Bild: fi Quelle: Lonely - Fotolia

Cloud-Dienstleister als hohes Datensicherheitsrisiko

Mit der Forcierung ihrer Internet-Geschäfte gewinnen die Cloud-Provider als Serviceleister für die Unternehmen an Bedeutung. Viele Internet-Größen aus den USA, oft im Verbund mit so genannten neutralen Analystenhäusern, werden nicht müde, die Wolke als Verarbeitungs- und Datenvermittler in den siebten Himmel zu heben. Um so tiefer könnten die Unternehmen, was die Sicherheit ihrer Daten und Compliance betrifft, mit einer falschen Wahl des Cloud-Dienstleisters künftig abstürzen.

Nach Dr. Thomas Lapp, Rechtsanwalt und Vorsitzender der Nationalen Initiative für Informations- und Internet-Sicherheit (NIFIS), ist Cloud-Computing zweifelsohne ein großer Technologiesprung, was eine effiziente und ressourcenschonende Datenverarbeitung betrifft. „Aber", fügt er hinzu, „es ist dringend notwendig, die damit verbundenen Gefahren zu sehen und zu reagieren." Besonders gefährlich für Unternehmen könne Cloud-Computing dann sein, wenn die Dienstleister, die die Server betreiben, aus den Vereinigten Staaten oder Großbritannien stammten. Die Daten der Unternehmen seien dann durch unmittelbare Zugriffe der Geheimdienste bedroht. Das gelte auch für Daten, die außerhalb der Vereinigten Staaten durch Cloud-Provider aus anderen Ländern gespeichert werden. „Auch dann verschafft sich die US-Regierung mit Verweis auf den Patriot-Act Zugriff auf die Daten, sofern dieser Dienstleister in den Vereinigten Staaten über eine Tochtergesellschaft verfügt", warnt Lapp. Dies alles sei ohne Richtervorbehalt und ohne Einschränkung schon bei bloßem Verdacht auf eine schwere Straftat möglich.

Dass Geheimdienste wie die NSA und GCHQ progressiv Industriespionage betreiben und die Terroristenbekämpfung nur als Deckmantel nutzen, steht seit den Enthüllungen von Edward Snowden und weiteren Enthüllungen der letzten Zeit außer Zweifel. Cloud-Dienstleister als geschäftliche Mittler für Unternehmen sind für die Geheimdienste eine ideale Bezugsquelle. Darüber können auch Beteuerungen der Cloud-Dienstleister aus den Vereinigten Staaten und Großbritannien, die Daten ihrer Kunden seien bei ihnen sicher, nicht hinwegtäuschen. Denn was außerhalb ihrer Verfügungsgewalt liegt, können sie auch nicht garantieren. Die große Gefahr, dass sich Geheimdienste sensibler Kundendaten bemächtigen, kann komplette Sicherheitsstrategien und Sicherheitsvorkehrungen der Unternehmen ad absurdum führen. In der Folge könnten mit einer falschen Wahl von Cloud-Dienstleistern ihre Geschäfte bald in eine gefährliche Schieflage geraten.

Die Vorbehalte gegenüber den Cloud-Dienstleistern, die mehrheitlich aus den USA stammen oder zumindest dort eine Tochtergesellschaft unterhalten, wächst bereits. NIFIS ist in einer aktuellen Studie den Ängsten deutscher Unternehmen auf den Grund gegangen. 58 Prozent von ihnen erachten das Hacken externer Clouds als ihr größtes Sicherheitsrisiko. An zweiter Stelle, 51 Prozent, folgt die Befürchtung, die Kontrolle über die Daten zu verlieren, wenn diese auf externen Servern verarbeitet werden. Auch der Aspekt „Kontrollver-

lust“ trifft die Unternehmen ins Mark ihrer digitalen Geschäfte. Nicht der Cloud-Dienstleister, sondern das Unternehmen haftet dafür, dass die Daten compliant behandelt werden. Steht die Sicherheit der Daten auf der Kippe, kippt auch Compliance, und die Unternehmen sind die Gelackmeierten.

Compliance war angesichts dieser rechtlichen Ausgangssituation schon zu Zeiten des klassischen IT-Outsourcing für Unternehmen ein schwieriges Unterfangen, obwohl die Anforderungen zu dieser Zeit deutlich geringer waren. In Zeiten des Cloud-Computing, gestiegener Anforderungen und wachsender Industriespionageaktivitäten kann der Anspruch, compliant sein zu müssen, für die Unternehmen in einem Debakel enden, mit allen damit verbundenen negativen wirtschaftlichen und Imagefolgen.

