

# RSA Security Brief

November 2009



## Cloud Computing – mit Sicherheit

Best Practices für  
vertrauenswürdige Umgebungen

### Autoren

Eric Baize  
Senior Director, Secure Infrastructure Group,  
EMC Corporation

Roland Cloutier  
Chief Security Officer, EMC Corporation

Bret Hartman, Chief Technology Officer  
RSA, The Security Division of EMC

Dr. Stephen Herrod  
Chief Technology Officer und Senior Vice President R&D,  
VMware, Inc.

Chuck Hollis  
Vice President und CTO Global Marketing,  
EMC Corporation

Uri Rivner  
Leiter New Technologies, Identity Protection &  
Verification  
RSA, The Security Division of EMC

Ben Verghese  
Chief Management Architect & Senior Director, R&D,  
VMware, Inc.



The Security Division of EMC

RSA Security Briefs bieten führenden Sicherheitsunternehmen und Führungskräften wichtige Leitlinien für dringliche Risiken in der Informationssicherheit und zeigen neue Möglichkeiten auf. Jeder Brief wird von einem ausgewählten Team aus Sicherheits- und Technologieexperten verschiedener Unternehmen erstellt, die ihr Expertenwissen zu einem wichtigen aktuellen Thema mitteilen. RSA Security Briefs beleuchten nicht nur das Gesamtbild, sondern bieten auch praktische technologische Beratung. Sie zählen zur Pflichtlektüre für moderne, zukunftsorientierte Sicherheitsunternehmen.

## Inhalt

---

Cloud-Gestaltung: Überblick Cloud Computing	3
Cloud-Steuerung: Überblick Cloud Sicherheit	3
Cloud-Beziehungen: Wer ist vertrauenswürdig?	4
1. Aufstellen und Durchsetzen klarer Richtlinien für die Vertrauensdefinition	6
2. Halten Cloud-Anbieter, was sie in Sachen Sicherheit versprechen?	6
3. Transparenz im Cloud-Betrieb für Mandantenfähigkeit und Datenisolation	6
4. Funktionstrennung für Administratoren	7
5. Richtlinienverwaltung für die Bereitstellung virtueller Maschinen	8
6. Datenverschlüsselung und Tokenisierung	8
7. Anwendung von Richtlinien für domainübergreifende Identitäten und starke Authentifizierungsmethoden	9
Fraud Protection: Schutz vor unerwünschten Besuchern	9
1. Implementierung starker Authentifizierungsdienste	10
2. Verschiedene Abwehrmechanismen zum Schutz vor ausgeklügelten Malware-Angriffen	11
3. Cyber-Kriminalität	11
Datenkonformität im Cloud Computing	12
1. Compliance-Prüfung für Cloud-Anbieter	12
2. Einhaltung rechtlicher Vorgaben in offenen Clouds	12
Übersicht	13
Über die Autoren	16
Cloud-Lösungen: Leitlinien für Experten im Bereich Identitäts- und Datenschutz im Cloud Computing	17
Überwachung von Rechenzentren und Mandantenfähigkeit	17
Datenverschlüsselung und Tokenisierung	17
Gemeinsame Verwaltung digitaler Identitäten	17
Starke, risikobasierte Authentifizierung	18
Fraud Prevention und Malware-Erkennung	18
Cloud Event Management und Audits	19
Schutz vor Datenverlust (DLP)	19
Einhaltung von Compliance-Anforderungen in offenen Clouds	19

## Cloud-Gestaltung: Überblick Cloud Computing

---

Cloud Computing ermöglicht den bequemen, bedarfsgerechten Zugriff auf gemeinsam genutzte Daten, Anwendungen und Hardware über das Internet. Cloud Computing wird durch ausgereifte Automatisierungs-, Bereitstellungs- und Virtualisierungstechnologien ermöglicht. Es unterscheidet sich deutlich von konventionellen IT-Modellen, da Daten und Software von den zugrundeliegenden Servern und Speichersystemen entkoppelt sind und sämtliche IT-Ressourcen als Service bereitgestellt werden. Dies geschieht entweder in Form von Komponenten, bei denen der Anwender bestimmte Anwendungen abonniert oder Rechenleistung mietet, oder als integriertes Ganzes.

Aus gutem Grund wurde viel über Cloud Computing diskutiert. Diese Technologie hat das Potenzial, die IT in Unternehmen drastisch zu verändern. Genauso, wie die meisten Menschen wohl meinen, dass das Reisen mit herkömmlichen Fluggesellschaften effizienter und praktischer ist als der Betrieb einer eigenen Fluglinie, stellt die Bereitstellung von IT-Funktionen mittels Cloud Computing für viele Unternehmen eine effizientere, bequemere und vor allem flexiblere Möglichkeit dar, eigene private Netzwerke, Server und Software zu besitzen und zu unterhalten.

Ob bewusst oder nicht, viele Unternehmen nutzen bereits einen Teil ihrer IT und Geschäftsfunktionen nach dem Modell des Cloud Computing. Beispielsweise laufen Anwendungen für den Vertrieb oder das Customer Relationship Management als Cloud-Service, oder Lohnbuchhaltung und andere vertrauliche Unternehmensfunktionen wurden an Experten außerhalb des Unternehmens vergeben, die Software als Service im Cloud Computing nutzen. Offenbar sind Unternehmen, die dem Cloud Computing skeptisch gegenüberstehen, oft weniger um die Technologie oder physische Unterschiede besorgt als um die Unterschiede im Hinblick auf Verfahren und Richtlinien.

Cloud Computing setzt vielen herkömmlichen physischen Einschränkungen ein Ende, die den Datenbestand von Unternehmen definieren und schützen. Physische Server werden durch virtuelle ersetzt. Die Sicherheit erfolgt nicht allein durch Firewalls, sondern auch durch den Datenverkehr auf virtuellen Maschinen. Die Komplexität der Risikofaktoren nimmt zu, da durch Cloud Computing ständig wachsende, kurzlebige Kontrollketten für vertrauliche Unternehmensdaten und -anwendungen entstehen.

Durch das Migrieren ihrer IT-Infrastruktur in ein Cloud-Modell geben Unternehmen teilweise die Kontrolle über ihre Informationsinfrastruktur und Prozesse ab, obwohl sie verpflichtet sind, verantwortlich mit Datenschutz und Compliance umzugehen. Die Folgen dieses Trends wirken sich auf zahlreiche Akteure in Unternehmen aus, besonders jedoch auf Führungskräfte, die für die Informationssicherheit verantwortlich sind.

## Cloud-Steuerung: Überblick Cloud-Sicherheit

---

Unternehmen setzen verstärkt auf Cloud Computing, aber dennoch herrscht Unsicherheit darüber, wie die Informationssicherheit im Cloud-Modell optimal gehandhabt werden sollte. Im RSA-Bericht [As Hyper-extended Enterprises Grow, So Do Security Risks\\*](http://www.rsa.com/innovation/docs/IDG_ResearchWhitePaper_Final_060409.pdf) (Englisch) räumten zwei Drittel der Befragten, die Anwendungen oder Geschäftsprozesse nach dem Cloud-Modell betreiben, ein, dass sie noch keine Sicherheitsstrategie für Cloud Computing entwickelt haben. Ein Großteil der Befragten war sich nicht darüber im Klaren, wie potenzielle Cloud Computing-Anbieter Daten schützen würden und welche Maßnahmen Sicherheitsteams in Unternehmen ergreifen, um Compliance-Anforderungen auch hier gerecht zu werden.

---

**Cloud Computing setzt vielen herkömmlichen physischen Einschränkungen ein Ende, die den Datenbestand von Unternehmen definieren und schützen. Die Komplexität der Risikofaktoren nimmt zu, da durch Cloud Computing ständig wachsende, kurzlebige Kontrollketten für vertrauliche Unternehmensdaten und -anwendungen entstehen.**

---

\*[http://www.rsa.com/innovation/docs/IDG\\_ResearchWhitePaper\\_Final\\_060409.pdf](http://www.rsa.com/innovation/docs/IDG_ResearchWhitePaper_Final_060409.pdf)

Es mag für viele führende Sicherheitsunternehmen beruhigend sein, dass die Informationssicherheit im Cloud Computing sich nicht grundlegend von den Sicherheitsmaßnahmen in herkömmlichen IT-Infrastrukturen in Unternehmen unterscheidet. Anforderungen, Bedrohungen, Richtlinien und Kontrollen sowie Governance und Compliance sind identisch. Moderne Verfahren und Tools in der Informationssicherheit lassen sich ebenfalls sinnvoll weiterverwenden. Aufgrund der Unterschiede in der gemeinsamen Nutzung, Teilung, Kontrolle und Verwaltung von Cloud-Ressourcen sind jedoch einige Anpassungen in Bezug auf die Art der Anwendung bewährter Sicherheitsmaßnahmen und Tools erforderlich.

Zunächst einmal stellt Cloud Computing für die Informationstechnologie und -sicherheit eine einmalige Gelegenheit dar, die Informationssicherheit zu verbessern: schneller, kostengünstiger, effizienter und weniger invasiv. Da sich Cloud-Plattformen noch immer weiterentwickeln, gibt es unzählige Möglichkeiten, wie sich Verfahren und Technologien für die Informationssicherheit noch tiefer in die Infrastruktur integrieren lassen. Die Informationssicherheit kann sich endlich aus dem althergebrachten Modell befreien, bei dem die Sicherheit nachträglich in Form von Code in Betriebssysteme, Netzwerke und Anwendungen integriert wurde. Im Cloud-Modell lassen sich Sicherheitsprotokolle auf Virtualisierungsebene integrieren und sorgen so für leistungsstarke, unkomplizierte und doch einheitliche Sicherheitssysteme. Im Cloud Computing werden virtuelle Maschinen bewegt, die verschiedene Funktionen haben. Sie verfügen alle über integrierte Richtlinien und Schutzmaßnahmen. Die Cloud-Sicherheit birgt ein enormes Potenzial, die heute mögliche Informationssicherheit noch zu verbessern.

Für das Cloud Computing müssen führende Unternehmen im Bereich der Informationssicherheit ihre Definition der Anwenderidentitäten erweitern. IT-Transaktionen sind zunehmend automatisiert: Interaktionen zwischen Software und System ähneln heute oft denen zwischen Mensch und Maschine oder gehen gar darüber hinaus. Durch das Cloud-Modell wird dieser Trend noch verstärkt. Folglich müssen IT- und Sicherheitsprozesse die Möglichkeit berücksichtigen, dass ein Anwender in der Cloud mit großer Wahrscheinlichkeit eher eine Maschine als eine Person ist (oder eine Maschine, die für eine Person agiert). All das hat enorme Auswirkungen auf die Art der Bereitstellung, Authentifizierung und Verwaltung von Identitäten.

