm vorgehalten, jeder hätte das tun können. Kolumbus erwiderte: „Der Unterschied ist, meine Herren, dass Sie es hätten tun können, ich hingegen habe es getan."

Das Ei des Kolumbus

IT-Outsourcing in "die Cloud" liegt im Trend. Die Anbieter locken mit skalierbaren und anpassungsfähigen Anwendungen und Infrastrukturen. Bei Cloud-Dienstleistungen befinden sich Hard- und Software ganz oder teilweise in den Rechenzentren des Anbieters. Auch kurzfristige Anpassungen an den tatsächlichen Bedarf sind oft viel schneller möglich als beim klassischen Outsourcing. Höhere Flexibilität bei geringeren Kosten ist die gewünschte Folge.

Eine solche Lösung ist auch Microsoft Office 365, bei dem die Anwendung aus der Microsoft-Cloud bezogen und Dokumente und E-Mails in Microsoft-Rechenzentren gespeichert werden. Könnte das das moderne Ei des Kolumbus sein?

Datenschutz-Denke

Während Cloud-Anwendungen bei Nutzern und IT-Verantwortlichen oft Jubelschreie ob der Möglichkeiten auslösen, zucken Datenschützer eher zusammen. Gerade wenn es um außereuropäische Anbieter geht, sind viele rechtliche Vorgaben zu beachten.

Oft überrascht der Ansatz des Gesetzgebers: Grundsätzlich darf man keine personenbezogenen Daten erheben, verarbeiten oder nutzen. Von dieser Regel gibt es zwei Ausnahmen: Entweder ein Gesetz erlaubt es bzw. ordnet es an oder der Betroffene, dessen Daten verarbeitet werden sollen, hat eingewilligt. Man spricht hierbei vom „Verbot mit Erlaubnisvorbehalt".[1]

Das Erheben, Verarbeiten und Nutzen sowie die Übermittlung personenbezogener Daten für eigene Geschäftszwecke ist zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines Vertrages mit dem Betroffenen erforderlich ist, es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen des Betroffenen dem entgegenstehen oder wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte.[2]

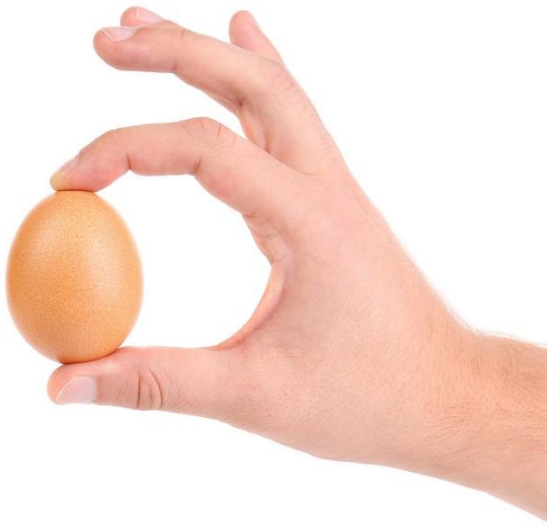


Bild: Indigolotos/Bigstock.com

[1] § 4 Abs. 1 BDSG

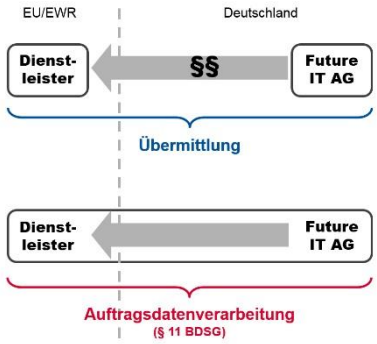
[2] § 28 Abs. 1 Satz 1 Nr. 1-3 BDSG

Eine Form des Verarbeitens im Sinne des Datenschutzes ist das Übermitteln[3] personenbezogener Daten. Dies liegt immer dann vor, wenn gespeicherte oder durch Datenverarbeitung gewonnene personenbezogene Daten Dritten[4] (außerhalb der für die Datenverarbeitung verantwortlichen Stelle) durch Weitergabe oder durch Bereithalten zum Abruf oder zur Einsicht bekanntgegeben werden.