Hinzu kommen bei den Cloud-Providern, unabhängig von ihrer Provenienz, die Risiken, die Unternehmenskunden drohen, wenn vor allem die NSA systematisch vorgearbeitet hat. Mathias Hein, freier IT-Berater in Neuburg an der Donau und mit Angriffsformen der NSA wohl vertraut, nennt sie:

- von den US-Herstellern aufgedeckte Verschlüsselungsalgorithmen, die es der NSA ermöglichen, heute die meisten verschlüsselten Datenströme on the fly wie Klartext mitzulesen,
- sich direkt oder auf dem Graumarkt beschaffte Software-Schwachstellen, die rigoros für Ausspähungen und sonstige Hacking-Angriffe ausgenutzt werden,
- Hintertüren, die im Quellcode von US-Software versteckt sind, über die nach Bedarf Trojaner und andere Malware eingeschleust wird,
- Updates und Upgrades von US-Software, mit denen sich die Cloud-Provider mit oder ohne ihr Wissen nachträglich Ausspähprogramme und sonstige Malware ins Haus holen.

„Und einmal drin“, so der IT-Berater, „können digitale Prozesse sogar sabotiert werden.“ Diese Gefahren drohten zwar direkt auch den Unternehmen. „Doch Cloud-Provider als Mittler für Unternehmenskunden sind für die NSA als Industriespionagequelle deutlich ergiebiger.“ Je mehr marktbedeutende Unternehmen der Cloud-Dienstleister bediene, um so größer sei für die Kunden die Ausspähgefahr. Er warnt die Unternehmen außerdem vor US-Offerten, die vor Advanced-Persistent-Threats (APTs) schützen sollen, unabhängig davon, ob sie im Unternehmen oder beim Cloud-Dienstleister eingesetzt werden. „Diese Sicherheitssoftware ist eine ursprüngliche Entwicklung des US-Militärs. Dass die darin eingesetzten Methoden genau die Angriffsformen aufdecken, mit denen die NSA aktuell ausspioniert, darf bezweifelt werden.“

Die Gefahr, dass in die Cloud ausgelagerte Daten dort ausgespäht werden, ist schon deshalb groß, weil jenseits der Unternehmensgrenzen der eigene Einfluss- und Verfügungsbereich endet. Werden externe Administratoren korrumpiert, erfahren die Unternehmensverantwortlichen davon in der Regel nichts, auch weil der Cloud-Dienstleister ansonsten um seine Reputation und Geschäfte fürchten müsste. Auch die Gefahr der Korruption ist höher als innerhalb des eigenen Unternehmens. Das liegt daran, dass in der Cloud der Personenkreis mit Administrationsaufgaben größer und die Aussicht der Geheimdienste auf fette Beute verlockender ist. Außerdem war es noch nie so einfach wie heute, Daten und Systeme quasi im Vorbeigehen über Funk zu manipulieren und zu sabotieren. Die dafür notwendigen Internet-of-Things-(IoT-)Geräte sind frei im Markt erhältlich.

