Security Insider

eBook

Datensicherheit in der Cloud

Sicherheit von Cloud-Diensten richtig bewerten und konsequent überwachen

Vogel Business Media

Powered by: Fabasoft

Inhalt

Powered by:

Fabasoft

Fabasoft Distribution GmbH
Honauerstraße 4, 4020 Linz, Austria
Tel. +43 732 606162 -0
www.foliocloud.com
E-Mail: sales@foliocloud.com

Vogel IT-Medien GmbH
August-Wessels-Str. 27, 86156 Augsburg
Telefon +49 (0) 821/2177-0
E-Mail redaktion@security-insider.de
Web www.Security-Insider.de
Geschäftsführer: Werner Nieberle
Chefredakteur: Peter Schmitz, V.i.S.d.P., peter.schmitz@vogel-it.de
Erscheinungstermin: Mai 2013
Titelbild: bannosuke - Fotolia.com

Vogel Business Media

Cloud-Sicherheit von Anfang an

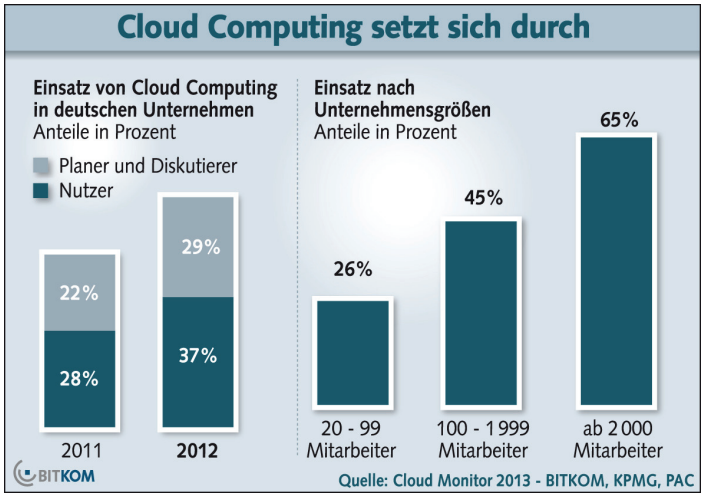
Worauf es bei der Cloud-Sicherheit ankommt

Die Sicherheit in der Cloud beginnt nicht in der Wolke, sondern am Schreibtisch des Nutzers. Der Cloud-Anbieter muss richtig ausgewählt und überwacht werden.

Bereits 37 Prozent der deutschen Unternehmen setzen Cloud Computing ein. Das Ergebnis des Cloud-Monitors 2013 des Hightech-Verbands BITKOM und der Wirtschaftsprüfungs- und Beratungsgesellschaft KPMG zeigt, dass Cloud Computing bei Unternehmen immer beliebter wird.
Die Vorteile einer Cloud wie flexible Nutzung, schneller Einstieg und mögliche Kostenersparnis dürfen aber nicht über die Herausforderungen hinweg täuschen: Cloud Computing befreit von vielem, nicht aber von der Verantwortung für Datenschutz und Datensicherheit.