Des Weiteren sind Unternehmen durch das Cloud Computing gezwungen, ihre Auswahlprozesse für IT-Lösungsanbieter erneut zu prüfen und Modelle zum Vertrauensaufbau sowie mögliche Konsequenzen zu überdenken. Da sich nun Teile der unternehmensweiten IT-Infrastruktur im Besitz Dritter befinden und von Fremdanbietern betrieben werden, müssen führende Sicherheitsanbieter sicherstellen können, dass Cloud-Anbieter in der Lage sind, sowohl die physische als auch die virtuelle Infrastruktur ausreichend zu schützen. Unternehmen müssen vertrauliche Informationen auf virtuellen Servern und Datenspeichern schützen und gleichzeitig sicherstellen, dass Cloud-Administratoren über alle notwendigen Zugriffs- und Benutzerrechte verfügen. Weiterhin muss die Arbeit der Cloud-Anbieter für Unternehmen transparent sein, um vereinbarte Sicherheits- und Geschäftsprotokolle nachprüfen zu können. Unternehmen sollten deutlich machen, dass sie IT-Richtlinien und Ressourcen selbst steuern könnten – auch dann, wenn sie solche Ressourcen nicht besitzen oder direkt handhaben. Durch die wiedererlangte Steuerung von Richtlinien nehmen die Risiken des Cloud Computing nicht unbedingt zu, sondern ändern sich lediglich.

Richtlinien im Cloud-Modell betreffen üblicherweise den Aufbau vertrauenswürdiger Beziehungen zwischen Unternehmen. Diese vertrauenswürdigen Beziehungen bilden die Grundlage für die Sicherheit des Cloud Computing.

---

## Cloud-Beziehungen: Wer ist vertrauenswürdig?

---

Im Wesentlichen ist die Sicherheit im Cloud Computing keine Frage der Technologie, sondern des Vertrauens. Zahlreiche, wenn auch längst nicht alle Technologien, Services, Methoden und Know-how zum Schutz der Cloud sind bereits vorhanden und müssen lediglich vom Unternehmen auf das Cloud-Modell ausgeweitet werden. Um Cloud Computing zu einer gängigen Serviceplattform zu machen, ist größeres Vertrauen notwendig, insbesondere zwischen den Eigentümern/Anbietern von Cloud-Ressourcen und den Unternehmen, die diese Ressourcen nutzen.

### Unterschiede zwischen privaten und öffentlichen Clouds

Private Clouds beschreiben eine IT-Infrastruktur, in der sich virtualisierte Server, Storage, Netzwerke und Anwendungen eines einzigen Unternehmens befinden. Die IT-Ressourcen dieser privaten Cloud befinden sich nicht notwendigerweise im Besitz des Unternehmens und müssen nicht vom Unternehmen selbst betrieben werden. Das Outsourcing oder Mieten von Ressourcen von Cloud-Anbietern ist möglich, z.B. Rechenkapazität, die von einem externen Rechenzentrum geleast wird. Dennoch befindet sich die private Cloud tatsächlich im Besitz des Unternehmens, da es die Richtlinien erstellt und steuert, die die Handhabung der virtuellen IT-Ressourcen bestimmen. Cloud-Anbieter garantieren bestimmte Serviceleistungen und verpflichten sich, zuvor vereinbarte Standards für den Zugriff auf Informationen sowie für Sicherheit und Compliance einzuhalten.

Wenn sich alle IT-Ressourcen einer privaten Cloud im physischen Besitz eines Unternehmens befinden und vom Unternehmen selbst betrieben werden, wird die Cloud oft auch als interne Cloud bezeichnet.

Öffentliche Clouds beinhalten vergleichbare virtualisierte IT-Infrastrukturen und Services. Die Richtlinien werden hier jedoch nicht vom Unternehmen definiert und durchgesetzt. Obwohl Unternehmen öffentliche Clouds für private Geschäftsvorteile nutzen können, liegen weder Betrieb noch Zugriff und Sicherheit in der Hand des Unternehmens. Bekannte Beispiele für öffentliche Clouds sind die Elastic Compute Cloud (EC2) von Amazon, Google Apps und Salesforce.com.

Definitionen zur Sicherheitsterminologie dieses Dokuments finden Sie im entsprechenden Glossar auf der Website von RSA: <http://www.rsa.com/glossary/>

Es gibt zahlreiche Unternehmen, die Services über private und öffentliche Clouds anbieten (siehe „Unterschiede zwischen privaten und öffentlichen Clouds“ oben). Jedes hat individuelle Anforderungen an und Prozesse für die Authentifizierung und Autorisierung von Anwendern. Da diese Services miteinander verbunden sind und gemeinsam Informationen nutzen, muss jeder Serviceanbieter sicher wissen, in welchem Umfang Clouds, Services und Anwender, mit denen Transaktionen stattfinden – ganz gleich ob Mensch oder Maschine – vertrauenswürdig sind. Selbst wenn Serviceanbieter das weltweit beste Informationssicherheitssystem einsetzen, ist dieses wertlos, wenn gleichgestellten Cloud-Partnern mit niedrigeren Sicherheitsstandards der Zugriff gewährt wird.

Bei vertrauenswürdigen Beziehungen geht es um das Erstellen von Hierarchien und das Erkennen verlässlicher Partner für den geeigneten Schutz sowie die Handhabung gemeinsam genutzter Ressourcen und vertraulicher Informationen. Es geht nicht nur darum, Transaktionspartnern zu vertrauen, sondern auch darum, wie diese Partner Services und Sicherheit anbieten. Werden Erwartungen zwischen Parteien mittels domainübergreifender Identitätsverwaltung formalisiert und organisiert, ergibt sich eine sicherere Anwendergemeinde, die bequemer, offener und produktiver agieren kann.

Ein Beispiel: Ein Anwender in einem Unternehmen muss auf eine Cloud-basierte CRM-Anwendung zugreifen. In der Regel muss der Anwender verschiedene separate Zugangsprozesse ausführen, um eine Verbindung zum Unternehmensnetzwerk und zur CRM-Anwendung herzustellen. Durch den zunehmenden Einsatz von Cloud-Technologien in der IT-Branche entfallen redundante Benutzerdaten und Anmeldevorgänge. Um eine nahtlose Anwendung zwischen Unternehmen und Cloud-Modellen zu ermöglichen, entwickeln Unternehmen Richtlinien für domainübergreifende Identitäten und leistungsstarke Authentifizierungssysteme. Diese erfordern nur einen einzigen Anmeldevorgang, der den Benutzern den benötigten Zugriff auf alle IT-basierten Services innerhalb und außerhalb des Unternehmens gewährt. Durch die Nutzung starker Authentifizierungsmechanismen für die Anbindung an Cloud-Services sorgen Unternehmen nicht nur für Benutzerfreundlichkeit, sondern untermauern auch die Unternehmenssicherheit, da die Anzahl der Authentifizierungsprozesse sinkt und folglich das Risiko nicht autorisierter Zugriffe abnimmt.

Viele der bewährten Verfahren und Technologien für die Verwaltung vertrauenswürdiger Identitäten in herkömmlichen IT-Umgebungen in Unternehmen lassen sich auch in privaten Unternehmens-Clouds einsetzen. So können Unternehmen z.B. traditionelle Verfahren für die Informationssicherheit wie Datenverschlüsselung, starke Authentifizierung und Fraud Detection auf ihre privaten Clouds ausweiten und sich so gegen Eindringlinge, Phishing, Malware und sogar Datenspionage schützen. Um die Portabilität und den Schutz von Informationen zu verbessern, können Unternehmen Richtlinien zur Verwaltung domainübergreifender Identitäten einsetzen.

Nachfolgend sind einige Best Practices zur Verwaltung vertrauenswürdiger Identitäten in privaten Clouds genannt:

### 1. Aufstellen und Durchsetzen klarer Richtlinien für die Vertrauensdefinition

In einer privaten Cloud werden vertrauenswürdige Beziehungen von dem Unternehmen, das das Cloud-Modell nutzt, selbst definiert und kontrolliert. Alle Beteiligten schützen natürlich die Informationen, die gesetzlichen Datenschutzvorschriften und anderen Compliance-Vorgaben unterliegen, z.B. Steuernummern von Mitarbeitern, vertrauliche Finanzdaten usw. Darüber hinaus müssen Unternehmen auch weitere Richtlinien für andere vertrauliche Daten aufstellen, die in der Cloud gemeinsam genutzt werden. Ein Unternehmen kann z.B. Daten wie Bestellungen oder getätigte Transaktionen von Kunden als vertraulich oder gar als Betriebsgeheimnis einstufen und risikobasierte Richtlinien festlegen, die festschreiben, wie Cloud-Anbieter und Geschäftspartner diese Daten außerhalb des Unternehmens speichern, handhaben und abrufen müssen.

Damit vertrauenswürdige Beziehungen funktionieren, müssen klare vereinbarte Richtlinien gelten, welche Informationen privilegiert sind, wie diese Daten verwaltet werden und wie Cloud-Anbieter ihre Leistung für die Durchsetzung dieser Unternehmensstandards nachweisen und validieren. Vereinbarte Richtlinien müssen durch verbindliche Service Level Agreements (SLA) untermauert werden, die im Falle einer Nichteinhaltung oder eines Sicherheitsverstößes ganz klar die Konsequenzen definieren.

### 2. Halten Cloud-Anbieter, was sie in Sachen Sicherheit versprechen?

Die Informationssicherheit ist nur so stark wie das schwächste Glied in der Kette. Aus diesem Grund ist es wichtig, dass Unternehmen die Eignung der Cloud-Anbieter gründlich prüfen. Ein hochkarätiger Markenname und ein eindeutiges SLA sind längst nicht ausreichend: Unternehmen müssen eindringlich prüfen, ob Cloud-Anbieter die angebotene Sicherheit wirklich anbieten und vor allem validieren können.

Unternehmen müssen sich überzeugend dafür engagieren, dass sie ihre Informationsbestände außerhalb der unternehmenseigenen IT-Umgebung mindestens mit demselben Sicherheitsstandard schützen, der für diese Daten innerhalb der IT-Umgebung gelten würde. Da diese Daten außerhalb des Unternehmens gespeichert sind, könnte man argumentieren, dass der Sicherheitsstandard sogar noch höher sein sollte. Sicherheitsunternehmen müssen besonders bei der Bewertung der Sicherheitsprofile solcher Cloud-Anbieter sorgfältig vorgehen, denen äußerst vertrauliche Daten oder geschäftskritische Funktionen anvertraut werden. Im Kasten auf Seite 5 („Fragen an Cloud-Anbieter“) haben wir einige wichtige Punkte für führende Sicherheitsunternehmen zusammengestellt, die bei der Bewertung der Sicherheitsprofile möglicher Cloud-Anbieter beachtet werden sollten.