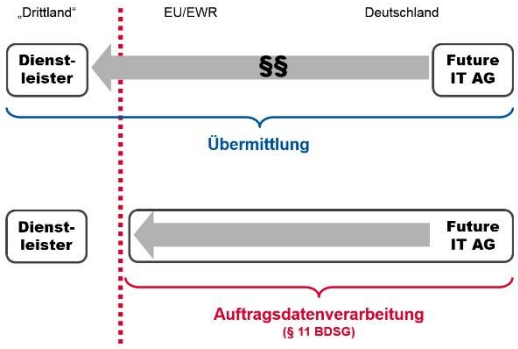
Für eine solche Übermittlung bedarf es einer Rechtsgrundlage, die unter Umständen nicht ohne größeren Aufwand oder auch gar nicht nachgewiesen werden kann.

Datenschutz und Dienstleister

Als Dritte gelten jedoch nicht Personen oder Stellen, die im Inland, in einem anderen Mitgliedstaat der EU/EWR personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen (Auftragsdatenverarbeitung).[5] Liegen die Voraussetzungen vor und schließt man einen entsprechenden Vertrag mit dem Dienstleister, erspart man sich das Erfordernis einer gesonderten Rechtsgrundlage. Dies macht viele Datenverarbeitungen durch Dienstleister überhaupt erst möglich, da man hierdurch nicht z. B. Einwilligungen aller seine Kunden einholen muss.



Problematischer wird es, wenn der Dienstleister in einem Drittland (außerhalb EU/EWR) sitzt. Eine Auftragsdatenverarbeitung ist in diesem Fall gar nicht möglich, so dass nur die Übermittlung als Lösung bleibt. Das Bundesdatenschutzgesetz (BDSG) stellt besondere Anforderungen an die Zulässigkeit einer Übermittlung in Drittländer.



Die Übermittlung ist unzulässig, wenn der Betroffene ein schutzwürdiges Interesse an dem Ausschluss hat, insbesondere dann, wenn bei den empfangenden Stellen außerhalb der EU kein angemessenes Datenschutzniveau gewährleistet ist. Die Gewährleistung eines angemessenen Datenschutzniveaus kann unter anderem durch den Abschluss der EU-Standardvertragsklauseln (EU-Model Clauses) erfolgen.

Safe Harbor

Bis vor kurzem konnten sich US-Unternehmen dem Safe Harbor-Abkommen unterwefen, wodurch formal ein angemessenes Schutzniveau hergestellt wurde. Datenschutz-Aufsichtsbehörden genügte Safe Harbor schon lang nicht mehr, allerdings musste zunächst der Europäische Gerichtshof (EuGH) tätig werden. Dieser hat Safe Harbor, einen Beschluss der EU-Kommission aus dem Jahr 2000, für unwirksam erklärt (Urteil vom 06.10.2015 – C-362/14).[6]

Besonders europäische Töchter amerikanischer Unternehmen stehen nun vor dem Problem, dass ihrer konzerninterne Datenverarbeitung – die meist auf Safe Harbor gestützt wurde – die Rechtsgrundlage fehlt.

Besondere Daten, besondere Probleme

Während man für „normale" personenbezogene Daten noch relativ schnell eine datenschutzrechtliche Lösung finden kann, gibt

3 § 3 Abs. 4 Satz 2 Nr. 3 BDSG
4 § 3 Abs. 8 Satz 2 BDSG
5 § 3 Abs. 8 Satz 3 BDSG
6 http://curia.europa.eu/juris/documents.jsf?num=C-362/14

es bestimmte Daten und Regelungen, die zusätzlich beachtet werden müssen.

Bei besonderen Arten personenbezogener Daten (Angaben über die rassische/ethnische Herkunft, politische Meinung, religiöse/philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) gelten zusätzliche Anforderungen – die schutzwürdigen Interessen der Betroffenen sind besonders hoch zu gewichten, weswegen eine Interessensabwägung als Rechtsgrundlage für die Übermittlung ausscheidet.

Sind Daten von Berufsgeheimnisträgern (Rechtsanwälte, (Betriebs-)Ärzte, Steuerberater, Psychologen…) betroffen, muss eine unberechtigte Kenntnisnahme der Daten[7] ausgeschlossen sein – auch durch Administratoren.

Will man Steuerdaten außerhalb Deutschlands speichern, bedarf es einer Genehmigung der Finanzbehörden.[8] In Betriebsvereinbarungen sind unter Umständen Ausschlüsse von Cloud-Datenverarbeitungen zu finden. Außerdem können vertragliche Ausschlüsse von Cloud-Verarbeitung mit Kunden vereinbart sein, deren Missachtung zu hohen Vertragsstrafen führen kann.

Während man die letzten Punkte schlicht beachten und ggf. regeln muss, bestehen insbesondere bei der Cloud-Verarbeitung besonderer Arten personenbezogener sowie einem Berufsgeheimnis unterliegender Daten hohe Hürden.