Cloud-Anbieter nicht alleine in der Pflicht

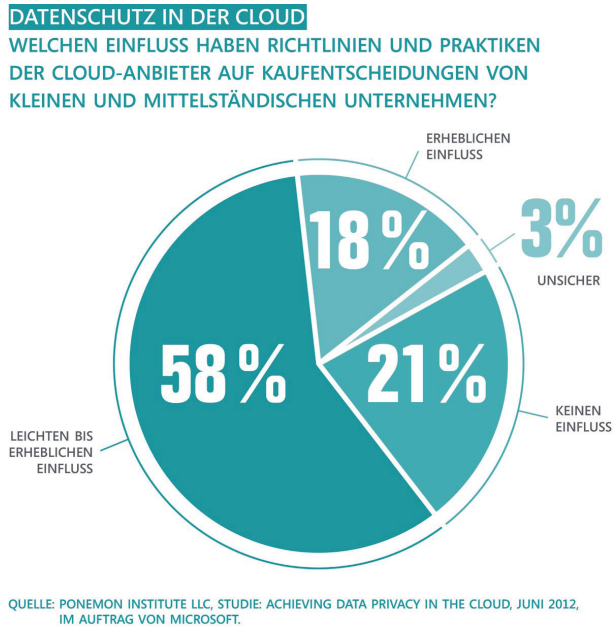
Leider machen es sich manche Unternehmen zu einfach, wenn sie Cloud Computing einführen. So zeigt die Ponemon-Studie „Encryption in the Cloud“, dass 46 Prozent der Unternehmen, die bereits sensible oder vertrauliche Daten in eine Cloud-Umgebung übertragen haben, der Meinung sind, vor allem der Cloud-Anbieter sei für den Datenschutz verantwortlich.
Dieses Missverständnis geht so weit, dass zwei Drittel der Befragten erklärten, sie wüssten nicht, welche Maßnahmen ihr Cloud-Anbieter zum Schutz der ihm anvertrauten Daten ergreift. Damit bewegen sich diese Unternehmen auf sehr dünnem Eis: Cloud Computing stellt datenschutzrechtlich in aller Regel eine Form von Auftragsdatenverarbeitung dar. Deshalb sind die Unternehmen verpflichtet, die Sicherheitsmaßnahmen des Cloud-Anbieters vor Auftragsvergabe und danach regelmäßig zu überprüfen.



Laut Cloud Monitor 2013 nutzen 65 Prozent der Großunternehmen ab 2.000 Mitarbeitern Cloud Computing, im Mittelstand mit 100 bis 1.999 Mitarbeitern waren es 45 Prozent, bei kleineren Unternehmen mit 20 bis 99 Beschäftigten ein Viertel (Bild: BITKOM).

Cloud-Risiken erkennen und abwehren

Laut der Ponemon-Untersuchung „Achieving Data Privacy in the Cloud“ hat der Datenschutz, den ein Cloud-Anbieter anbietet, bei 76 Prozent der Unternehmen Einfluss auf die Kaufentscheidung. Ob die Sicherheitsmaßnahmen des Cloud-Anbieters ausreichen oder nicht, hängt von dem Schutzbedarf der Daten und den ermittelten Cloud-Risiken ab, denen begegnet werden muss. Den individuellen Schutzbedarf der Daten muss jedes Unternehmen für sich bestimmen. Welche Risiken mit einer Cloud verbunden sein können, wurde unter anderem von ENISA (European Network and Information Security Agency) dargestellt.



Das Datenschutzniveau eines Cloud-Anbieters ist für die Nutzer durchaus wichtig bei der Entscheidung. Allerdings müssen Cloud-Nutzer auch wissen, wie sie das Datenschutzniveau eines Cloud-Providers bewerten können (Bild: Microsoft).

Insbesondere der mögliche Kontrollverlust über die eigenen Daten, die Unkenntnis, wo sich die Daten befinden, und die Schwierigkeiten, die gesetzlichen Compliance-Vorgaben nachweisbar umzusetzen und selbst ein Audit bei dem Cloud-Anbieter zu machen, bereiten Kopfzerbrechen. Hier sind Lösungen gefragt, die die Cloud-Nutzung für den Anwender transparenter machen. Verschiedene Möglichkeiten werden in diesem eBook näher vorgestellt, darunter die Verwendung von Cloud-Logging, die richtige Bewertung von Cloud-Zertifikaten und das Aufdecken von Cloud-Vorfällen.

Interne Sicherheit nicht vergessen

Bei all den Kontrollpflichten gegenüber dem Cloud-Anbieter sollten aber die eigenen Maßnahmen für die Datensicherheit nicht aus dem Blick geraten. Diese beginnen mit der regelmäßigen Aktualisierung von Browsern, die in der Regel für den Cloud-Zugang genutzt werden, beinhalten die Verwendung einer professionellen Anti-Viren-Lösung auf allen Endgeräten, die für den Cloud-Zugriff genutzt werden – also auch Smartphones und Tablets, und schließen die mögliche, zusätzliche Verschlüsselung der Daten vor einer Übertragung in die Cloud ein.