Was mit den eigenen Daten in den Clouds passiert, ist für die Unternehmen

funkschau EXPERTENKOMMENTAR

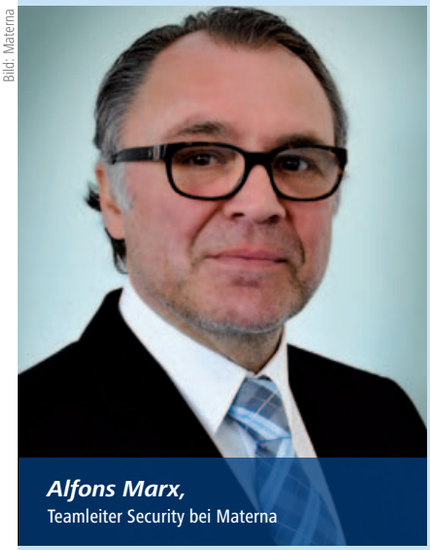

Bild: Materna

Alfons Marx,
Teamleiter Security bei Materna

Aggressive Industriespionage

Die Dienste externer Clouds in Anspruch zu nehmen, war für Unternehmen noch nie so risikoreich wie heute. Aus Sicht der Unternehmen sind alle Verbindungen nach außen potenzielle Einstiegspunkte für Ausspähungen. Dabei sind Internet-, mobile und Provider-Verbindungen besonders gefährdet. Aber auch fernab des Unternehmensnetzes werden an zentralen Knotenpunkten Telefon- und Datenleitungen von Geheimdiensten wie der NSA und der britischen GCHQ angezapft. So als wäre dies nicht genug, zwingen die Vereinigten Staaten mit dem Patriot-Act US-Cloud-Provider weltweit dazu, bei Verdacht auf eine Straftat Kundendaten in unverschlüsselter Form den US-Behörden preiszugeben.

Damit sind Cloud-Provider mit US-, aber auch mit britischer Provenienz, für Unternehmen nur noch dann eine tragfähige Dienstleistungsalternative, wenn die Daten für die Öffentlichkeit bestimmt sind. Die Unternehmen kommen somit nicht umhin, ihre Datenbestände zu sichten und zu analysieren, um so die Spreu – Daten, die problemlos nach draußen gegeben werden können – vom Weizen – Daten, die das eigene Unternehmen nicht verlassen sollten – zu trennen. Gleiches gilt für den Datenaustausch mit Geschäftspartnern. Auch in dieser Konstellation sollten Unternehmen kritisch hinterfragen, welche Daten die Grenzen des eigenen Unternehmens überschreiten können und welche nicht. Für Daten, die, obwohl sensibel, ausgetauscht werden müssen, um durchgehende Geschäftsprozesse aufrechtzuerhalten, wird das führende Unternehmen seine Geschäftspartner verstärkt in die Absicherungspflicht nehmen müssen. Dies könnte soweit führen, dass Partner, die sich die zusätzlichen Investitionen in die IT-Sicherheit nicht leisten können oder wollen, aus Geschäftsverbünden ausgeschlossen werden. In der Automobilindustrie ist diese Entwicklung bereits voll im Gange.

Die Unternehmen sollten außerdem ihre Zugriffskonzepte, sowohl intern als auch remote, kritisch überdenken. Wer braucht welche Zugriffsrechte auf welche Anwendungen und Daten, um seine Aufgaben zu erfüllen, und welche nicht? Zugriffssparsamkeit sichert nicht nur einzelne Datenbestände besser ab. Sie begrenzt auch im Fall der Inanspruchnahme eines US-Cloud-Anbieters die Auditierungs- und Anwendungsdaten ein – wer hat wann worauf zugegriffen –, die gegebenenfalls US-Behörden übergeben werden müssen.

Die aktuelle Entwicklung macht wenig Hoffnung, dass sich die Ausgangssituation für die Unternehmen verbessern wird. Die Unternehmen werden sich wohl auf Dauer auf aggressive Industriespionage einstellen und darauf mit veränderten Datenhaltungs- und Sicherheitskonzepten reagieren müssen. Ob Cloud-Provider unter der Kandare von Geheimdiensten künftig für Unternehmen noch eine große Rolle spielen werden, scheint deshalb fraglich. Europäische Unternehmen sollten bevorzugt zertifizierte europäische Cloud-Dienstleister mit durchgängiger Verschlüsselung nutzen.

funkschau EXPERTENKOMMENTAR

Bild: Blue Elephant Systems

Joachim Hörnle,
Geschäftsführer von Blue Elephant Systems

Unternehmen haften für Governance, Risiko-Management, Compliance

Die Ausspähungen der Geheimdienste, allen voran der NSA, belasten das Cloud-Computing. Es fällt schwer, gerade US-Cloud-Providern, aber auch britischen Cloud-Anbietern, zu glauben, dass sie unter Offenbarungsdruck durch die Geheimdienste sorgsam mit den Daten der Unternehmenskunden umgehen. Zumal US-Cloud-Anbieter, nicht nur in den USA, sondern auch in anderen Ländern, aufgrund des Patriot-Act keine Wahl haben. Sie müssen schon bei bloßem Verdacht auf eine Straftat die Daten ihrer Kunden als Klartext offenlegen. Damit können Unternehmenskunden auch den Verschlüsselungen, die US-Provider einsetzen, nicht vertrauen.