Die einzige Möglichkeit, diese Daten eventuell doch bei einem Cloud-Dienstleister verarbeiten zu dürfen, ist eine angemessene Verschlüsselung, die aber gewissen Anforderungen gerecht werden muss. So muss der Auftraggeber die Ver- und Entschlüsselung sowie die Schlüssel selbst vollständig beherrschen. Dies in einer Cloud-Umgebung zu gewährleisten ist nicht trivial und bei Office 365 derzeit nur mit einer Drittanbieter-Lösung denkbar.

Stolpersteine

Microsoft hat den Datenschutz schon früh als Nadelöhr erkannt und ist in einen Diskussionsprozess mit den europäischen Aufsichtsbehörden (Art.-29-Gruppe[9]) eingetreten.

Das Ergebnis dieses mehrjährigen Prozesses sind die im Juli 2014 veröffentlichten und zuletzt im Januar 2015 aktualisierten Online Service Terms (OST)[10], die eine Vielzahl bisher einzelner Vertragsdokumente zusammenfassen und als Anlage die EU-Standardvertragsklauseln enthalten.

Um den europäischen Datenschutzanforderungen gerecht zu werden garantiert Microsoft unter anderem die Speicherung von Daten innerhalb Europas, nämlich in den Rechenzentren in Dublin und Amsterdam.

Ganz ohne die USA kommt Office 365 dennoch nicht aus, da die Microsoft-Infrastruktur auf einen globalen Betrieb ausgerichtet ist. Unter anderem wird das AD-Adressverzeichnis auch außerhalb Europas (in den USA) verarbeitet.

Hinzu kommen Support-Fälle, in denen die Unterstützung von US-Mitarbeitern erforderlich ist. Daher genügt ein Vertrag zur Auftragsdatenverarbeitung mit Microsoft Irland allein nicht. Zusätzlich müssen die EU-Standardvertragsklauseln mit der Microsoft Corporation (USA) geschlossen werden.

Rechtsgrundlage für Microsoft Office 365

Neben der Vereinbarung zur Auftragsdatenverarbeitung mit Microsoft Irland werden EU-Standardvertragsklauseln mit der Microsoft Corporation (USA) geschlossen. Da dies mit einer Datenübermittlung in die USA einhergeht, wird eine Rechtsgrundlage benötigt.

Wie eingangs erläutert kommen dafür eine gesetzliche Erlaubnis oder die Einwilligung der Betroffenen (in der Regel der Mitarbeiter und/ oder Kunden) in Betracht.

7 § 203 Abs. 1 StGB

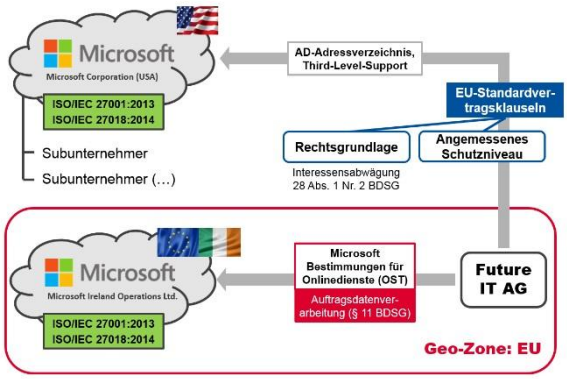
8 § 146 Abs. 2a S. 1 AO

9 http://ec.europa.eu/justice/data-protection/article-29/index_de.htm

10 http://www.microsoftvolumelicensing.com/ DocumentSearch.aspx?Mode=3&DocumentTypeId=31

Die Einwilligung der Mitarbeiter scheidet beim Cloud-Outsourcing als Rechtsgrundlage regelmäßig aus. Eine der gesetzlichen Anforderungen an die Einwilligung ist die Freiwilligkeit.[11] Im Arbeitsverhältnis ist Freiwilligkeit allerdings kaum zu gewährleisten.

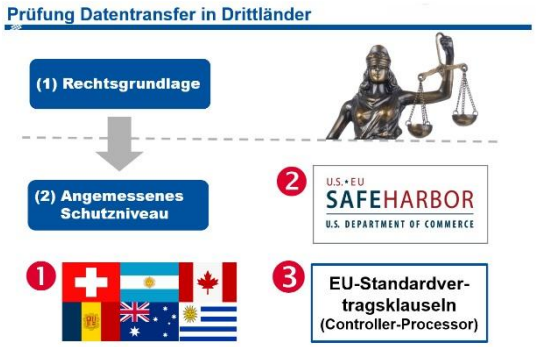
Als gesetzliche Grundlage könnte die Interessensabwägung zwischen den berechtigten Interessen des Unternehmens und den schutzwürdigen Interessen der Mitarbeiter/Kunden herangezogen werden.