Dabei müssen die internen Sicherheitsmaßnahmen aber zu Ende gedacht werden: Die zuvor zitierte Ponemon-Studie zur Cloud-Verschlüsselung zeigt auch, dass selbst von den Unternehmen, die ihre Daten selbst verschlüsseln, mehr als die Hälfte die Kontrolle über das Schlüsselmaterial dem Cloud-Anbieter übertragen. Hier stellt sich dann die Frage, wie der Cloud-Anbieter die Kundenschlüssel vor einem Zugriff durch das eigene Personal schützt. Eine Frage, die wieder der Cloud-Nutzer beantworten können muss, wenn es zum Beispiel zu einer Kontrolle durch die Aufsichtsbehörde für den Datenschutz kommt.

Oliver Schonschek

Logging vom Netzwerk bis in die Cloud

Wie man die Sicherheit des Cloud-Providers überwachen kann

Den meisten Cloud-Nutzern sind Kontrollen beim Provider vor Ort nicht möglich. Ein Ausweg kann die Ausweitung der Netzwerkprotokollierung in die Cloud sein.

Wenn es um die Verfügbarkeit des Cloud-Dienstes geht, haben viele Nutzer gut daran getan, ihre Anforderungen vertraglich festzuhalten: Laut der ENISA-Umfrage „Survey and analysis of security parameters in cloud SLAs“ sind die Verfügbarkeitsanforderungen bei 75 Prozent der Befragten Vertragsbestandteil, 78 Prozent haben zudem vereinbart, bei Störungen informiert zu werden.

Doch die Umsetzung in der Praxis sieht anders aus: Nur 15 Prozent der befragten Cloud-Nutzer erhalten tatsächlich Berichte zur Verfügbarkeit. Ohne entsprechende Berichte ist allerdings weder die gesetzlich vorgesehene Überwachung der Cloud-Sicherheit machbar, noch lassen sich die erforderlichen Gegenmaßnahmen bei einem Cloud-Ausfall zeitnah einleiten.

Cloud-Provider bieten Dashboards

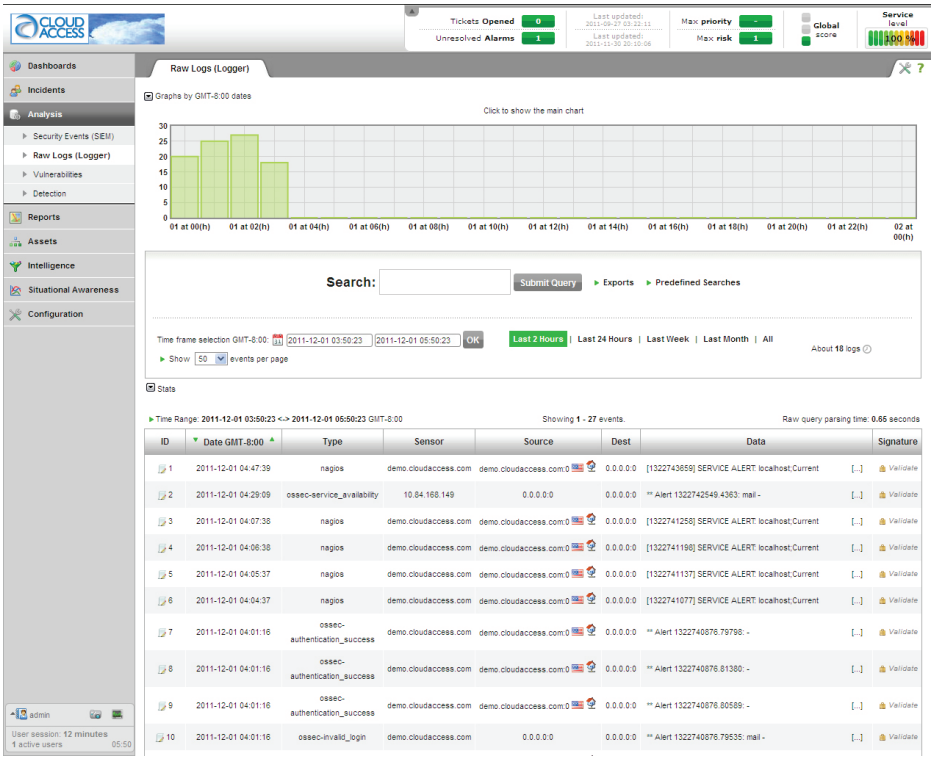
Eine wichtige Informationsquelle für Cloud-Nutzer können die Dashboards sein, die viele Provider mit grundlegenden Systemdaten öffentlich anbieten. Kundenindividuelle Dashboards und Berichte stehen nach der Anmeldung zur Verfügung. Je nach Anbieter können für individuelle Berichte jedoch Zusatzkosten entstehen. So sind zum Beispiel bei Amazon CloudWatch eine bestimmte Zahl Metriken, Abfragen und Alarmdienste ohne weiteres Entgelt verfügbar, zusätzliche werden abgerechnet.
Microsoft bietet für Windows Azure ein Dashboard, das den aktuellen Status der verschiedenen Cloud-Dienste zeigt. Auch Daten zu abgelaufenen Zeiträumen lassen sich abfragen. Nutzer können die Meldungen zu den sie betreffenden Diensten über RSS (Really Simple Syndication) abonnieren.