Den Unternehmen, die dennoch die Dienste externer Clouds – öffentlicher, virtueller privater und hybrider Clouds – in Anspruch nehmen wollen, um so beispielsweise Kosten einzusparen, kommen somit nicht umhin, sich die Anbieter und ihr Herkunftsland genau anzuschauen. Außerdem sind die Unternehmen mit externen Cloud-Ambitionen gefordert, ihre Datenbestände genau zu sichten und zu hinterfragen, wie kritisch sie für das Geschäft sind. Sind die Daten weniger schutzbedürftig, können sie getrost in externe Clouds ausgelagert werden, unabhängig vom Herkunftsland des Anbieters, weil nichts geheim gehalten werden muss. Bei allen anderen Daten ist höchste Vorsicht geboten. In diesem Fall sollten nur vertrauenswürdige und von Geheimdiensten nicht herangezogene Dienstleister ausgewählt werden. Zum Schutz sensibler Daten sollte außerdem darauf geachtet werden, dass die Daten innerhalb des EU-Rechtsraums verarbeitet werden. Denn nicht der Cloud-Dienstleister, sondern das Unternehmen haftet dafür, dass die Vorschriften und Regeln bezüglich GRC (Governance – Risiko-Management – Compliance) eingehalten werden.

Für die Auslagerung von Daten in externe Clouds ist aber nicht nur die Vertrauenswürdigkeit des Dienstleisters bestimmend. Er muss darüber hinaus Anforderungen erfüllen wie eine schnelle Provisionierung, eine hinreichende Integration seiner IT-Management-Dienste sowie eine transparente Informationsgabe. Die schnelle Provisionierung und Dekommissionierung von Cloud-Diensten mit den dazugehörigen Komponenten ist erforderlich, weil der Lebenszyklus der Dienste, also ihre Relevanz für die Unternehmenskunden, immer kürzer ausfällt, sie außerdem auf eine wirtschaftliche Dienstebereitstellung dringen. Beides, wiederum, ruft förmlich nach einer höheren Integrationstiefe des IT-Managements, sowohl auf der Seite der Cloud-Provider als auch im Zusammenspiel mit der Unternehmens-IT. Ohne die deutlich höhere Informationstransparenz der Cloud-Anbieter kann kein Unternehmen seinen GRC-Anforderungen nachweislich nachkommen. In diesem Kontext wird ein semantisches IT-Management immer mehr an Bedeutung gewinnen, damit beide Seiten immer vom selben sprechen und die Informationen gleich bewerten.

funkschau EXPERTENKOMMENTAR

Bild: Evidian

Erwin Schöndlinger,
Geschäftsführer von Evidian Deutschland

Identity-Federation schirmt Daten ab

Mit dem Einbezug externer Clouds wird IAM (Identity- and Access-Management) und Identity-Federation für Unternehmen immer wichtiger. Identity-Federation als Erweiterung des IAM-Systems eröffnet einen sicheren, domänenübergreifenden Datenaustausch und allseits abgeschirmte Anwendungen und Datenbestände. Außerdem ermöglicht Identity-Federation, die sichere Zugriffskontrolle per SSO (Single-Sign-on) auf beliebig große Organisationsverbünde auszudehnen. Natürlich greift über Federation-Protokolle wie SAML (Security-Assertion-Markup-Language) der SSO auch gegenüber Anwendungen und Datenbeständen, die innerhalb externer Clouds angesiedelt sind. Benutzer, die sich innerhalb ihrer Domäne authentisiert und dadurch den SSO ausgelöst haben, müssen sich für den Zugriff auf Anwendungen und Daten anderer Domäne nicht erneut authentisieren. Voraussetzung dafür ist, dass die beteiligten Domänen, beispielsweise die von Cloud-Providern, vorab als Trusted-Domains definiert worden sind.