Prüfung des Datentransfers in Drittländer

Die Prüfung erfolgt in zwei Schritten:

(1) Es muss eine Rechtsgrundlage gefunden werden.
(2) Im Zielland muss ein angemessenes Datenschutzniveau sichergestellt werden.



Bei der Interessenabwägung als Rechtsgrundlage muss eine sorgfältige Abwägung aller Aspekte – positiver wie negativer – erfolgen. Insbesondere muss bewertet werden, welche Arten von Daten in der Cloud verarbeitet werden sollen und welche nicht. Auch mögliche Zugriffe durch US-Strafverfolgungsbehörden oder Geheimdienste müssen bewertet werden.

Die möglichen Vorteile eines Cloud-Outsourcings dürfen dabei nicht vergessen werden – möglicherweise kann durch die Auslagerung sogar ein höheres Sicherheitsniveau erreicht werden. In jedem Fall sollte die Abwägung auf Fakten basieren.

Auf der zweiten Prüfungsstufe muss sichergestellt werden, dass im Zielland (hier: USA) ein dem europäischen Datenschutzrecht entsprechendes „angemessenes Schutzniveau“ herrscht. Neben einer von der EU-Kommission definierten Liste[12] von sicheren Drittländern (Œ), auf der die USA nicht zu finden sind, käme das Safe-Harbor-Abkommen[13] (•) in Frage. Dieses wurde jedoch kürzlich vom EuGH für unwirksam erklärt. Microsoft bietet daher im Rahmen seiner OST die EU-Standardvertragsklauseln als Grundlage an. (Ž)

Trau, schau, wem

Auch nach der Abstimmung des Microsoft-Vertragswerks mit der Art.-29-Gruppe obliegen dem Auftraggeber umfangreiche Prüfpflichten der Verträge. Problematisch ist insbesondere, dass die Auftragsdatenverarbeitung in Deutschland sehr explizit geregelt ist. Denn es finden sich nicht alle Anforderungspunkte des Bundesdatenschutzgesetzes direkt im Vertrag wieder.

…oder Kuckucksei

Vielleicht ist Office 365 aber auch eher ein Kuckucksei. Das Risiko des möglichen Datenherausgabeanspruchs seitens US-Strafverfolgungsbehörden gegenüber Tochterunternehmen und Niederlassungen US-amerikanischer Unternehmen muss bewertet werden. Dies wird besonders in den Medien oft diskutiert und heftig kritisiert. Microsoft wehrt sich derzeit in einem Rechtsstreit in

11 § 4a Abs. 1 Satz 1 BDSG

12 http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

13 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF

den USA gegen einen solchen Herausgabeanspruch. Der Ausgang des Prozesses kann derzeit nicht abgesehen werden. Die bloße Unterstellung, die USA hätten jederzeit Zugriff auf Daten amerikanischer Unternehmen in Europa, kann jedoch nicht in einer grundsätzlichen Beurteilung der datenschutzrechtlichen Zulässigkeit die rechtliche Unzulässigkeit bereits vor der tatsächlichen Vornahme einer solchen rechtswidrigen Übermittlung annehmen.

Fraglich ist, wie der oft diskutierte Datenzugriff durch (US-)Geheimdienste zu bewerten ist. Hierzu gibt es keine gesicherte Faktenlage, die bewertet werden kann. Der Geheimdienstzugriff ist daher im Rahmen einer Risikoeinschätzung zu betrachten.

Und nun?

Cloud-Datenverarbeitung wird sich vermutlich nicht aufhalten lassen. Derzeit tun sich die Datenschutz-Aufsichtsbehörden in Deutschland noch sehr schwer damit. Unternehmen können sich nicht allein auf die Microsoft-Verträge verlassen. Soll Office 365 eingeführt werden, muss eine ausführliche Prüfung und Bewertung – unter anderem durch den betrieblichen Datenschutzbeauftragen – erfolgen. Ein datenschutzrechtliches Restrisiko lässt sich nicht ausschließen.