Empfehlung: Protokollieren wie im eigenen Netzwerk

Für den erforderlichen Umfang und Inhalt der Statusberichte gibt es einen guten Maßstab: Da die Cloud-Dienste genauso sicher genutzt werden können sollten wie das interne Netzwerk des Anwenderunternehmens, sollte auch die Protokollierung für die Cloud so aussagekräftig sein wie die eigene Netzwerkprotokollierung.
Was liegt da näher, als die im Netzwerk eingesetzten Logging-Systeme auf die Cloud auszuweiten, wenn dies möglich ist. Oder aber man erweitert die eigene Logging-Lösung um eine Cloud-Komponente.

Tibco LogLogic LogManagement Intelligence zum Beispiel kann als Appliance betrieben werden, um neben den internen IT-Systemen auch die genutzten Cloud-Dienste in die Protokollierung und Analyse zu integrieren. Je nach Appliance können bis zu 250.000 Events pro Sekunde verarbeitet werden, ob aus dem eigenen Rechenzentrum oder der Cloud.

Das Cloud-Logging kann auch selbst als Cloud-Dienst bezogen werden, zum Beispiel mit CloudAccess Log Management. Die cloud-basierte Logging-Lösung kann für Public und Private Clouds eingesetzt werden.



Logging-Lösungen wie CloudAccess LogManagement bieten Cloud-Nutzern die Möglichkeit, selbst eine Protokollierung der Cloud-Aktivitäten vorzunehmen. CloudAccess LogManagement ist selbst Cloud-basiert und kann entsprechend schnell eingerichtet werden (Bild: CloudAccess).

Cloud-Logging richtig nutzen

Eine Kontrolle der Cloud-Sicherheit ist im bestimmten Maße mit Hilfe von Cloud-Logging möglich. Voraussetzung ist zum einen, dass keine entscheidenden Sicherheitsparameter fehlen. Hinweise zu den wichtigen Sicherheitsparametern liefert zum Beispiel der ENISA-Leitfaden „Procure Secure“.

Des Weiteren müssen Cloud-Protokolle genauso behandelt werden wie andere Systemprotokolle, sie müssen also insbesondere regelmäßig ausgewertet, vor Manipulationen geschützt und für spätere Analysen lange genug aufbewahrt werden.

Oliver Schonschek

Hilfe bei der Suche nach sicheren Cloud-Lösungen

Was sagen Cloud-Zertifikate aus und was nicht

Cloud-Nutzer müssen sich von den Sicherheitsmaßnahmen des Anbieters überzeugen. Dabei können Zertifikate helfen, wenn die Vergabekriterien stimmen.

