Datenfilter für die Cloud

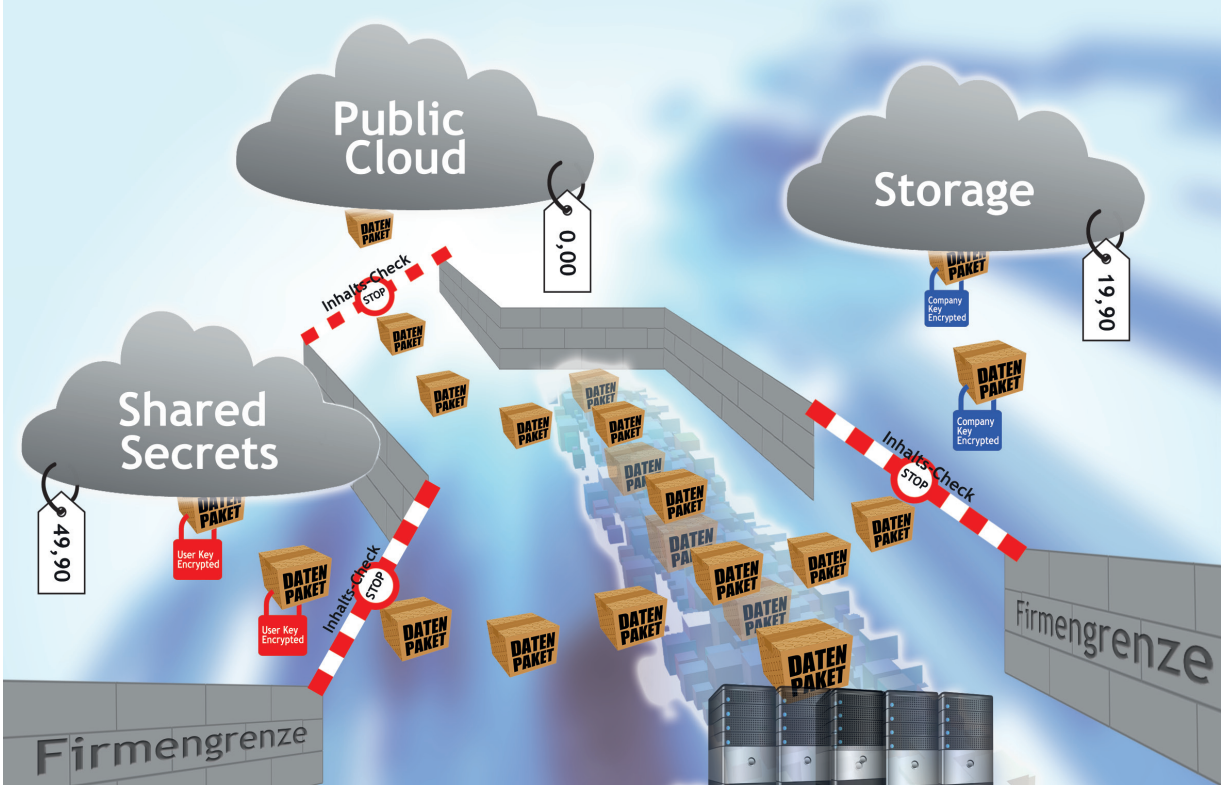
Schwarz-Weiß-Lösungen passen nicht zum Cloud-Computing

„Cloud oder nicht Cloud" ist die falsche Frage – eine „vollständig sichere Wolke" die falsche Forderung. Entscheidend ist, was wo gespeichert und wie verarbeitet wird – daher sind Modelle zur Klassifikation und Verschlüsselung von Daten gefordert, um eine passende Auswahl und zusätzliche Sicherung von Cloud-Angeboten zu ermöglichen.

Von Ramon Mörl, München

Die Cloud ist bequem: Datenzugriffe überall ermöglichen, Zugriffe gezielt an Kollegen, Partner, Kunden oder Interessierte weltweit weitergeben, synchronisieren von Arbeitsumgebungen – Cloud-Angebote machen das möglich – überall. Der Preis für diese „Convenience" kann aber hoch sein, wenn man Sicherheitsdefizite in Kauf nimmt: Das Risiko, dass ungewollt unberechtigte Dritte ebenfalls Zugriff auf firmeneigene Daten bekommen, ist hoch. Hier gilt es jedoch, nicht schwarzweiß zu malen und die Cloud für alles oder gar nichts zuzulassen, sondern eine geschickte Balance zwischen Convenience und Sicherheit zu finden.