Office 365 kann möglich sein

Unter den oben dargestellten Voraussetzungen kann ein datenschutzkonformer Einsatz von Microsoft Office 365 möglich sein, wenn er auch nicht frei von Risiken ist. Trotz valider Prüfung bleibt aufgrund der erforderlichen Interessensabwägung als Teil der Rechtsgrundlage aus § 28 Abs. 1 Nr. 2 BDSG ein Rechtsrisiko bezüglich der Auslegung bestehen: Die zuständige Datenschutz-Aufsichtsbehörde könnte zu einer anderen Wertung gelangen und die Datenverarbeitung in Office 365 untersagen.

Dies kann auch nachträglich beispielsweise durch eine Veränderung des Kenntnisstandes über Datenzugriffe oder -herausgabeverlangen aus Drittstaaten eintreten. Übrigens: Microsoft behält sich die Änderungen an seinen Diensten aufgrund der Änderung rechtlicher Rahmenbedingungen vor, so dass der geprüfte Stand plötzlich ganz anders aussehen kann. Für diesen Fall benötigt man eine Fallback-Strategie, um die Daten aus der Cloud zurückholen zu können.

Die Sicht der Aufsichtsbehörden

Insbesondere müssen die künftigen Aussagen von Datenschutz-Aufsichtsbehörden verfolgt werden. Sowohl der Berliner als auch der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit haben im Rahmen des 9. Europäischen Datenschutztages am 28.01.2015 geäußert, die Vorgaben für Datenübermittlungen in die USA kritisch prüfen und gegebenenfalls untersagen zu wollen. Die Auswirkungen des Safe Harbor-Urteils sind noch nicht absehbar. Der EuGH kritisierte insbesondere, dass durch das Abkommen kein angemessenes Datenschutzniveau in den USA hergestellt werden kann. Konsequent weitergedacht, ist dies durch EU-Standardvertragsklauseln allerdings ebenso wenig möglich.

Kolumbus oder Kuckuck?

Ob Microsoft Office 365 nun das Ei des Kolumbus oder das des Kuckucks ist, lässt sich weder pauschal noch final beantworten. Unternehmen müssen den Einsatz in jedem Fall sehr kritisch prüfen und letztlich entscheiden, ob der Einsatz trotz eines Rechtsrisikos gewollt ist. Die Antwort auf diese Frage wird je nach Unternehmen unterschiedlich ausfallen

Über den Autor:

Christoph Schäfer ist Security Consultant bei der Secorvo Security Consulting GmbH, zertifizierter betrieblicher Datenschutzbeauftragter (GDDcert.), Datenschutzauditor (TÜV) und TeleTrusT Information Security Professional (T.I.S.P.). Seine Beratungsschwerpunkte sind datenschutzrechtliche Fragestellungen und technisch-organisatorischer Datenschutz. Zudem hält er regelmäßig Schulungen und Vorträge zu Datenschutzthemen.

Telefon: 0721 255171-312 | E-Mail: christoph.schaefer@secorvo.de

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.

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).