Neben dem barrierefreien, aber abgesicherten Zugriff auf Anwendungen und Daten anderer Domänen, erschließt die Identitäten-Föderation kombiniert mit dem SSO dem Unternehmen einen weiteren Vorteil: Sie können innerhalb der Gesamtkonstellation die Administration von Benutzern und ihren Zugriffsrechten flexibel delegieren, dadurch ihre eigenen Administrationsaufwendungen herunterfahren. Allerdings setzt die Definition von externen Trusted-Domains sowie die flexible Delegation der Administration von Benutzern und ihren Zugriffsrechten voraus, dass das Unternehmen dem IdP (Identity-Provider) und den Cloud-Providern, die die Anwendungen und Daten vorhalten, vertrauen können muss. So sollte der IdP, der die Authentisierung von Benutzern übernimmt und damit über SAML den SSO und die Zugriffskontrolle einleitet, kein Anbieter sein, der einem Geheimdienst zuarbeiten muss. Das gleiche gilt für den Cloud-Provider: Dort sind die Zugriffsberechtigungen der Benutzer in den Anwendungskonten hinterlegt. Diese Vorsichtsmaßnahmen sollten Unternehmen schon deshalb beherzigen, weil ansonsten auf Verlangen des Geheimdienstes auch die Auditierungsdaten – wer hat wann worauf zugegriffen? –weitergegeben werden. Nur wenn Unternehmen auf Seiten des IdP und des Cloud-Providers vor den Machenschaften von Geheimdiensten gefeit sind, können Unternehmen ihre GRC-(Governance-, Risiko-Management- und Compliance-)Anforderungen nachkommen. Nicht die Cloud-Anbieter, sondern das Unternehmen haftet dafür, dass gesetzliche Vorschriften und Regelungen bei der externen Speicherung und Verarbeitung von Daten nachweislich eingehalten werden.

ohnehin kaum mehr transparent. Das liegt an den nebulösen Wolkengebilden wie Public-, Hybrid- und so genannten Virtual-Private-Clouds. Wo und in welchem Land die Daten im einzelnen verarbeitet, gespeichert und gegebenenfalls abgegriffen werden, ist für die Dateneigner nicht mehr nachvollziehbar. Die Folge: Die Unternehmen setzen über externe Clouds buchstäblich die Vertraulichkeit und Integrität ihrer Daten aufs Spiel. Compliance, für die sie in der Haftung stehen, ist für sie nicht mehr darstellbar, von einer nachweislichen Befolgung der Datenschutzgesetze ganz zu schweigen. Die von Rechtsanwalt Lapp eingeräumte große Technologiesprung, eine effiziente und ressourcenschonende Datenverarbeitung, offenbart so seine hässlichen Schattenseiten: mangelnde Datensicherheit und unzureichende Compliance. Beides kann im schlimmsten Fall das Unternehmen schnell ins geschäftliche Aus katapultieren.

Um so erstaunlicher ist es, dass Cloud-Anbieter, oft verbandelt mit Analysten, dem Cloud-Computing weiterhin große Wachstumschancen einräumen. Sie versuchen mit allen Mitteln, ungeachtet der vielen Gefahren, die ihren Kunden drohen, die Vermarktungsmaschinerie immer wieder anzuheizen, damit sich ihre bereits getätigten Investitionen rentieren. Das ist beim Cloud-Anbieter CWCS Managed Hosting nicht anders. Der britische Cloud-Provider, der zudem mit einer Tochtergesellschaft in den Vereinigten Staaten vertreten ist, gehört zum Kreis der Anbieter, denen Unternehmen aufgrund der Hintergrundaktivitäten von NSA und GCHQ mit äußerster Vorsicht begegnen sollten. Mit Blick auf das Geschäft sieht CWCS natürlich den Markt für Cloud-Computing weiter wachsen, was der Anbieter mit eigenen Hochrechnungen zu hinterlegen versucht. Danach sollen bereits in 2016 weltweit zwei Drittel aller Data-Workloads auf Servern, positioniert in externen Clouds, verarbeitet werden. Doch selbst CWCS räumt ein, dass dann der Business-Bereich (596 Exabytes) gemessen am Workload nur ein Sechstel des Consumer-Bereichs (3.659 Exabytes) ausmachen werde.

Die Marktrealität könnte in 2016 ganz anders aussehen, wenn die Geheimdienste weiterhin, wovon auszugehen ist, rigoros ausspähen werden. Zumal aus Deutschland und Europa heraus kaum politischer Druck aufgebaut wird. Die Unternehmen werden, schon zur eigenen Sicherheit, vermehrt Cloud-Dienstleistern die kalte Schulter zeigen und sich auf eine Verarbeitung der Daten innerhalb des eigenen Unternehmens zurückbesinnen. Denn sie werden zunehmend erkennen: Solange Monopolisten und zwangsrekrutierte Geheimdienstgehilfen wie Microsoft und Intel, Google, Apple, IBM & Co. den ITK-Markt prägen werden, wird es – Big Brother is Watching You – für Unternehmen keine Sicherheit ihrer Daten und Geschäftsgeheimnisse mehr geben.