Bevor man sich für einen Cloud-Anbieter entscheidet, sollte man nicht nur den Funktionsumfang des Cloud-Dienstes und die Kosten hinterfragen. Auch die Sicherheitsmaßnahmen des Cloud-Providers müssen überzeugend sein, schließlich vertraut man dem Anbieter mehr oder weniger vertrauliche Unternehmensdaten an.

Welche Sicherheitsmaßnahmen bei dem Cloud-Provider nicht fehlen sollten, das wurde unter anderem vom Bundesamt für Sicherheit in der Informationstechnik (BSI, Sicherheitsempfehlungen für Cloud Computing Anbieter) und von der European Network and Information Security Agency (ENISA, Cloud Computing Information Assurance Framework) zusammengestellt. Werden personenbezogene Daten in die Cloud verlagert, sollte zudem der Beschluss des Düsseldorfer Kreises „Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing“ Beachtung finden.

Cloud-Zertifikate geben Orientierung

Kaum ein Cloud-Anwender wird jedoch in der Lage sein, selbst alle Sicherheitseigenschaften des geplanten Cloud-Dienstes zu überprüfen. Die von den Aufsichtsbehörden für den Datenschutz herausgegebene Orientierungshilfe Cloud Computing verweist deshalb auf die Bedeutung von geeigneten Cloud-Zertifikaten. Sie entbinden den Cloud-Nutzer zwar nicht von seinen Kontrollpflichten, doch Cloud-Zertifikate können eine wichtige Informationsquelle bei der Beurteilung der Cloud-Sicherheit sein. Auch die genannten Empfehlungen des BSI besagen zum Beispiel, dass der Cloud-Anbieter „vorzugsweise nach ISO 27001 auf Basis von IT-Grundschutz oder einem anderen etablierten Standard zertifiziert sein sollte“.

Die Checklisten, die Cloud-Anbieter im Rahmen der Zertifizierung für das Siegel „Trust in Cloud“ ausfüllen, werden mit den Ergebnissen veröffentlicht. Dies sorgt für mehr Transparenz bei Cloud-Angeboten und damit für mehr Vertrauen bei den Anwendern (Bild: Cloud-EcoSystem e.V.).

Cloud-Zertifikate richtig interpretieren

Die Analysten von Gartner gehen davon aus, dass im Jahre 2016 40 Prozent der Unternehmen auf unabhängige Cloud-Zertifikate achten, wenn ein neuer Cloud-Dienst ausgewählt werden soll. Schon heute gibt es eine ganze Reihe von Cloud-Gütesiegeln und -Zertifikaten. Die Aussagekraft der Zertifikate ist allerdings unterschiedlich und sollte durch das Anwenderunternehmen jeweils hinterfragt werden.

1. Cloud-Zertifikate auf Basis einer Selbstauskunft

Die Open Cloud Business Initiative (OCBI) hatte ein „Open-Cloud-Zertifikat" vorgestellt, welches besagt, dass der betreffende Cloud-Anbieter seine Konformität zu den Prinzipien der OCBI erklärt hat. Eine externe Prüfung war dabei nicht vorgesehen. Bei einem solchen Gütesiegel liegt somit eine Selbstauskunft zugrunde und kein externes Audit.

Cloud-EcoSystem e.V. bietet ein Cloud-Zertifikat namens „Trust in Cloud". Basis der Zertifizierung ist die Überprüfung der Antworten, die der Cloud-Anbieter auf einem Fragebogen unter anderem zur Datensicherheit gegeben hat. Wenn falsche Angaben im Fragebogen gemacht werden, kann das Zertifikat aberkannt werden. Eine Vor-Ort-Prüfung ist in den Zertifikatsbedingungen nicht genannt. Die Antworten zum Fragebogen werden veröffentlicht, was die Transparenz des Cloud-Anbieters erhöht.

Beim EuroCloud Star Audit SaaS prüfen unabhängige Auditoren Cloud-Anbieter in den Bereichen Vertrag und Compliance, Sicherheit, Betrieb und Infrastruktur, Prozesse, Anwendung und Implementierung (Bild: EuroCloud Deutschland_eco).