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

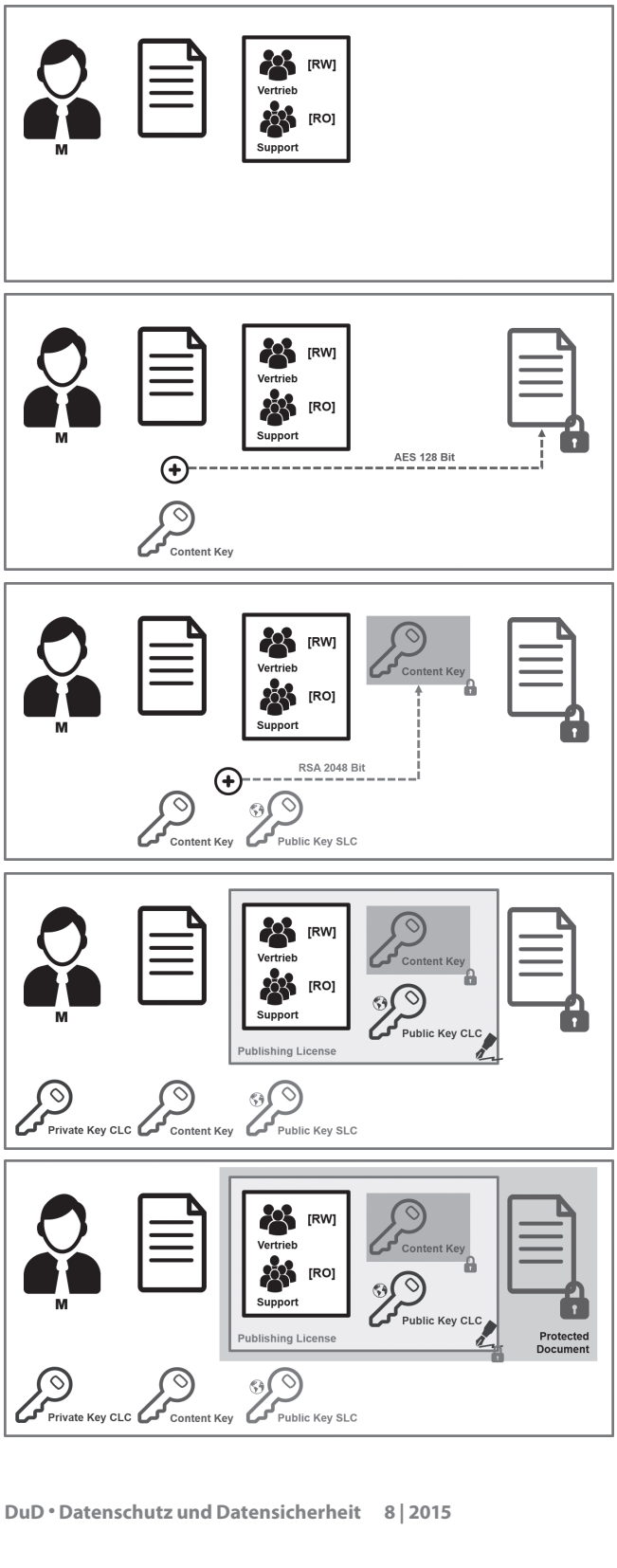
Christoph Schäfer

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

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

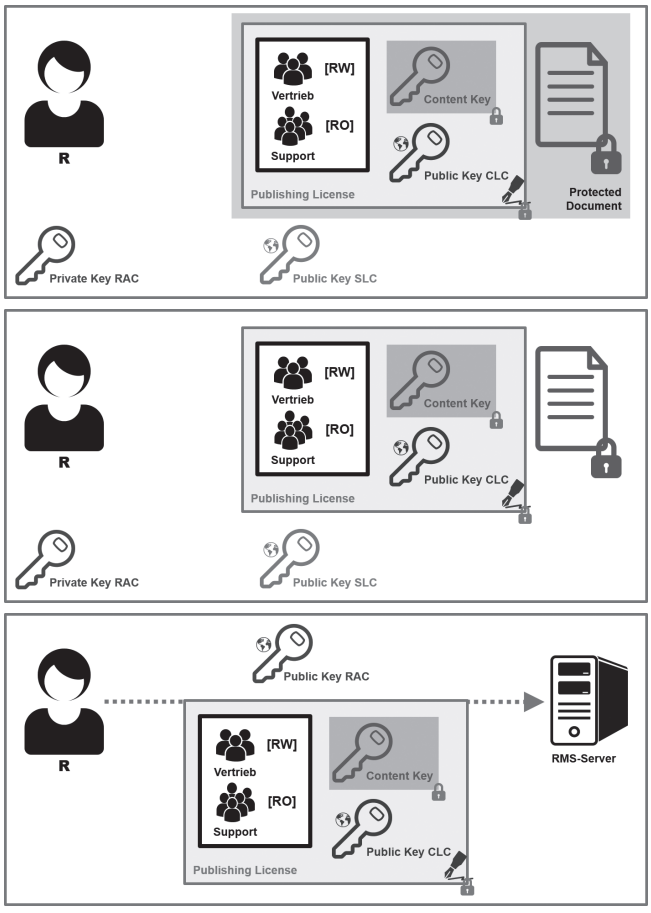
Der Prozess der Entschlüsselung erfordert einige Schritte mehr als die Verschlüsselung.