Mittlerweile registrieren auch die US-Technologiegrößen selbst, dass ihnen im Ausland mit den harschen Gesetzen des eigenen Landes beim Cloud-Computing bald die Felle wegschwimmen könnten. Das Ansinnen von Microsoft und vier anderen großen US-Technologieunternehmen, die Regierung der Vereinigten Staaten habe kein Recht dazu, sich der Kundendaten außerhalb der USA zu bemächtigen, ist allerdings vor Gericht gescheitert. Jetzt fürchtet Microsoft: „Wenn sich diese Entwicklung fortsetzt, könnte dies weltweit das Geschäft von Cloud-Providern, die Unternehmenskunden bedienen, substanziell unterhöhlen."

Hadi Stiel,
Freier Journalist und Kommunikationsberater
in Bad Camberg

funkschau EXPERTENKOMMENTAR

Bild: KPMG

Marc Ennemann,
Partner im Bereich Consulting bei KPMG

Schützenswerte Daten sollten den EU-Rechtsraum keinesfalls verlassen

Der Patriot-Act gilt für alle US-Provider weltweit, also auch, wenn sie für Unternehmenskunden Daten innerhalb ihrer Rechenzentren außerhalb der USA vorhalten. Diese Dienstleister müssen Maßnahmen zur Umgehung der eingesetzten Verschlüsselungen sicherstellen, damit sie bei entsprechendem Beschluss die Daten im Klartext aushändigen können. Aktuelle Beispiele aus der Praxis machen deutlich, dass die Online-Service-Anbieter sogar ihren privaten SSL- (Secure-Socket-Layer-)Schlüssel an die staatlichen US-Behörden aushändigen müssen. Deren Ziel ist es, alle vom Dienstleister verarbeiteten Metadaten in Echtzeit zu verarbeiten, zu analysieren und auszuwerten.

Die Konsequenzen aus solchen Auflagen für Unternehmen sind offensichtlich: Selbst durch den Einsatz starker Verschlüsselungsverfahren sind die Daten gewerblicher und privater US-Anbieter nicht geschützt, weil die Schlüssel an die US-Behörden weitergegeben werden. Zwar bleibt den Unternehmenskunden auf den ersten Blick die Alternative, ihre eigene Ende-zu-Ende-Verschlüsselung einzusetzen. Doch auch diese Alternative haben die Unternehmen oftmals nicht, weil die gehosteten Anwendungen meist keine private End-to-End-Verschlüsselung einräumen. Hinzu kommt, dass die Geheimdienste, allen voran die NSA, weite Strecken der interkontinentalen Kommunikationsverbindungen kontrollieren, teilweise sogar kompletter Staaten, wie der Bahamas und des Oman.

Die Bedrohung für die Unternehmensdaten durch den Provider dazwischen muss demzufolge als außerordentlich hoch eingestuft werden. Das gilt besonders für US-Provider. Unternehmen, die ihre Daten sicher speichern wollen, müssen deshalb selbst initiativ werden und neue Cyber-Schutzkonzepte entwickeln und umsetzen. Die eigene private Cloud und einzelne Sicherheitsprodukte reichen aufgrund der Komplexität und Vielfältigkeit der Bedrohungen nicht aus. Gefordert ist stattdessen eine strikte Befolgung von IT-Security/Governance-Grundsätzen, um die Wirksamkeit der getroffenen Maßnahmen zu erhöhen und die Kosten für diese Maßnahmen in Grenzen zu halten. Dazu muss jedes Unternehmen im Vorfeld den Schutzbedarf für seine Datenbestände analysieren und im einzelnen die erforderlichen Schutzmaßnahmen festlegen. Eine Regel, die unbedingt befolgt werden sollte: Vertrauliche und unternehmenskritische Daten (Information-Assets) sollten nie außerhalb Europas verarbeitet und gespeichert werden. Die beiden Ausnahmen von dieser Regel: Global operierende Unternehmen kommen oft nicht an US-Clouds vorbei. Daten mit geringem Schutzbedarf und niedriger Risikoklassifizierung können auch in Clouds außerhalb der EU verarbeitet und gespeichert werden. Doch bereits Daten mit mittlerem Schutzbedarf sollten den EU-Rechtsraum keinesfalls verlassen.