2. Cloud-Zertifizierung mit Vor-Ort-Kontrolle

Das „EuroCloud Star Audit" zum Beispiel sieht detaillierte Anforderungen an Datenschutz und Datensicherheit des Cloud-Anbieters vor, abhängig von der Anzahl der im Zertifikat genannten Sterne (maximal fünf). Die Kriterien zur Zertifizierung enthalten unter anderem eine Vor-Ort-Begehung durch externe Auditoren. Ein weiteres Beispiel für eine Zertifizierung, die auch eine Vor-Ort-Prüfung des Cloud-Anbieters beinhaltet, ist die Zertifizierung Cloud Security von TÜV Rheinland.

Fazit: Cloud-Standards müssen vereinheitlicht werden

Bereits diese Beispiele zeigen, wie unterschiedlich Cloud-Zertifikate zu bewerten sind. Damit Cloud-Nutzer leichter Cloud-Angebote vergleichen und die Cloud-Sicherheit einschätzen können, sollten zumindest auf europäischer Ebene die zahlreich vorhandenen Cloud-Standards harmonisiert werden. Entsprechende Initiativen laufen bereits, unter anderem bei The European Telecommunications Standards Institute (ETSI). Dadurch würde die Transparenz bei den Cloud-Angeboten deutlich steigen, eine wichtige Maßnahme zur weiteren Vertrauensbildung bei den Cloud-Anwendern.

Oliver Schonschek

Spuren in der Cloud sind flüchtig

Sicherheitsvorfälle in Clouds aufdecken

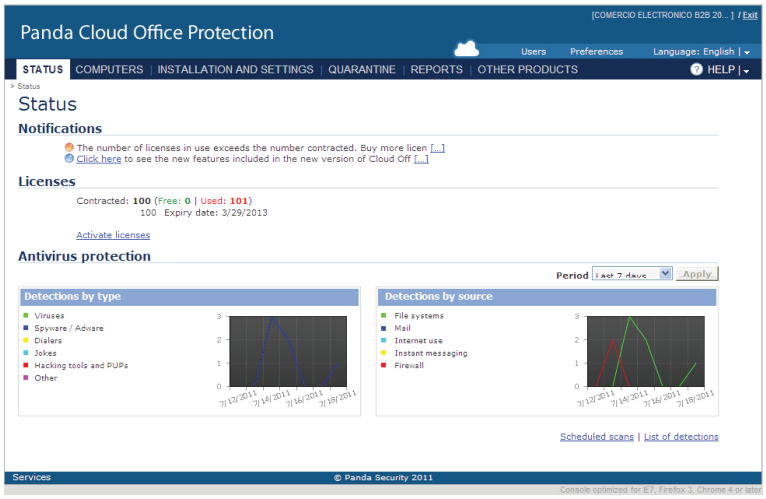
Werden Daten aus der Cloud gestohlen, müssen die digitalen Spuren schnell gesichert werden. Doch die Forensik in der Cloud ist vielschichtig.

Der aktuelle „State of Cloud Security Report“ von Alert Logic berichtet von über 45.000 Sicherheitsvorfällen. Die häufigsten Angriffstypen auf Cloud-Umgebungen waren demnach Versuche, Cloud-Zugänge zu knacken, das Ausnutzen von Schwachstellen in Cloud-Applikationen und Malware-Attacken. Alert Logic stellt in dem Bericht fest, dass Clouds nicht generell unsicherer sind als selbst betriebene Server und Anwendungen, denn die Systeme in den Unternehmen erfahren ähnliche Angriffe. Doch aus Sicht der IT-Forensik gibt es deutliche Unterschiede zwischen der Spurensuche in der Cloud und in eigenen IT-Systemen.

Spurensuche mit Hindernissen

Gibt es den Verdacht, dass Daten missbraucht oder gestohlen wurden, lassen sich in selbst betriebenen Systemen forensische Analysen durchführen. Im Fall von Cloud-Daten ist dies nicht so einfach. Die betroffenen Daten befinden sich auf Systemen Dritter, die im Fall von Public Clouds auch von anderen Nutzern verwendet werden. Ein Sicherstellen der betroffenen Datenspeicher wie im Fall einer lokalen Spurensuche ist nicht ohne weiteres möglich.