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

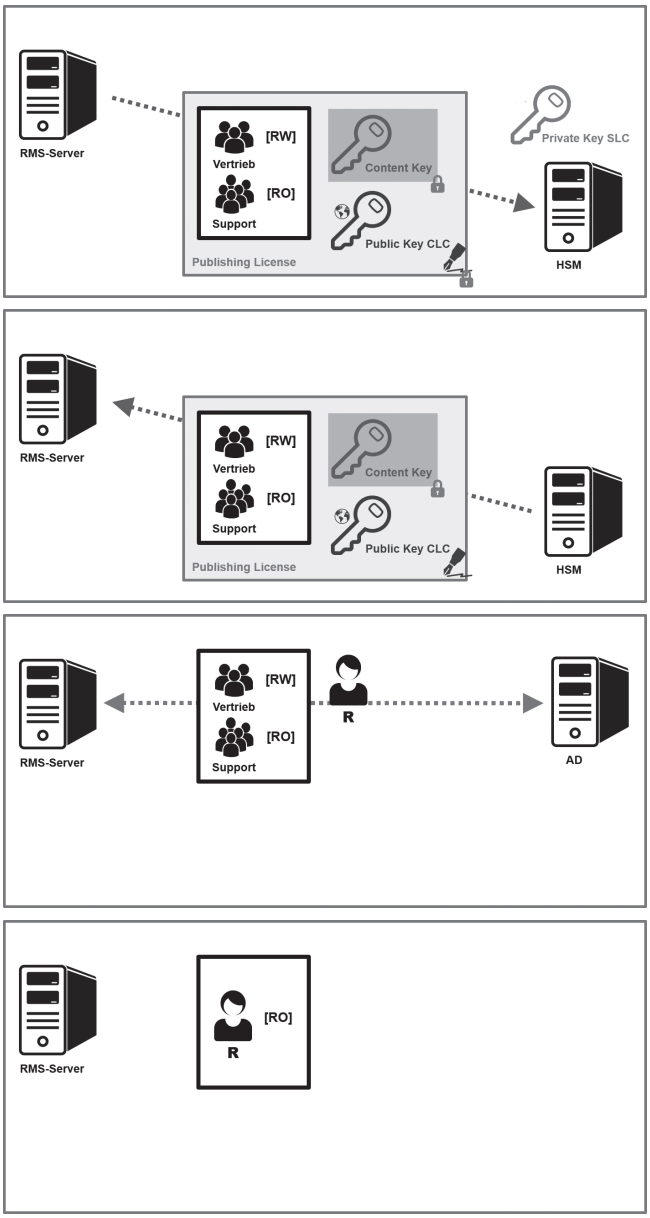


Abbildung 13 - 16 | Entschlüsseln – RSM, HSM

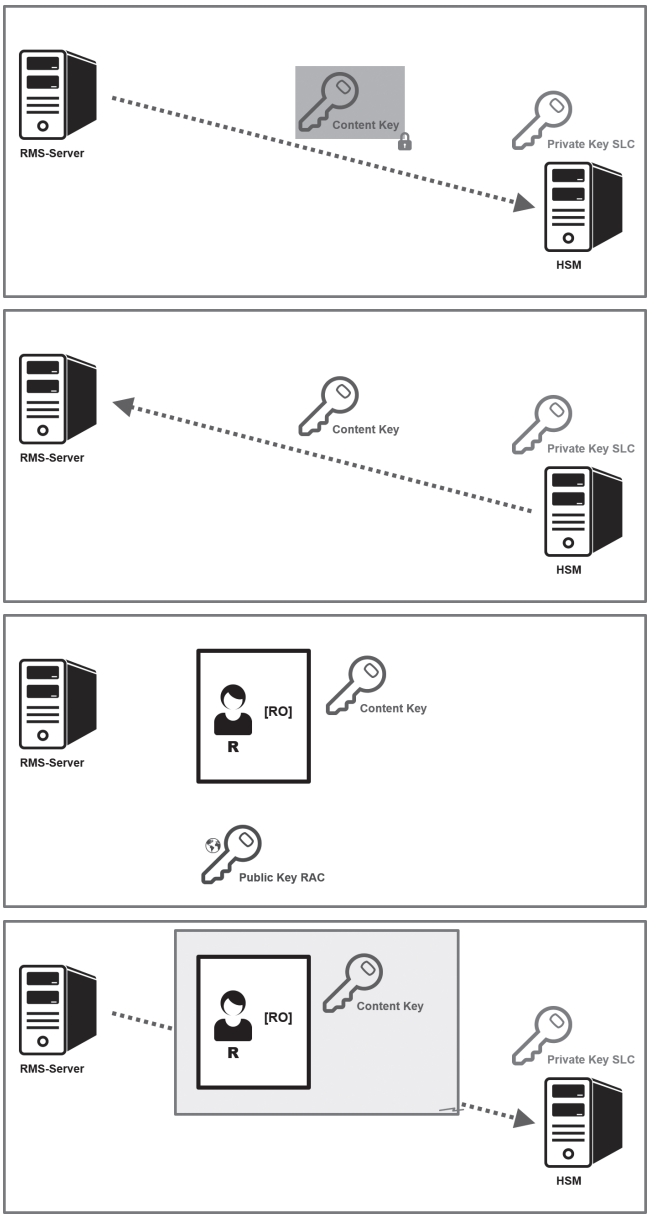
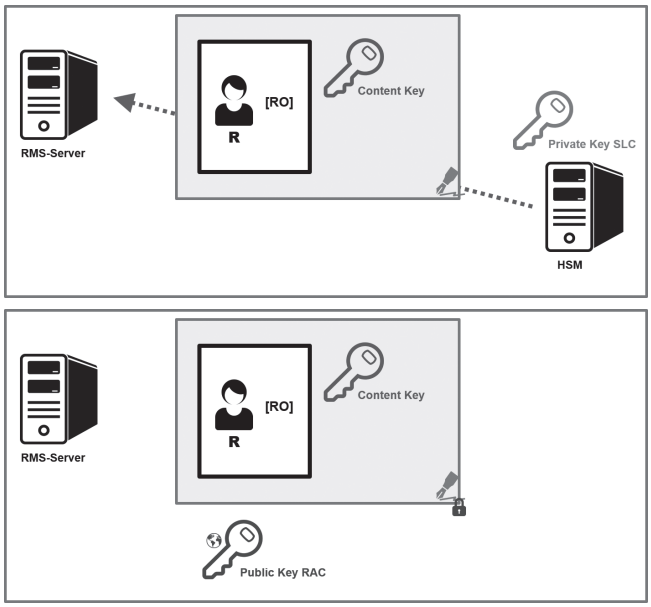