### 3. Transparenz im Cloud-Betrieb für Mandantenfähigkeit und Datenisolation

In der virtualisierten Cloud-Umgebung nutzen viele verschiedene Unternehmen bzw. „Mandanten“ dieselbe physische Rechner-, Storage- und Netzwerkinfrastruktur. Cloud-Anbieter müssen die Zugriffsisolation sicherstellen. Software, Daten und Services müssen sich innerhalb der Cloud eindeutig trennen lassen, damit Mandanten, die gemeinsam eine Infrastruktur nutzen, nicht auf benachbarte proprietäre Informationen und Anwendungen zugreifen können.

Am besten lassen sich Datenisolation und Mandantenfähigkeit (separater Zugriff auf geeignete Cloud-Ressourcen für alle Nutzer) umsetzen, indem Unternehmenskunden maximale Transparenz für die Aktivitäten ihres Cloud-Anbieters fordern. Cloud-Anbieter sollten Protokolldateien und Berichte über Anwenderaktivitäten erstellen. Einige Cloud-Anbieter bieten sogar eine noch bessere Transparenz anhand von Anwendungen, mit denen IT-Administratoren in Unternehmen die Daten überwachen können, die sich in ihren virtuellen Netzwerken bewegen.

Ebenfalls lassen sich Ereignisse innerhalb der Cloud nahezu in Echtzeit anzeigen. Servicevereinbarungen sollten bestimmte Leistungskennzahlen enthalten. Für den Fall, dass vereinbarte Leistungen nicht eingehalten werden, sollten Geldstrafen festgelegt werden.

Unternehmen mit privaten Clouds sollten mit Cloud-Anbietern zusammenarbeiten, um die Übertragbarkeit von Sicherheitskontrollen sicherzustellen. Anders gesagt, falls und wenn Daten oder virtuelle Ressourcen auf einen anderen Server verschoben oder in einem Rechenzentrum gesichert werden, sollten die Sicherheitsrichtlinien des ursprünglichen Servers oder primären Rechenzentrums automatisch auch für die neuen Speicherorte implementiert werden.

#### 4. Funktionstrennung für Administratoren

Die Datenisolation und das Abwenden von Datenverlusten sind unabdingbar, aber dennoch muss gewährleistet sein, dass die Administratoren von Unternehmenssystemen über die geeigneten Zugriffsrechte für die Verwaltung und Konfiguration ihrer Unternehmensanwendungen innerhalb der gemeinsam genutzten Infrastruktur verfügen. Hinzu kommt, dass neben System- und Netzwerkadministratoren in privaten Cloud-Modellen noch eine weitere vertrauenswürdige Funktion zu finden ist: der Cloud-Administrator. Cloud-Administratoren sind IT-Experten, die für den Cloud-Anbieter arbeiten. Sie benötigen ausreichende Zugriffsrechte auf die virtuellen Geräte von Unternehmen, um die Cloud-Performance zu optimieren. Gleichzeitig dürfen sie jedoch keinen Zugang zu vertraulichen Daten von Mandanten haben. Unternehmen, die private Clouds auf gehosteten Servern unterhalten, sollten über die Möglichkeit nachdenken, dass der Datenbankbetreiber die lokale Administration von Hypervisoren deaktiviert und stattdessen eine zentrale Verwaltungslösung einsetzt, um die Risiken eines nicht autorisierten Administratorzugriffs besser überwachen und verwalten zu können.

#### Fragen an Cloud-Anbieter

Unternehmen, die Teile ihrer IT-Infrastruktur out-sourcen, müssen den Anbietern der Cloud-basierten Services vertrauen können. Diese notwendige Vertrauensbasis ergibt sich nicht durch den guten Ruf des Serviceanbieters allein. Sie sollte anhand umfassender Bewertungen validiert werden, um zu prüfen, ob der Cloud-Anbieter zusätzliche Schritte einleiten muss, um den Anforderungen und Richtlinien in Bezug auf die Informationssicherheit des Unternehmens gerecht zu werden. Des Weiteren sollten Leistungen und Standards in SLAs und Vereinbarungen für Managed Services in Schriftform festgehalten werden.

Nachfolgend haben wir einige Fragen zusammengestellt, die Unternehmen, die ein privates Cloud-Modell nutzen möchten, möglichen Anbietern von Cloud-Infrastrukturen stellen sollten:

- Ist es möglich, beispielhafte Protokolldateien einzusehen, um besser verstehen zu können, welche Datentypen in Berichten erfasst werden und erfasst werden können?
- Wie werden Daten in Ihren verschiedenen Systemen und Netzwerken geschützt? Welche

Daten werden z.B. unter welchen Umständen verschlüsselt (bei der Datenübertragung, im gespeicherten Zustand)?

- Mit welchen Maßnahmen sorgen Sie für sichere Mandantenfähigkeit, Authentifizierung, Autorisierung und Aktivitätsüberwachung? Wurden diese Maßnahmen durch einen unabhängigen Auditor abgenommen? Falls nicht, würden Sie einem Audit durch uns oder einen unabhängigen Auditor zustimmen?
- Unterstützen Sie die Verwaltung domainübergreifender Identitäten? Wenn Sie unsere Assertions nicht unterstützen und uns Benutzeridentitäten zur Verfügung stellen, wie werden diese Konten erstellt und validiert? Wie werden Benutzeridentitäten bereitgestellt, verwaltet und terminiert?
- Welche speziellen Auditrechte, Haftungssteuerung und Schutzmaßnahmen bieten Sie im Rahmen Ihrer Vereinbarungen für Managed Services üblicherweise an?
- Können Ihre Rechenzentren besichtigt werden? Können wir uns bei einem Besuch vor Ort von der physischen Sicherheit überzeugen?

Als zusätzliche Sicherheitsmaßnahme sollten Unternehmen im Cloud-Modell eine Funktionstrennung für Administratoren anwenden. Es mag verlockend sein, verschiedene Funktionen zu konsolidieren, da sie zentral über die Software zur Virtualisierungsverwaltung administriert werden können. Durch eine solche Trennung der Funktionen – ebenso wie in physischen IT-Umgebungen, in denen Server, Netzwerke und Sicherheitsfunktionen auf mehrere Administratoren oder Abteilungen aufgeteilt sind – steigt jedoch aufgrund der verteilten Kontrolle die Sicherheit. Darüber hinaus können Unternehmen zentrale Funktionen für die virtuelle Verwaltung nutzen, um den administrativen Zugang einzuschränken, Rollen zu definieren und einzelnen Administratoren die geeigneten Benutzerrechte zuzuweisen. Durch die Funktionstrennung für Administratoren und die Nutzung einer zentralen Virtualisierungsverwaltung können Unternehmen ihre privaten Clouds vor unberechtigten Administratorzugriffen schützen.

#### 5. Richtlinienverwaltung für die Bereitstellung virtueller Maschinen

Innerhalb der Cloud sind virtuelle Maschinen äußerst produktiv und mobil. Von ihnen geht die meiste Aktivität in der Cloud aus. Virtuelle Maschinen werden üblicherweise automatisiert bereitgestellt, um SLAs zu entsprechen, die Ausführungszeit von Anwendungen zu optimieren und die allgemeine Ressourcennutzung zu maximieren. In Cloud-Umgebungen spielen virtuelle Maschinen eine wichtige Rolle, die deutliche Auswirkungen auf die Informationssicherheit hat. Um die virtuelle Infrastruktur zu schützen, müssen Unternehmen mit privaten Clouds wissen, wie viele virtuelle Maschinen in ihren Clouds vorhanden sind und verwaltet werden. Besonders wichtig ist hier die Verwaltung von Identitäten virtueller Maschinen. Sie werden für grundlegende administrative Funktionen verwendet, z.B. die Erkennung von Systemen und Benutzern, denen die Maschinen physisch zugeordnet sind, oder das Verschieben von Software auf neue Host-Server.

Unternehmen, die eine Sicherheitsstruktur auf Basis von virtuellen Maschinenidentitäten aufbauen möchten, sollten wissen, wie diese Identitäten erstellt, validiert und verifiziert werden und welche Maßnahmen die Cloud-Anbieter zum Schutz dieser Identitäten einsetzen. Außerdem sollten führende Sicherheitsanbieter ihre Richtlinien für Benutzerzugriffe und -verwaltung so auslegen, dass alle Anwender – gleich ob Mensch oder Maschine – in die geringste Zugriffsebene eingestuft werden, die für ihre jeweils autorisierten Funktionen innerhalb der Cloud notwendig sind.

#### 6. Datenverschlüsselung und Tokenisierung

Unternehmensdaten, die in Cloud-Anwendungen genutzt werden, werden gelegentlich vom Cloud-Anbieter gespeichert, z.B. in Online-Backups. Die Datenverschlüsselung stellt oftmals die einfachste Methode dar, vertrauliche Informationen vor unberechtigtem Zugriff, besonders durch Administratoren und anderen Parteien in der Cloud, zu schützen. Unternehmen sollten Daten verschlüsseln, die von Cloud-Anbietern gehostet werden oder auf die diese Anbieter zugreifen können. Genau wie in herkömmlichen IT-Unternehmensumgebungen sollten Anwendungsdaten zum Zeitpunkt der Erfassung verschlüsselt werden. Des Weiteren sollte sichergestellt sein, dass Cloud-Anbieter Verschlüsselungsmechanismen einsetzen, mit denen Daten auf jeder IT-Ebene abgesichert werden können.

Eine zusätzliche Maßnahme zum Schutz von Cloud-Daten ist die Trennung vertraulicher Daten von den jeweils zugeordneten Benutzern oder Identitäten. Unternehmen, die Kreditkartendaten speichern, hinterlegen Kreditkartennummern oftmals in separaten Rechenzentren getrennt von den persönlichen Daten des Karteninhabers. So wird die Wahrscheinlichkeit reduziert, dass eine Sicherheitsverletzung einen Kartenmissbrauch zur Folge hat.

Eine Alternative, wie Unternehmen vertrauliche Daten von Karteninhabern in der Cloud schützen können, ist eine Art Datenverdeckung, auch Tokenisierung genannt. Bei dieser Datenschutzmethode wird die ursprüngliche Zahl durch einen Token-Wert ersetzt, der in keiner eindeutigen Beziehung zum eigentlichen Wert steht. Die Kartennummer selbst wird separat in einer sicheren Datenbank gespeichert.