Auch die Auswertung der Systemprotokolle kann nicht so einfach erfolgen. Zum einen sind Unternehmen ohne eigenes Cloud-Logging von den Protokollen des Cloud-Anbieters abhängig. Zum anderen müssen die Protokolle des Cloud-Providers so gefiltert werden, dass nur die Aktivitäten zu sehen sind, die das jeweilige Unternehmen und seine Nutzer betreffen. Gerade bei der Verwendung von Public Clouds sind deshalb auch andere Untersuchungsmethoden gefragt.



Wird der betriebliche Internetzugang abgesichert, können Lösungen wie Panda Cloud Internet Protection auch Cloud-Zugriffe aufzeichnen und in forensischen Analysen bereitstellen. Mögliche Innentäter, die Daten in eine Cloud ausschleusen, könnten so aufgespürt werden (Bild: Panda Security).

Indirekte Spurensuche notwendig

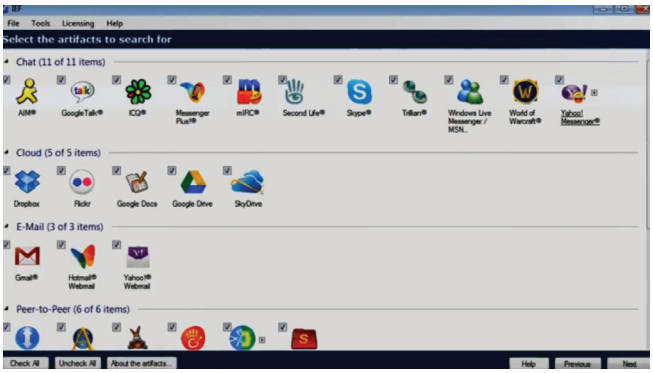
Neben den Sicherheitsberichten des Cloud-Anbieters gibt es andere Hilfsmittel bei der digitalen Spurensuche in der Cloud: Besteht der Verdacht, dass einer der eigenen Mitarbeiter Cloud-Daten missbraucht hat, hilft die zentrale Absicherung der Internetaktivitäten im Unternehmen. Internet Security Gateways protokollieren die Internetzugriffe der Nutzer und damit auch die Cloud-Zugriffe, wenn dafür ein Gerät aus dem Firmennetzwerk genutzt wird. Ein Ausschleusen von vertraulichen Daten in die Cloud könnte so ebenfalls registriert werden wie ein heimliches Herunterladen von Cloud-Daten. Die Protokolle der eigenen Internetsicherheitslösung werden dann zu einem Augenzeugen-Bericht für Cloud-Vorfälle.

Digitale Spuren auf Smartphones

Mobile Endgeräte nutzen jedoch oftmals einen eigenen Internetzugang und könnten sich so der durchgehenden Überwachung durch ein Internet Security Gateway entziehen. Doch die mobile Cloud-Nutzung hinterlässt Spuren auf den Smartphones selbst.
Die Studie „Using Smartphones as a Proxy for Forensic Evidence contained in Cloud Storage Services“ von der University of Glasgow ergab, dass sich die mobile Nutzung bestimmter Cloud-Speicher-Dienste nachvollziehen lässt. Werden über ein Firmen-Smartphone unerlaubt Daten in eine Cloud verschoben, könnte dies in den dazu genutzten Smartphone-Apps nachweisbar sein.

Speziallösungen für Cloud-Untersuchungen

Neben der indirekten Spurensuche über intern betriebene Sicherheitslösungen und auf den Endgeräten gibt es auch Lösungen, die speziell die IT-Forensik in Cloud-Umgebungen unterstützen: Mit Cloud Audit von CipherCloud zum Beispiel lassen sich alle lesenden und schreibenden Cloud-Zugriffe aufzeichnen. Im Verdachtsfall kann der einzelne Cloud-Nutzer zu einer bestimmten Aktivität ermittelt werden, mit Zeitangaben, durchgeführten Aktionen und betroffenen Cloud-Daten. Der Internet Evidence Finder (IEF) von Magnet Forensics sucht mögliche Spuren einer Datenverbindung zu bestimmten Cloud-Diensten wie Dropbox, Carbonite, Skydrive, Google Docs und Google Drive.