Denn in jedem Unternehmen gibt es unkritische Daten, deren „Verarbeitung" mit beliebigen Anwendungen in der Cloud unproblematisch ist. Daneben gibt es Daten, deren Verarbeitung unter bestimmten rechtlichen Auflagen an Dritte ausgelagert werden darf – aber auch Daten, die das Verantwortungsgebiet des Unternehmens nicht verlassen sollten oder sogar dürfen. Statt pauschal eine „sichere Cloud" zu fordern, können konkrete Sicherheitsanforderungen an vorher klassifizierte Daten und die darauf zugelassenen Verarbeitungsverfahren geknüpft werden. Falls rechtlich zulässig, kann ein Unternehmen dann auch seine Daten durch geeignete Service-Level-Agreements (SLAs) absichern. Die SLAs beschreiben grundsätzlich, welche



Gleichmacherei ist beim Cloud-Computing fehl am Platze – so wie es verschiedene Cloud-Angebote mit unterschiedlichen Sicherheitslevels gibt, haben auch Unternehmensdaten verschiedene Sicherheitserfordernisse. Hier gilt es, passende Kombinationen aus Services, Daten und Sicherheitsmechanismen zu nutzen.

Leistungen der Cloud-Anbieter zu erbringen hat und wie diese abgerechnet werden – Faktoren wie Verfügbarkeiten, Garantien, Reaktionszeiten und auch Angaben zu Sicherheitsstandards können Teil solcher Vereinbarungen sein.

Um Convenience gegen Sicherheit abzuwägen gilt es daher zuerst zu verstehen, wo Verallgemeinerungen zulässig sind und an welchen Stellen auf eine feine Granularität zu achten ist (vgl. Kasten „Goldene Regeln…"). Schon vielfach implementierte Verfahren aus der DLP-Welt können dann ebenfalls eine gute Lösung bieten. Die sieben goldenen Regeln im Umgang mit der Cloud liefern eine gute Motivation für eine Echtzeitklassifizierung der Daten zur Verarbeitung in unterschiedlichen Cloud-Systemen.

DLP hilft

Mit den Bordmitteln der Betriebssysteme ist dieser Gefährdungslage weder auf Clients noch auf Servern beizukommen – um der Convenience Rechnung zu tragen, ist allerdings der direkte Zugriff vom Client oder sonstigen Endgerät des Nutzers wünschenswert. Data-Leakage-Prevention (DLP) für die Cloud sollte deshalb ganz organisch am Endpunkt angesiedelt werden: Das heißt DLP-Systeme, die an den File-Schnittstellen von Clients und Servern die Daten inhaltlich prüfen und im Zweifelsfall eine Echtzeitklassifizierung anstoßen, stellen hier die geeignete Lösung dar – sofern sie die folgende Anforderungen erfüllen:

_____ Plug-in-Fähigkeit, also eine Möglichkeit, kundenspezifische Anbindungen und Klassifizierungsmodelle einfach per Standardschnittstelle einzubinden,
_____ direkte Reaktion auf verschiedene Cloudsysteme und die dafür zur Verfügung stehenden Anwendungen (z. B. Drop Box),
_____ hinreichende Flexibilität, sprich: als Ergebnis einer inhaltlichen Prüfung von Dokumenten nicht nur ein „erlaubt" oder „verboten" – also eine Schwarz-weiß-Entscheidung – zu liefern, sondern eine beliebig komplexe automatisierte Handlungskette ermöglichen, die beispielsweise Monitoring und Verschlüsselung am Client umfassen kann.

Diese Anforderungen vergrößern zwar die DLP-Problematik um eine weitere Dimension, aber so kann

Goldene Regeln für sicheren Umgang mit der Cloud

_____ Die Cloud als sicherer Datenspeicher ist kein Problem, wenn geeignete Verschlüsselung angewendet wird. Das gilt für Firmendaten, wenn sie mit Firmenschlüsseln verschlüsselt sind, die nicht von Dritten gebrochen werden können. Daten können also immer in die Cloud verlagert werden, wenn die Ver- und Entschlüsselung auf firmeneigenen sicheren Rechenkernen stattfindet und die entschlüsselten Daten das sichere Firmennetz nicht mehr verlassen.

_____ Alle Services rund um die Schlüssel zur Sicherstellung der Vertraulichkeit in der Cloud, also deren Generierung, Verwaltung, Nutzung et cetera, gehören *nicht* in die Cloud, wenn die damit geschützte Information nicht-delegierbare Risiken birgt.

_____ Schlüssel unterschiedlicher Qualität sollten zum Einsatz kommen: Zum einen Firmenschlüssel, die niemandem (auch nicht der IT-Abteilung des Unternehmens) im Klartext vorliegen, zum anderen beliebige bilateral mit Kunden, Partnern oder anderen Kommunikationspartnern verhandelte oder ausgetauschte Krypto-Keys – beim Austausch Letzterer müssen sichere Verfahren verwendet werden.