---

**In Cloud-Umgebungen spielen virtuelle Maschinen eine wichtige Rolle, die deutliche Auswirkungen auf die Informationssicherheit hat. Um die virtuelle Infrastruktur zu schützen, müssen Unternehmen mit privaten Clouds wissen, wie viele virtuelle Maschinen in ihren Clouds vorhanden sind und verwaltet werden.**

---

## 7. Anwendung von Richtlinien für domainübergreifende Identitäten und starke Authentifizierungsmethoden

Ganz einfach ausgedrückt ermöglicht eine domainübergreifende Identität einem Benutzer den Zugriff auf Websites, Unternehmensanwendungen und Cloud-Services mit nur einem einzigen Anmeldevorgang (Single Sign-On). Domainübergreifende Identitäten können genutzt werden, wenn Unternehmen die jeweils anderen vertrauenswürdigen Identitäten in Bezug auf Zugriffsrechte und Berechtigungen anerkennen. Durch diese Vereinbarungen zwischen den Parteien, gemeinsame Richtlinien für Benutzeridentitäten, Authentifizierung und Autorisierung zu nutzen, können Benutzer noch bequemer und sicherer auf Services zugreifen, sie verwenden und zwischen verschiedenen Services wechseln. Dabei spielt es keine Rolle, ob diese Services in einem Unternehmen oder in einer Cloud hinterlegt sind.

Richtlinien für domainübergreifende Identitäten gehen mit starken Authentifizierungsrichtlinien einher. Domainübergreifende Identitäten schließen die Vertrauenslücken zwischen Mitgliedern innerhalb der domainübergreifenden Gruppe, während starke Authentifizierungsrichtlinien Sicherheitslücken schließen. So entsteht eine sichere Zugangsinfrastruktur für alle Mitglieder der Anwendergemeinde.

In der Cloud werden domainübergreifende Richtlinien für Benutzerdaten und -authentifizierung über kurz oder lang zum Standard werden – und das nicht nur deshalb, weil Benutzer dies aufgrund der hohen Benutzerfreundlichkeit wünschen. Für Unternehmen ergeben sich außerdem Kostenvorteile und eine verbesserte Sicherheit. Sie können Zugriffs- und Authentifizierungssysteme separater Geschäftsbereiche zentralisieren. Darüber hinaus gibt es deutlich weniger Schwachstellen wie unsichere Methoden zur Passwortverwaltung, da Benutzer nicht mehr wiederholt Benutzername und Passwort eingeben müssen.

Damit domainübergreifende Identitäten verstärkt genutzt werden, müssen Informationstechnologie und Sicherheitsbranche noch einige Hindernisse überwinden, die der Implementierung solcher Richtlinien im Weg stehen. Es hat den Anschein, dass diese Hindernisse weder wirtschaftlicher noch technologischer Natur sind, sondern mit Vertrauen zu tun haben.

Modelle domainübergreifender Identitäten wie z.B. die starken Authentifizierungsservices, die sie durchsetzen, sind immer nur so stark wie das schwächste Glied in der Kette. Jedes einzelne Mitglied muss das Vertrauen genießen, dass die Sicherheitsrichtlinien der Gruppe eingehalten werden. Durch eine Erweiterung dieses „Vertrauenskreises“ steigt auch das Bedrohungsrisiko, wodurch Probleme entstehen können und die Wahrscheinlichkeit von einzelnen Versagenpunkten (Single Point of Failure) in der geschlossenen Gemeinschaft steigt.

Die beste Möglichkeit sicherzustellen, dass innerhalb von solchen Gemeinschaften Vertrauen und Sicherheit gewahrt werden, ist eine einheitliche starke Authentifizierung für alle Mitglieder. Einige Initiativen in der IT-Branche zielen darauf ab, Sicherheitsstandards zu implementieren, die domainübergreifende Identitäten und die Authentifizierung vereinfachen. So hat beispielsweise das OASIS Security Services Technical Committee die Security Assertion Markup Language (SAML) entwickelt, einen XML-basierten Standard zum Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Sicherheitsdomänen, der das Single Sign-On über Webbrowser erleichtert. SAML entwickelt sich offenbar zum Standard für Unternehmen, die Lösungen für das Single Sign-On anbieten.

---

## Fraud Protection: Schutz vor unerwünschten Besuchern

---

Das Cloud-Modell entwickelt sich recht schnell, aber gleichzeitig nimmt auch die Cyber-Kriminalität rasant zu. Bisher haben Cyber-Kriminelle Anwender zu Sicherheitslücken gelotst, wo dann ein Trojaner oder andere Malware (Schadsoftware) auf deren Rechner geladen wurde. Für Betrüger stellt die zunehmende Anzahl privater Clouds eine willkommene Gelegenheit dar, illegal auf Unternehmensdaten zuzugreifen. Ebenso wie vertrauenswürdige Beziehungen von enormer Bedeutung für die produktive Beteiligung an einem Cloud-Modell sind, ist die Fraud Protection essentiell, um sich vor unerwünschten Besuchern zu schützen.

Eine der effizientesten Arten der Fraud Protection ist der Schutz von Identitäten: Sind Benutzer auch tatsächlich die Personen, für die sie sich ausgeben? Die Betrugsprävention und der Identitätsschutz gehören zu den schwierigsten und schnelllebigsten Aufgaben in der Informationssicherheit. Die Anzahl neuer Bedrohungen nimmt fast täglich zu.

Cloud-Anbieter können nicht alle gleich gut vor Betrug und unerlaubtem Zugriff schützen. Öffentliche Clouds sind besonders anfällig für Cyber-Kriminalität, besonders durch Phishing und Malware.

Der Finanzdienstleistungsbereich ist seit vielen Jahren führend, wenn es um die Bekämpfung von Online-Betrug geht. Finanzunternehmen haben ausgereifte Verfahren und Tools für die Sicherheit entwickelt, die in angepasster Form auch von anderen Branchen in Clouds verwendet werden können. Die Cloud-Sicherheit entwickelt sich ständig weiter. Die risikobasierte Authentifizierung, die für den Ausgleich zwischen Sicherheit, Benutzerfreundlichkeit und Kosten sorgt, indem geeignete Schutzmaßnahmen auf Basis des zugrundeliegenden Risikos von Aktivitäten angewendet werden, wird bei der Betrugsprävention sowohl in privaten als auch öffentlichen Clouds zweifelsohne eine große Rolle spielen.

Die Finanzdienstleistungsbranche setzt die risikobasierte Authentifizierung als eine von vielen Schutzmaßnahmen ein, die sich mit den Bedrohungen weiterentwickeln. Zum Beispiel setzen Finanzunternehmen auf Tools für die Überwachung im Hintergrund, um finanzielle Transaktionen und Aktivitätsmuster automatisch zu kennzeichnen und zu melden, die vom typischen Anwenderverhalten abweichen. Bei sehr hohem Risiko reichen herkömmliche Authentifizierungsprotokolle längst nicht mehr aus, und das Finanzunternehmen bräuchte zusätzliche Methoden zur Prüfung von Benutzeridentitäten. Diese Methoden könnten sein: persönliche Fragen, deren Antworten nur dem Unternehmen und dem Benutzer bekannt sind; ein automatischer Out-of-Band-Telefonanruf, bei dem der Benutzer über die Telefontastatur einen Code eingeben muss, der auf dem Computerbildschirm angezeigt wird; oder ein einmalig gültiges Passwort, das per SMS übermittelt wird.

In den nächsten Jahren müssen Unternehmen mit privaten Clouds ihre Maßnahmen für die starke Authentifizierung und Betrugsprävention zum Schutz vor Phishing, Malware und den Diebstahl geistigen Eigentums drastisch ausweiten. Um den Schutz vor unberechtigtem Zugriff und Online-Betrug zu optimieren, können Unternehmen sich der Maßnahmen zur Betrugsprävention bedienen, die die Finanzdienstleistungsbranche entwickelt hat:

#### 1. Implementierung starker Authentifizierungsdienste

An erster Stelle beim Identitätsschutz steht meist die Authentifizierung. Anhand mehrerer Sicherheitsverfahren wird geprüft, dass Benutzer auch tatsächlich die Personen sind, für die sie sich ausgeben. Diese Benutzer erhalten dann entsprechende Zugriffs- und Benutzerrechte. Die Authentifizierungsmethoden reichen von schwachen Formen, die oft mit öffentlichen Cloud-Services in Verbindung gebracht werden (Benutzername und Kennwort), bis hin zu leistungsstarken Verfahren wie Tokenlösungen, die z.B. oft von Unternehmen für Mitarbeiter im Außendienst eingesetzt werden.

Einige Anbieter öffentlicher Clouds nutzen die Zwei-Faktor-Authentifizierung für Ihre Anwender. Andere wiederum finden diese Methode für die gesamte Anwenderschaft aufgrund der Kosten für Bereitstellung und Wartung ungeeignet. Diese Cloud-Anbieter können nur einigen wenigen Anwendern Sicherheitsgeräte zur Verfügung stellen. Da statische Passwörter jedoch nicht sicher genug sind, stellt der Schutz der übrigen Anwender ein Problem dar. Aus diesem Grund möchten zahlreiche Cloud-Anbieter unbedingt eine Authentifizierungstechnologie implementieren, die einen stärkeren Schutz als herkömmliche Passwörter bietet.

Eine der besten Möglichkeiten, Online-Identitäten in öffentlichen Cloud-Modellen zu schützen, ist die risikobasierte bzw. adaptive Authentifizierung. Hier werden Authentifizierungsprozesse auf Basis von Echtzeit-Risikoberechnungen intelligent variiert. Der risikobasierte Identitätsschutz nutzt Verhaltensprofile und unsichtbare Authentifizierung im Hintergrund. Dabei werden Benutzeranfragen für Cloud-Services mit Daten bisheriger Benutzeraktivitäten verglichen. Verdächtige Aktivitäten oder Verhaltensmuster, die von der Norm abweichen, werden automatisch gemeldet.