Eine Lösung wie der Internet Evidence Finder (IEF) hilft dabei, die Cloud-Nutzung zu rekonstruieren. Dazu werden die Endgeräte, die für den Cloud-Zugriff verwendet wurden, auf Spuren untersucht, die zum Beispiel bei der Verwendung von Dropbox lokal entstehen können (Bild: Demo Magnet Forensics).

Fazit: Cloud-Sicherheit ist Trumpf

Auch bei der Cloud-Sicherheit bewahrheitet es sich, dass Vorbeugen immer besser ist. Cloud-Nutzer sollten es erst gar nicht zu einem Sicherheitsvorfall in der Cloud kommen lassen, indem sie einen zuverlässigen, sicheren Cloud-Anbieter auswählen und ihre Verantwortung für den Datenschutz ernst nehmen. Eine Überwachung der Cloud-Aktivitäten mittels Cloud-Logging, die richtige Bewertung von Cloud-Gütesiegeln bei der Wahl des Cloud-Anbieters und ein Notfallkonzept, wie man Sicherheitsvorfälle in der Cloud schnell aufspüren kann, gehören dazu. *Oliver Schonschek*

Lösung: Folio Cloud von Fabasoft

Business in der Cloud braucht Sicherheit und Vertrauen

Cloud Computing bietet effiziente Möglichkeiten für Zusammenarbeit und Informationsaustausch im B2B-Bereich. Viele neue Cloud-Angebote werfen allerdings Sicherheitsfragen auf. Folio Cloud dagegen gibt Antworten.

Sicherheit auf Ebene des Teams

Die Zusammenarbeit in Folio Cloud basiert auf „Teamrooms“. Auf dieser Ebene werden auch die Zugriffsrechte vergeben. Nur Kontakte, die eine Einladung erhalten und sich für den Zugriff authentifizieren, gelangen in den Teamroom. Wie die Authentifizierung erfolgt, kann individuell festgelegt werden – per E-Mail-Adresse und Passwort, Zwei-Faktor-Authentifizierung oder über digitale Identitäten (neuer deutscher Personalausweis, österreichische Bürgerkarte bzw. Handy-Signatur oder SuisseID). Bei der Kommunikation sind die Inhalte verschlüsselt.

Compliance auf Dokumentebene

Nachvollziehen, was mit Dokumenten in Folio Cloud passiert? Neben Auditing und durchgängiger Versionierung der Änderungen unterstützt Folio Cloud das Anbringen von nicht entfernbaren, dynamischen Wasserzeichen. Damit wird ein völlig neues Sicherheitsniveau erreicht. Selbst wenn Dokumente aus dem Teamroom entfernt werden, ist jederzeit eindeutig nachvollziehbar, woher das Dokument stammt und wer es exportiert oder gedruckt hat. Teammitglieder, die nur Leseberechtigung haben, erhalten statt des Dokuments automatisch eine PDF-Version mit definiertem Wasserzeichen und anderen Sicherheitsmerkmalen.

Wahlfreiheit und Gewissheit über den Standort der Datenhaltung

Je umfassender die Möglichkeiten der Zusammenarbeit, umso wichtiger ist die Frage des Speicherortes und die physische Greifbarkeit. Folio Cloud bietet dafür eine Wählbarkeit des Speicherortes. Sie bestimmen, wo die Datenspeicherung erfolgt: in Hochsicherheits-Rechenzentren in Deutschland, Österreich oder der Schweiz.

Transparenz schafft Vertrauen

Folio Cloud ist zertifiziert nach ISO 20000 und geprüft nach ISAE 3402 Type 2. Unter http://trust.fabasoft.com finden Sie einen umfassenden Überblick, welche Maßnahmen Fabasoft für die Datensicherheit in der Cloud bietet.