_____ Feldspezifische Verschlüsselungen in gemeinsam benutzten Cloud-Anwendungen (z. B. Doodle) sind häufig trügerisch, da sich allein durch die Existenz der Daten schon wesentliche Rückschlüsse ziehen lassen oder häufig die „Convenience" schon verloren geht, wenn es um ganz natürliche Sortierfunktionen und Anordnungen geht.

_____ Applikationen sollten aus der Cloud nur dann in die sichere Firmeninfrastruktur „eingelassen" werden, wenn ihre Integrität bewiesen ist, da sich sonst Schadcode aus der Cloud in die Anwendung eingenistet haben könnte.

_____ Software-as-a-Service (SaaS) liefert „Software aus der Cloud" – ein Sicherheitsproblem beginnt, wenn die Daten und die Applikationen in der Cloud zusammentreffen, also potenziell gefährdete Daten mit potenziell unbekannten Anwendungen auf fremden „Rechenkernen" verarbeitet werden, auf welche die Cloud-Betreiber administrativen Zugriff haben. Das Problem: Daten können von Anwendungen nur im Klartext verarbeitet werden. Daten, die in die Cloud zur Verarbeitung gehen, müssen also zur Verarbeitung in der Cloud entschlüsselt werden oder schon im Klartext übertragen werden – in diesen Verarbeitungsmodus sollten daher nur Daten gehen, die keinen Vertraulichkeitsanforderungen unterliegen.

_____ Nicht vergessen: Die Haftung für Sicherheitsdefizite (z. B. für die Vertraulichkeit personenbezogener Daten von Dritten) kann *nicht* delegiert oder über Verträge auf Dritte (z. B. Cloud-Anbieter) abgegeben werden.

man zur Sicherung von Cloud-Services die gleichen Lösungen einsetzen, die bisher Daten überwachen, die via USB-Sticks und traditionellen Anwendungen das Unternehmen verlassen.

Und so kann ein Unternehmen genau bestimmen, welche Daten für welche spezifischen Cloud-Anbieter, -Services oder auch eine Public Cloud geeignet sind. „Die Cloud" als solche wird dazu filigraner unterteilt, um ein genaues Bild der Verfügbarkeit, der SLAs und der Kosten zu erstellen – so lassen sich gute Skalierungseffekte und Kostenstrukturen der Cloud nutzen, ohne die Sicherheit zu gefährden.

Echtzeitklassifizierung

Hat ein Unternehmen noch keine durchgängige Klassifizierung seiner Daten vorgenommen, dann kann eine Echtzeitklassifizierung helfen: Häufig ist das Vertrauen in bestimmte Anwendergruppen und langjährige Mitarbeiter groß, sodass man ihnen die Wahl der richtigen Klassifikation von Daten – also die Einstufung ihrer Kritikalität – durchaus zutraut. In diesem Fall bietet sich eine Dialogsteuerung an: Der Anwender klassifiziert dann die in die Cloud ausgelagerten Daten in Echtzeit. Die Klassifizierung und der gesamte Vorgang wird mit den beteiligten Informationen protokolliert und lässt sich später beliebig in vordefinierten Reports auswerten. Anschließend können auch Anwendergruppen mit geringerem Vertrauenslevel die – dann bereits klassifizierten – Daten in der Cloud ihren Zugriffsrechten gemäß weiterverarbeiten.

Fazit

Sicherheit in der Cloud kann mit Methoden der Data-Leakage-Prevention problemlos am Endpunkt und am Server umgesetzt werden, ohne etwa Firewall-Systeme mit zu viel Kontextabhängigkeit zu belasten. Ein passendes DLP-Verfahren gewährleistet die Kontrolle des Datenflusses von der „eigenen Umgebung" in verschiedene Cloud-Services oder auch virtualisierte Umgebungen. Eine filigrane Einteilung der Cloud und ihrer Nutzung sowie die Echtzeitklassifikation von nach außen gehenden Daten, die in der Cloud gespeichert oder verarbeitet werden sollen, helfen dabei, die passenden Maßnahmen zum Schutz zu finden. Durch entsprechende Klassifikationen bestimmen die Daten dann entlang ihrer Kritikalität selbst die Umgebung, in der sie wie (nur verschlüsselt, gespeichert oder für bestimmte Anwendungen „sichtbar" …) verarbeitet werden dürfen. ■

Ramon Mörl ist Geschäftsführer der itWatch GmbH.