Die Authentifizierung im Hintergrund erfolgt oft durch die Geräteerkennung anhand verschiedener Parameter des Endanwendergeräts sowie IP-Ortsbestimmung und Netzwerkinelligenz. So wird erkannt, ob ein Benutzer versucht, von einem unbekanntem Standort oder einem unbekanntem Gerät aus auf Cloud-Services zuzugreifen. Kombiniert mit Verhaltensprofilen kennzeichnen diese unsichtbaren Authentifizierungsprozesse vermeintlich verdächtiges Verhalten wie z.B. illegalen Zugriff auf die Cloud. In solchen Fällen können adaptive Authentifizierungssysteme automatisch weitere Authentifizierungsanforderungen nutzen. Dabei werden den Benutzern persönliche Fragen gestellt (z.B. „Wer war 2007 Ihr Arbeitgeber?“) oder sie werden aufgefordert, sich mit einem einmalig gültigen Passwort anzumelden, das per SMS an ein Mobiltelefon gesendet wird. Solche risikobasierten Authentifizierungsmethoden werden bereits in zahlreichen öffentlichen Clouds eingesetzt, besonders im Bereich Finanzdienstleistungen.

Unternehmen mit vielen Außendienstmitarbeitern setzen ebenfalls auf fortschrittliche, risikobasierte Authentifizierungsprozesse. Diese Authentifizierungsmethode kann noch durch Hard- oder Software Token ergänzt werden. Solche starke Zwei-Faktor Authentifizierung durch Token generiert eine unveränderbare, einzigartig Identität. Die Token dienen als sekundäre Methode zur Identitätsprüfung, nachdem der Benutzer andere Zugangsdaten wie Passwort oder PIN eingegeben hat. Diese Mehrfachauthentifizierung mit Token sorgt für eine leistungsstarke Authentifizierung und Identitätsschutz.

Obwohl mithilfe der risikobasierten Authentifizierung und den Tokenlösungen eine leistungsstarke Identitätsprüfung samt -schutz möglich ist, ist das Unternehmen selbst möglicherweise nur ein Glied einer umfassenden Zugriffskette. Selbst starke Authentifizierungsmethoden sind für ein Unternehmen u.U. nutzlos, wenn die IT-Infrastruktur an einen Cloud-Anbieter gebunden ist, der eine weniger wirksame Form der Zugriffssicherheit einsetzt. Damit Unternehmen einen gleichbleibenden Schutz für Identitäten sicherstellen können, muss auch der Cloud-Anbieter gleichwertige, leistungsstarke Applikationen für die Verwaltung von Zugriffsrechten und digitalen Identitäten einsetzen.

## 2. Verschiedene Abwehrmechanismen zum Schutz vor ausgeklügelten Malware-Angriffen

Die Techniken der Betrüger werden von Tag zu Tag ausgeklügelter. Die Anzahl der Phishing-Angriffe steigt jedes Jahr stetig, und Malware-Angriffe (Trojaner wie Zeus und Sinowal) nehmen zehnmal schneller als noch 2008 zu. Jede Woche fallen mehrere Zehntausend Identitäten in die Hände von Betrügern, die Benutzernamen und Passwörter durch Aufzeichnung von Online-Aktivitäten und Tastatureingaben mittels Malware herausfinden.

Bisher waren zumeist Banken und Kreditkartenunternehmen bedroht. Es ist jedoch wahrscheinlich, dass in den nächsten Jahren auch andere Unternehmen zunehmend Bedrohungen ausgesetzt sind, da immer mehr vertrauliche Daten und Anwendungen in Cloud-Infrastrukturen gespeichert werden. Durch die Zunahme von Malware könnten Zugangsdaten für Unternehmen auf dieselbe Weise von Trojanern erfasst werden, wie es jetzt in öffentlichen Clouds von Finanzdienstleistern der Fall ist. Ein Beispiel dafür, wie Zugangsdaten abgefangen werden können, auch wenn starke Authentifizierungsverfahren eingesetzt werden, finden Sie im aktuellen RSA-Whitepaper „Making Sense of Man-In-The-Browser: Strategies for Mitigating a Menacing Threat“\* (Englisch).

Die Bedrohung, die von zunehmend ausgeklügelten Malware-Angriffen ausgeht, ist ein ausgezeichnetes Beispiel dafür, warum mehrstufige Ansätze für den Schutz von Identitäten so wichtig sind. Unternehmen innerhalb eines Cloud-Modells sollten sich nicht ausschließlich auf starke Authentifizierungsprozesse verlassen, um unerwünschte Zugriffe zu verhindern. Vielmehr sollten Tools zur risikobasierten Authentifizierung um weitere Verfahren wie Geräte- oder IP-Verfolgung, Verhaltensprofile und Out-of-Band-Technologien ergänzt werden, die den gesamten Online-Dienst abdecken, z.B. Benutzerauthentifizierung per Telefon. Darüber hinaus können Unternehmen auch externe Dienste nutzen, um sich vor Bedrohungen zu schützen und die Auswirkungen von Malware-Angriffen so gering wie möglich zu halten, z.B. ein Abonnement eines Netzwerks zur Betrugsüberwachung.

## 3. Cyber-Kriminalität

Für Cloud-Modelle nutzen Unternehmen Ressourcen von Drittanbietern, um ihr Unternehmen voranzubringen.

Cyber-Kriminelle hingegen nutzen die Ressourcen der Unternehmen für ihre Geschäftstätigkeit. Betrüger haben so ihre eigene Infrastruktur innerhalb der Cloud, die mithilfe von Ressourcen entstanden ist, die von Privatpersonen und Unternehmen gehackt wurden.

Das Finanzwesen und andere Branchen, die von Phishing und Malware betroffen sind, nutzen häufig Services gegen Cyber-Kriminalität, um einen Einblick in die betrügerische Infrastruktur zu ermöglichen. Solche Services bieten die Möglichkeit, Malware-Angriffe auf Benutzer zu erkennen, von Benutzern gestohlene Zugangsdaten wiederzuerlangen,

---



---

**Die Techniken der Betrüger werden von Tag zu Tag ausgeklügelter. Die Anzahl der Phishing-Angriffe steigt jedes Jahr stetig, und Malware-Angriffe (Trojaner wie Zeus und Sinowal) nehmen zehnmal schneller als noch 2008 zu. Jede Woche fallen mehrere Zehntausend Identitäten in die Hände von Betrügern.**

---



---

\* <http://www.rsa.com/go/wpt/wpindex.asp?WPID=10459>

Sicherheitslücken und gefälschte Webseiten zu schließen und Bot-Netze sowie Steuer- und Kommandozentralen zu überwachen. Um Betrügern immer einen Schritt voraus zu sein, nutzen viele Unternehmen ebenfalls Services gegen Cyber-Kriminalität, um weitere Informationen über Methoden und Netzwerke zu erhalten. Cloud-Anbieter erkennen allmählich den Wert, den solche Überwachungsdienste für die Anwender haben.

## Datenkonformität im Cloud Computing

---

In Cloud-Umgebungen ermöglicht die Virtualisierungsebene eine einmalige Einsicht in Systemaktivitäten. Hypervisoren sind jeder Komponente und Funktion im virtuellen System ausgesetzt – von CPU-Anweisungen und Speicherzugriffen bis hin zu Festplatten-E/A und Netzwerkpaketen. Diese außerordentliche Transparenz bedeutet, dass fast jede Aktivität im Zusammenhang mit Anwendungsservices überwacht und für Audit- und Compliance-Zwecke verwendet werden kann – meist ohne zusätzliche Software.

Die häufig detaillierten Überwachungsfunktionen von Hypervisoren vereinfachen in Cloud-Umgebungen oft die Berichterstellung für Audits. Andererseits können fehlende physische Grenzen in Cloud-Modellen die Richtlinienkonformität verschiedener Rechtsprechungen kompliziert gestalten. Wir haben einige Best Practices zusammengestellt, wie diese Probleme behoben werden können und wie Compliance in privaten Clouds möglich ist:

### 1. Compliance-Prüfung für Cloud-Anbieter

Die Audit-Protokollierung ist für die Sicherheitsverwaltung jeder IT-Umgebung enorm wichtig und Voraussetzung vieler gesetzlicher Vorgaben und Standards. Unternehmen mit privaten Clouds sollten sich mit den verschiedenen Cloud-Anbietern abstimmen und sicherstellen, dass die Daten, die als Konformitätsnachweis benötigt werden, wieder an das Unternehmen weitergeleitet werden. Servicevereinbarungen sollten bestimmte Leistungskennzahlen für Berichterstellung und Audits enthalten. Darüber hinaus können Protokolle der Cloud-Anbieter in das SIEM-System (Security Information and Event Management) des Unternehmens importiert werden. So lassen sich virtuelle Ereignisse in der privaten Cloud parallel zur unternehmensinternen IT-Infrastruktur in der zentralen Sicherheitsabteilung des Unternehmens überwachen und analysieren. Protokolle und Berichte einer SIEM-Lösung sind unverzichtbare Tools zum Konformitätsnachweis für interne und externe Auditoren.

### 2. Einhaltung rechtlicher Vorgaben in offenen Clouds

Verschiedene Länder und Rechtsprechungen verfügen über unterschiedliche Richtlinien zum Datenschutz und zur Speicherung, Übermittlung und gemeinsamen Nutzung vertraulicher Daten. Große, multinationale Konzerne sind mit den unterschiedlichsten internationalen Anforderungen vertraut und haben komplexe Prozesse für deren Handhabung entwickelt. Viele kleinere Unternehmen mit Cloud-Services spüren durch die quasi grenzenlose Cloud erst jetzt die Auswirkungen gesetzlicher Compliance-Vorgaben. Im Cloud-Modell werden Computer- und Speicherressourcen virtualisiert. Sie können gleichzeitig an mehreren unterschiedlichen Standorten gehostet werden. Daher können hier vertrauliche Daten eher in falsche Hände gelangen. Durch gesetzliche Vorgaben ist es gelegentlich erforderlich, in eigentlich offenen Clouds künstliche Grenzen zu schaffen.

Unternehmen, die eine zunehmende Anzahl gesetzlicher Vorgaben erfüllen müssen, können von Cloud-Speicherplattformen profitieren, die die intelligente Bereitstellung unterstützen und gleichzeitig für Datenschutz sorgen. Als extremes Beispiel sei das Bundesdatenschutzgesetz genannt. Es verbietet die Speicherung oder Übertragung persönlicher Daten von Bundesbürgern außerhalb des Gültigkeitsbereichs der bundesdeutschen Rechtsprechung. Um dem Bundesdatenschutzgesetz und anderen gesetzlichen Vorschriften gerecht zu werden, nutzen einige Unternehmen intelligente Cloud-Speicherplattformen, die die Eigenschaften der hinterlegten Daten erkennen und diese entsprechend handhaben.

Im Fall des Bundesdatenschutzgesetzes filtern solche „datenbewussten“ Clouds die entsprechenden persönlichen Daten automatisch heraus und speichern sie vorschriftsmäßig in deutschen Rechenzentren.