Abbildung 17 - 18 | Entschlüsseln – RSM, HSM



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).

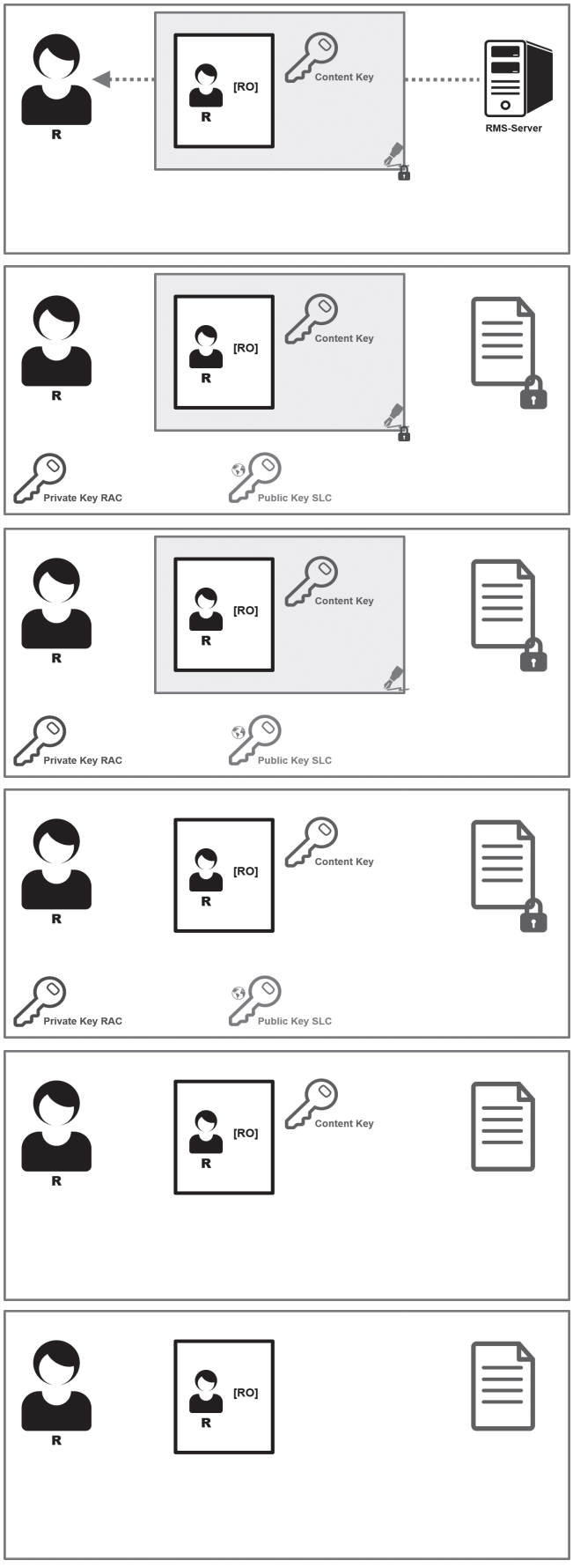
3.5 Zurück zum Empfänger

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).

Abbildung 19 - 24 | Entschlüsseln – Zurück zum Empfänger



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.

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 – beispielsweise 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.