## Übersicht

---

Man rechnet damit, dass die Anzahl der Unternehmen, die Cloud Computing nutzen, in den kommenden zehn Jahren rapide zunehmen wird. Ein Grund dafür ist, dass immer mehr Unternehmen erkennen, dass sie die hohe Skalierbarkeit der Cloud-Modelle nutzen können, um ihre IT-Funktionen schnell und bequem auszuweiten, während gleichzeitig Ressourcen eingespart und Kosten gesenkt werden können. Unternehmen, die sich für das Cloud Computing entscheiden, sollten unbedingt sicherstellen, dass die Serviceanbieter und alle an Transaktionen innerhalb der Cloud Beteiligten absolut vertrauenswürdig sind. Unternehmen müssen vertrauliche Informationen auf virtuellen Servern und Datenspeichern schützen und gleichzeitig dafür sorgen, dass Cloud-Administratoren über alle notwendigen Zugriffs- und Benutzerrechte verfügen. Weiterhin muss die Arbeit der Cloud-Anbieter für Unternehmen transparent sein, um vereinbarte Sicherheitsprotokolle nachprüfen zu können. Darüber hinaus erwarten die Nutzer eine hohe cloudübergreifende Identitätsmobilität, wobei die Sicherheit der Identitäten gewährleistet sein muss. Benutzer erwarten zudem von Cloud-Anbietern den nötigen Betrugsschutz. All diese Punkte haben mit vertrauenswürdigen Beziehungen zu tun, die den Grundstein für die Sicherheit des Cloud Computing bilden.

Viele der bewährten Verfahren und Technologien für die Verwaltung vertrauenswürdiger Beziehungen in herkömmlichen IT-Umgebungen lassen sich erweitern und somit in privaten und öffentlichen Clouds einsetzen. So können Unternehmen z.B. traditionelle Verfahren für die Informationssicherheit wie Datenverschlüsselung, starke Authentifizierung und Fraud Detection auf ihre privaten Clouds ausweiten und sich so gegen unerwünschten Zugriff, Phishing, Malware und sogar den Diebstahl geistigen Eigentums schützen. Um die Portabilität und den Schutz von Informationen zu verbessern, können Unternehmen Richtlinien zur Verwaltung domainübergreifender Identitäten einsetzen.

Wir haben bereits einige der Best Practices zur Verwaltung vertrauenswürdiger Identitäten in privaten Clouds genannt:

1. Aufstellen und Durchsetzen klarer Richtlinien für die Vertrauensdefinition: Damit vertrauenswürdige Beziehungen funktionieren, müssen klare, vereinbarte Richtlinien gelten, welche Informationen privilegiert sind, wie diese Daten verwaltet werden und wie Cloud-Anbieter ihre Leistung für die Durchsetzung dieser Unternehmensstandards nachweisen und validieren.
2. Halten Cloud-Anbieter, was sie in Sachen Sicherheit versprechen? Unternehmen können sich nicht ausschließlich auf den guten Ruf des Serviceanbieters verlassen. Sie müssen eingehend prüfen, ob Cloud-Anbieter in Sachen Leistung und Sicherheit das liefern, was sie versprechen, und dies auch nachweisen können.
3. Transparenz im Cloud-Betrieb für Mandantenfähigkeit und Datenisolation: Die wirksamste Methode für sichere Datenisolation und Mandantenfähigkeit für Unternehmenskunden ist eine maximale Transparenz der Aktivitäten der Cloud-Anbieter. Erreichen lässt sich dies durch das Prüfen von Protokollen und anderen Berichten zu Ereignissen und Aktivitäten.

---

**Unternehmen, die sich für das Cloud Computing entscheiden, sollten unbedingt sicherstellen, dass die Serviceanbieter und alle an Transaktionen innerhalb der Cloud Beteiligten absolut vertrauenswürdig sind. Unternehmen müssen vertrauliche Informationen auf virtuellen Servern und Datenspeichern schützen und gleichzeitig dafür sorgen, dass Cloud-Administratoren über alle notwendigen Zugriffs- und Benutzerrechte verfügen.**

---

4. Funktionstrennung für Administratoren: Es mag verlockend für Unternehmen sein, Administratorfunktionen in der Cloud zu konsolidieren, da viele Funktionen sich bequem und zentral über die Software zur Virtualisierungsverwaltung verwalten lassen. Durch eine Trennung der Funktionen – ebenso wie in physischen IT-Umgebungen, in denen Server, Netzwerke und Sicherheitsfunktionen auf mehrere Administratoren oder Abteilungen aufgeteilt sind – steigt jedoch aufgrund der verteilten Kontrolle die Sicherheit.
5. Richtlinienverwaltung für die Bereitstellung virtueller Maschinen: Unternehmen, die eine Sicherheitsstruktur auf Basis von virtuellen Maschinenidentitäten aufbauen möchten, sollten wissen, wie diese Identitäten entstehen und welche Maßnahmen die Cloud-Anbieter zum Schutz dieser Identitäten einsetzen.
6. Datenverschlüsselung und Tokenisierung: Unternehmen sollten Daten verschlüsseln, die von Cloud-Anbietern gehostet werden oder auf die diese Anbieter zugreifen können. Des Weiteren sollte sichergestellt werden, dass Cloud-Anbieter Verschlüsselungsmechanismen einsetzen, mit denen Daten auf jeder IT-Ebene abgesichert werden können.
7. Anwendung von Richtlinien für domainübergreifende Identitäten und starke Authentifizierungsmethoden: Richtlinien für domainübergreifende Identitäten wie z.B. die zugehörigen Authentifizierungsservices sind immer nur so stark wie das schwächste Glied in der Kette. Jedes einzelne Mitglied muss das Vertrauen genießen, dass die Sicherheitsrichtlinien der Gruppe eingehalten werden. Eine einheitliche, starke Authentifizierung für alle Mitglieder ist unabdingbar, um das Vertrauen zu fördern, damit Modelle domainübergreifender Identitäten zunehmend Verbreitung finden.

In den nächsten Jahren müssen Unternehmen mit privaten Clouds ihre Maßnahmen für die starke Authentifizierung und Betrugsprävention zum Schutz vor Phishing, Malware und Datenspionage drastisch ausweiten. Um den Schutz vor unrechtmäßigem Zugriff und Online-Betrug zu optimieren, können Unternehmen sich der Maßnahmen zur Betrugsprävention bedienen, die üblicherweise bei Online-Betrug zum Einsatz kommen:

1. Implementierung starker Authentifizierungsdienste: Eine der besten Möglichkeiten, Benutzeridentitäten in Cloud-Modellen zu schützen, ist die Bereitstellung risikobasierter Lösungen für die Verwaltung von Zugriffsrechten und digitalen Identitäten. Sie variieren Authentifizierungsprozesse aufintelligente Weise und auf Basis von Echtzeit-Risikoberechnungen.
2. Verschiedene Abwehrmechanismen zum Schutz vor ausgeklügelten Malware-Angriffen: Durch die zunehmende Anwendung starker Authentifizierungsverfahren haben Betrüger neue, ausgeklügelte Methoden zum Ausspionieren von Benutzeridentitäten für kriminelle Absichten entwickelt. Unternehmen können ihre privaten Clouds vor betrügerischen Malware-Angriffen schützen, indem ein mehrstufiger Ansatz zum Schutz vor Eindringlingen und zur Prüfung von Benutzeridentitäten verfolgt wird.
3. Cyber-Kriminalität: Analyse-Tools und Services gegen Cyber-Kriminalität können wertvolle und zeitnahe Einblicke in operative Methoden und Netzwerke von Betrügern liefern. Anhand der so erhaltenen Informationen können Unternehmen Malware-Angriffe auf Benutzer erkennen, von Benutzern gestohlene Zugangsdaten wiedererlangen, Sicherheitslücken und gefälschte Webseiten schließen und Bot-Netze sowie Steuer- und Kommandozentralen überwachen.

---

**Damit vertrauenswürdige Beziehungen funktionieren, müssen klare vereinbarte Richtlinien gelten, welche Informationen privilegiert sind, wie diese Daten verwaltet werden und wie Cloud-Anbieter ihre Leistung für die Durchsetzung dieser Unternehmensstandards nachweisen und validieren.**

---

In Cloud-Umgebungen ermöglicht die Virtualisierungsebene eine einmalige Einsicht in Systemaktivitäten für Auditing-Zwecke. Nachfolgend sind einige Best Practices für die Identitätskonformität in privaten Clouds genannt:

1. Compliance-Prüfung für Cloud-Anbieter: Unternehmen mit privaten Clouds sollten sich mit den verschiedenen Cloud-Anbietern abstimmen und sicherstellen, dass die Daten, die als Konformitätsnachweis benötigt werden, wieder an das Unternehmen weitergeleitet werden.
2. Einhaltung rechtlicher Vorgaben in offenen Clouds: Die Einhaltung gesetzlicher Vorgaben zum Datenschutz kann im Cloud Computing problematisch sein, da Daten an verschiedenen Orten gleichzeitig gespeichert und gemeinsam genutzt werden. Zu den ausgereiftesten Lösungen, die Unternehmen zur Richtlinienkonformität in der Cloud-Umgebung nutzen können, zählen „datenbewusste“ Clouds.

In den kommenden Jahren wird sich der Trend, wie neue Produkte für die Informationssicherheit auf den Markt kommen, drastisch ändern. Cloud Computing erfreut sich zunehmender Beliebtheit, und die Anforderungen nehmen rasant zu. Wir gehen davon aus, dass Sicherheitslösungen und -services fortan verstärkt gemeinsam entwickelt werden. Führende Sicherheitsexperten werden Sicherheits- und Cloud-Anbieter dabei unterstützen, Anforderungen für künftige Produkt- und Servicegenerationen zu formulieren. In der Folge werden Lösungen schneller entwickelt, und das Angebotsportfolio ist stärker auf die Anforderungen der Experten zugeschnitten und individuell an diese anpassbar.

## Über die Autoren

---

### Eric Baize

#### Senior Director, Secure Infrastructure Group, EMC Corporation

Eric ist bei EMC verantwortlich für die Gewährleistung der Produktsicherheit und leitet die RSA-Produktstrategie zum Schutz virtueller und physischer IT-Infrastrukturen. Eric war Gründungsmitglied des führenden Teams, das die EMC-Vision einer informationsbezogenen Sicherheit formuliert hat. Diese hat 2006 schließlich zum Kauf von RSA Security und Network Intelligence geführt. Baize ist Certified Information Security Manager, Inhaber eines US-Patents und Autor internationaler Sicherheitsstandards.

### Roland Cloutier

#### Chief Security Officer, EMC Corporation

Roland leitet die Global Security & Business Protection Programs von EMC und ist weltweit funktional und operativ für die EMC-Geschäftsbereiche Informations- und Cyber-Sicherheit, Geschäftsrisiken, Krisenmanagement und Unternehmensschutz verantwortlich. Er ist Mitglied der High Tech Crime Investigations Association, der State Department Partnership for Critical Infrastructure Security und des InfraGard-Programms des FBI. Außerdem ist er Mitglied des Security for Business Innovation Council und des Center for Information Policy Leadership. Außerdem ist er als Berater für das Board for Vigilant Corporation tätig.

### Bret Hartman

#### Chief Technology Officer RSA, The Security Division of EMC

Bret ist für die Definition der technologischen Strategie für Unternehmenssicherheit bei EMC verantwortlich, die von RSA implementiert wird. Er verfügt über mehr als 25 Jahre Erfahrung in der Entwicklung von Datenschutzlösungen für große Unternehmen. Zu seinen Fachgebieten zählen Service Oriented Architecture (SOA) und die Sicherheit von Web Services, Entwicklung und Verwaltung von Richtlinien sowie die Entwicklung und Analyse von Sicherheitsmodellen.

### Dr. Stephen Herrod

#### Chief Technology Officer und Senior Vice President R&D, VMware, Inc.

Stephen ist bei VMware für neue Technologien und die Zusammenarbeit mit Kunden, Partnern und Standard-Gruppen verantwortlich. Stephen ist seit 2001 im Unternehmen und war in leitender Funktion für mehrere erfolgreiche Versionen von VMware ESX verantwortlich. Vor seiner Tätigkeit bei VMware war Herrod Senior Director of Software bei Transmeta Corporation und zählte zu den federführenden Entwicklern der „Code Morphing“-Technologie.

### Chuck Hollis

#### Vice President und CTO Global Marketing, EMC Corporation

Chuck ist ein bedeutendes Mitglied des EMC-Management-Teams und arbeitet im strategischen Bereich für Marketing, Business Development und Technologie. Er ist ein in der Branche bekannter Blogger (<http://chucksblog.emc.com>) und leitet die Initiative sozialer Medien von EMC.

### Uri Rivner

#### Head of New Technologies, Identity Protection & Verification, RSA, The Security Division of EMC

Uri ist bei RSA dafür verantwortlich, neue Technologien und Innovationen von der Idee in die Wirklichkeit umzusetzen. Er war wesentlich an der Entwicklung der risikobasierten Authentifizierung, der Anti-Fraud-Technologie und des RSA eFraudNetwork beteiligt. Er blickt auf 15 Jahre Erfahrung in den Bereichen Business Development, internationales Marketing und Projektmanagement zurück und hat bereits eng mit zahlreichen international führenden Finanzdienstleistern an der Entwicklung von Lösungen gegen Online-Angriffe zusammengearbeitet. Uri hält regelmäßig Vorträge über weltweite Trends im Bereich Online-Betrug.

### Ben Verghese

#### Chief Management Architect & Senior Director, R&D, VMware, Inc.

Ben ist für die Koordination und Konsistenz der Architektur der Management-Produkte und -Plattformen von VMware verantwortlich. Ben kam im Jahr 2000 als Teil des VMware ESX Server 1.0-Teams zu VMware und war danach für das Produkt VMware vCenter verantwortlich. Vor seiner Zeit bei VMware arbeitete Ben als Forscher im Bereich Rechnerarchitektur und Betriebssysteme bei DEC Western Research Labs. Außerdem war er bereits für Apollo Computers und Hewlett-Packard tätig.

## Cloud-Lösungen: Leitlinien für Experten im Bereich Identitäts- und Datenschutz im Cloud Computing

Der Vormarsch des Cloud Computing wird neue Möglichkeiten für leistungsstarke und benutzerfreundliche Datenschutzlösungen schaffen. Der Grund dafür ist die Zusammenarbeit von Unternehmen aus den Bereichen Informationstechnologie und Sicherheit, um die Möglichkeiten der Virtualisierungsebene für Überwachung und Steuerung in vollem Umfang nutzen zu können.

Um Best Practices für den Schutz von Daten und Identitäten in Clouds zu implementieren, müssen Unternehmen möglicherweise neue technologische Lösungen in Betracht ziehen. Die unten beschriebenen Produkte und Services entsprechen den Best Practices, die in diesem RSA Security Brief beschrieben wurden. Diese Lösungsübersicht stellt keine umfassende Liste geeigneter Lösungen von RSA, EMC oder VMware dar. Sie dient vielmehr als Ausgangspunkt für Sicherheitsverantwortliche, die sich über ihre Möglichkeiten informieren möchten.

### Überwachung von Rechenzentren und Mandantenfähigkeit

VMware verfügt über ein umfassendes Portfolio an Sicherheitslösungen und -services für virtualisierte Plattformen, die eine detaillierte Zugangskontrolle ermöglichen, um die Aktivitäten von Cloud-Anbietern möglichst transparent zu gestalten.

- VMware ESX® und ESXi sind die meistgenutzten Hypervisoren weltweit. Beide Lösungen ermöglichen Unternehmen die Nutzung eigener Sicherheitszertifikate zum Schutz von Remote-Sitzungen. Der Benutzername, das Passwort und die Netzwerkpakete, die zum ESX Server durch Übermittlung über das Netzwerk geschickt werden, werden standardmäßig verschlüsselt, wenn die VMware Remote Console oder das VMware Management Interface verwendet werden.
- VMware vCenter® Server bietet eine IT-Administratoren eine einmalige Einsicht und zentrale Steuermöglichkeit jeder Ebene der virtuellen VMware vSphere-Infrastruktur. Mittels einer detaillierten Rechteverwaltung wird festgelegt, welche Personen virtuelle Maschinen für bestimmte Clouds und Speichergeräte bereitstellen dürfen. In Kombination mit gut definierten betrieblichen Prozessen und Abläufen bieten diese Funktionen im Idealfall maximale Mobilität für virtuelle Maschinen bei der Risikoverwaltung.
- VMware vCenter Lifecycle Manager ermöglicht IT-Administratoren die Nachverfolgung der Eigentümer virtueller Maschinen und verfügt über Berichterstellungsfunktionen, die die Einrichtung, Bereitstellung und Stilllegung virtueller Maschinen aufzeichnen. So können IT-Administratoren die Bereitstellung virtueller Maschinen besser steuern und die Ressourcennutzung optimieren, um einen höheren ROI zu erzielen.

- VMware vShield Zones versetzt Unternehmen in die Lage, Anwendungen effizient in einem Pool gemeinsam genutzter Rechnerressourcen zu nutzen, während die Netzwerksegmentierung von Benutzern und Daten erhalten bleibt. Administratoren können virtuelle Maschinen über mehrere Zonen so überbrücken, mit einer Firewall versehen oder isolieren, je nachdem, welche Unternehmensrichtlinien gelten. Des Weiteren ist eine bequeme, zentrale Verwaltung möglich, da sich die gesamte virtuelle Maschine und das Netzwerk selbst detailliert einsehen lassen. Außerdem können zonenbasierte Richtlinien einfach konfiguriert werden. Somit sinkt das Fehlerrisiko.

### Datenverschlüsselung und Tokenisierung

Verschlüsselungslösungen haben üblicherweise viele verschiedene Anwendungen, Clients und Geräte, die kryptografische Funktionen ausüben. Die Verwaltung aller Rechte bzw. die Verschlüsselung, Entschlüsselung und Erzeugung von Schlüsseln für all diese Komponenten ist nicht nur schwierig, sondern auch zeitraubend und kostspielig. RSA bietet Unternehmen ein Managementsystem für Verschlüsselungsschlüssel, das sich problemlos auch für private Netzwerke nutzen lässt.

- RSA® Key Manager Suite ist ein Managementsystem für Verschlüsselungsschlüssel, mit dem Unternehmen diese auf Anwendungs-, Datenbank- und Speicherebene verwalten lassen. RSA Key Manager senkt die Total-Cost-of-Ownership für die Verschlüsselung, da Administratoren die Speicherung und Verwaltung der Schlüssel über eine zentrale Konsole genauestens steuern können.
- RSA Professional Services bieten einen neuen Tokenisierungs-Service, der die RSA Key Manager Suite ergänzt und die Verwendung von Token-Werten zur Maskierung und zum Schutz vertraulicher Daten ermöglicht. Die RSA SafeProxy™-Architektur nutzt eine einzigartige Kombination von Tokenisierung, erweiterter Verschlüsselung und PKI-Technologien zum Schutz vertraulicher Daten mit mehrstufigem Sicherheitsansatz.

### Gemeinsame Verwaltung digitaler Identitäten

Systeme für domainübergreifende Identitäten schlagen einen Mittelweg zwischen sicheren Transaktionen und der Benutzerfreundlichkeit für Anwender beim Zugriff auf Cloud-Services ein. Der Anwender kann bereits vorhandene Benutzerdaten verwenden, um auf Informationen und Services auf einer anderen Website oder in einem anderen Cloud-Modell zuzugreifen. Domainübergreifende Identitäten ermöglichen Unternehmen den bequemen und zugleich sicheren Zugriff auf verteilte Ressourcen. Dabei ist die Kontrolle sensibler Daten zu jeder Zeit sichergestellt.

- RSA® Federated Identity Manager ist für Cloud Computing geeignet. Diese flexible Lösung für die gemeinsame Nutzung digitaler Identitäten verwendet aktuellste Standards für Web-Services und ermöglicht Unternehmen den sicheren Austausch von Anwenderidentitäten zwischen internen Geschäftsbereichen sowie mit Kunden und Partnern. RSA Federated Identity Manager bietet Out-of-the-Box-Funktionalität und eine leistungsstarke Verwaltungskonsole, die die Verwaltung domainübergreifender Identitäten deutlich vereinfacht. RSA Federated Identity Manager lässt sich problemlos in jede beliebige Infrastruktur für die Identitätsverwaltung integrieren und ist vollständig zu anderen Systemen kompatibel, da die Lösung auf Branchenstandards wie XML, SOAP, SAML 2.0 und WS-Federation 1.0 basiert und zeitgleich mit neuen Standards weiterentwickelt wird.
- RSA® Access Manager gewährt berechtigten Benutzern Single Sign-On-Zugriff auf Anwendungen in Intranets, Extranets, privaten Clouds und Internetmärkten. So können Unternehmen eine große Anzahl von Benutzerkonten verwalten, während gleichzeitig eine zentralisierte Sicherheitsrichtlinie eingehalten wird, die Compliance sicherstellt und Unternehmensressourcen vor unberechtigtem Zugriff schützt.

### Starke, risikobasierte Authentifizierung

Die branchenführenden Authentifizierungslösungen von RSA unterstützen Unternehmen dabei, Benutzeridentitäten und den Zugriff auf Informationen zu schützen. RSA sorgt bei mehr als 250 Millionen Anwendern für sichere digitale Identitäten, schützt pro Jahr mehrere Milliarden geschäftliche Transaktionen und verwaltet die Vertraulichkeit von Daten in zehntausenden Anwendungen weltweit.

- RSA® Identity Verification ermöglicht die wissensbasierte Authentifizierung bei der ersten Anmeldung. Der Benutzer wird gebeten, seine Identität durch das Beantworten von Fragen nachzuweisen, die auf Informationen basieren, die aus öffentlichen Datensätzen und kommerziell verfügbaren Quellen stammen. Die von RSA Identity Verification vorgeschlagenen Antwortmöglichkeiten sind für jede Person einzigartig. Die Wahrscheinlichkeit, dass eine andere als die richtige Person die korrekten Antworten geben kann, ist verschwindend gering. RSA Identity Verification sorgt auch für verbesserte Genauigkeit bei der Benutzerauthentifizierung, da das mit einer Identität verbundene Risiko ermittelt wird. Das System lässt sich an Identitäten oder Transaktionen mit hohem Risiko anpassen, indem der Schweregrad der Fragen beim Authentifizierungsprozess geändert wird.
- RSA SecurID® ist die Standardlösung für die starke Zwei-Faktor-Authentifizierung und zeichnet sich seit 25 Jahren durch herausragende Leistung und Innovation aus. Markenzeichen dieser Lösung ist ein Sicherheitstoken, z.B. ein physisches Gerät (Schlüsselanhänger oder USB-Stick) oder

ein Software-Token, der in Mobiltelefonen gespeichert ist. Der Token generiert alle 60 Sekunden einen neuen Authentifizierungscode. RSA SecurID gilt als weitaus sicherer als Authentifizierungssysteme, die mit herkömmlichen Passwörtern arbeiten. Außerdem ist RSA SecurID einfacher in der Handhabung als Challenge-Response-Verfahren, bei denen ein gültiger Zugangscode erst nach Ausführung mehrerer Schritte generiert wird.

- RSA® Adaptive Authentication ist eine risikobasierte Multifaktor-Authentifizierungsplattform, die umfassenden Schutz für Webportale, SSL-VPN-Anwendungen und Verwaltungslösungen für den Cloud-Zugriff bietet. Verdächtige und risikoreiche Aktivitäten werden anhand mehrerer Hundert gemessener Indikatoren erkannt. In den meisten Fällen erfolgt die Risikobewertung im Hintergrund anhand von Geräteerkennung, Verhaltensmustern, Benutzerprofilen und RSA eFraudNetwork™-Daten. Diese transparente Multifaktor-Authentifizierung sorgt für eine höhere Sicherheit im Unternehmen, ohne die Benutzerfreundlichkeit zu beeinträchtigen. RSA Adaptive Authentication ist als Software-as-a-Service oder als Standortinstallation erhältlich und schützt mehr als 250 Millionen Online-Nutzer in aller Welt. Derzeit wird die Lösung in mehr als 8.000 Unternehmen im Gesundheitswesen, im Bereich Finanzdienstleistungen, staatlichen Stellen, im Versicherungswesen, der Automobilindustrie, in Fertigungsunternehmen, der Immobilienbranche und der Pharmaindustrie eingesetzt.

### Fraud Prevention und Malware-Erkennung

RSA bietet modernste Tools und Services an, die Unternehmen dabei unterstützen, sich selbst und auch Kunden vor Betrug zu schützen. Die RSA-Lösungen zur Erkennung und Vermeidung von Online-Betrug setzen auf dem umfangreichen Know-how von RSA über Betrugstrends und verwertbare Informationen, Forensik und Entwicklung auf und bieten Online-Nutzern und ihren Aktivitäten vollständigen Schutz. Die Services RSA eFraudNetwork™ und RSA FraudAction™ werden hauptsächlich zum Schutz vor Finanzbetrug verwendet, sie können aber auch vor Cyber-Kriminalität in Unternehmen und unberechtigtem Zugriff schützen, z.B. der Industriespionage oder der versehentlichen Offenlegung vertraulicher Kundendaten und Transaktionen.

- RSA eFraudNetwork™ ist das branchenweit erste und größte Netzwerk zum Thema Online-Betrug. Die Anwendergemeinde nutzt Informationen über betrügerische Aktivitäten und macht sie publik. Zu den Mitgliedern zählen mehr als 50 der weltweit führenden Finanzdienstleister sowie Kunden- und Kreditkartenunternehmen, mehrere Tausend regionale Banken und Kreditgenossenschaften sowie die meisten großen Internetdienstleister. Der eFraudNetwork-Service dient dazu, proaktiv Profile, Muster und Verhaltensweisen von Betrügern in mehr als 65 Ländern zu erkennen und zu verfolgen. Sobald ein aktives Betrugsmuster identifiziert wird, werden alle

Informationen über den Betrugsversuch an alle Mitglieder des Netzwerks weitergeleitet, um Finanzdienstleistern und deren Kunden proaktive Sicherheit gegen neue schädliche Betrugsfälle zu bieten.

- RSA Fraud Action™ ist ein bewährter, verwalteter Service, der von über 300 Unternehmen genutzt wird, um Kunden vor Online-Phishing, Pharming und Trojaner-Angriffen zu schützen. RSA FraudAction ist ein schlüsselfertiger Outsourcing-Service, der Unternehmen dabei unterstützt, Investitionen in Ressourcen zu senken und dennoch schnell eine Lösung bereitzustellen. Gefährdete Bereiche werden rund um die Uhr überwacht und durch Erkennungsmaßnahmen, sofortige Alarme und Berichte, Forensik und weitere Gegenmaßnahmen vor Online-Betrug geschützt. Dieser Service wird auch von weltweit führenden Internetdiensteanbietern genutzt, um betrügerische Webseiten erkennen, blockieren und schließen zu können.

Kernstück des FraudAction-Service von RSA ist das hochmoderne Anti-Fraud Command Center (AFCC). Erfahrene Betrugsanalysten bieten Services in nahezu 200 Sprachen an, um Betrugsfälle in aller Welt besser erkennen und abwehren zu können. Seit 2003 haben der FraudAction-Service und das AFCC dazu beigetragen, Finanzbetrug in Höhe von 1,5 Mrd. US-Dollar und 225.000 Phishing-Angriffe zu unterbinden.

#### Cloud Event Management und Audits

- Die RSA enVision®-Plattform für das Log-Management dient zur Erfassung, Benachrichtigung und Analyse von Protokoll-daten, mit der Unternehmen die Compliance vereinfachen und schnell auf gefährliche Sicherheitsprobleme reagieren können. Die RSA enVision 3-in-1-Plattform ist ein leistungsstarkes SIEM- und Log-Management-System, mit dem sich große Datenmengen in Echtzeit aus jeder Ereignisquelle und beliebig großen Rechnerumgebungen zusammenstellen und analysieren lassen. Die RSA enVision-Plattform lässt sich einfach skalieren, sodass Filterung und Bereitstellung von Agenten nicht mehr notwendig sind. Mehr als 1.700 Kunden, darunter große internationale Unternehmen und Regierungsbehörden, haben sich für RSA enVision entschieden, um ihre Compliance zu vereinfachen, die Sicherheit zu erhöhen und den IT- und Netzwerkbetrieb zu optimieren.

#### Schutz vor Datenverlust (DLP)

Heutzutage ist das Unternehmenspersonal stark von der Zusammenarbeit mit Kollegen, Lieferanten und Kunden abhängig, die große Datenmengen in digitaler Form über E-Mail, Sofortnachrichten (IM) und andere Cloud- und Netzwerkanwendungen gemeinsam nutzen. Ein Großteil dieser Daten ist vertraulich und unterliegt Compliance-Richtlinien. Werden solche auf unangemessene Weise mit Dritten außerhalb des Unternehmens genutzt, entstehen geschäftliche Risiken. Lösungen zum Schutz vor Datenverlust verhindern die nicht autorisierte Übertragung

von Daten – ganz gleich, ob diese versehentlich oder in krimineller Absicht erfolgt – durch Überwachung, Nachverfolgung und, falls nötig, das Blockieren von Datenströmen.

- Die RSA® Data Loss Prevention (DLP) Suite bietet einen richtlinienbasierten Ansatz zum Schutz von Daten in Rechenzentren, Netzwerken und an Endpunkten. So können Kunden vertrauliche Daten im gesamten Unternehmen klassifizieren, lokalisieren und nachverfolgen, Kontrollmechanismen implementieren und Aktivitäten berichten und prüfen, um die Richtlinienkonformität zu gewährleisten. Die RSA DLP Suite senkt die Total-Cost-of-Ownership durch hohe Skalierbarkeit, automatisierte Datenschutz-Services und die branchenweit umfassendste Bibliothek zum Schutz und zur Klassifizierung von Daten. Sie umfasst drei Komponenten:

##### RSA DLP Datacenter

DLP Datacenter unterstützt Unternehmen dabei, vertrauliche Daten zu finden und nachzuverfolgen. Dabei spielt es keine Rolle, wo sich diese Daten im Rechenzentrum befinden, z.B. in Dateisystemen, Datenbanken, E-Mail-Systemen und großen SAN/NAS-Umgebungen.

##### RSA DLP Network

DLP Network überwacht und steuert vertrauliche Daten, die das Netzwerk verlassen.

##### RSA DLP Endpoint

DLP Endpoint unterstützt den Anwender dabei, vertrauliche Daten an Endpunkten wie z.B. auf Notebooks und Desktops zu finden, zu überwachen und zu steuern.

Die RSA DLP-Suite ist mit RSA enVision für Log-Management und -Analyse integriert, um Sicherheitsmaßnahmen durch verschlankte Vorfallesverwaltung und Arbeitsabläufe zu vereinfachen.

#### Einhaltung von Compliance-Anforderungen in offenen Clouds

EMC verbessert die Richtlinienkonformität durch optimierte Services für das Cloud Computing, die die intelligente Bereitstellung und die automatische Verschiebung von Daten unterstützen. Diese Services unterstützen Unternehmen wirksam dabei, die richtigen Informationen automatisch zum richtigen Zeitpunkt an den richtigen Ort weiterzuleiten.

- EMC Atmos ist ein optimierter Service für das Cloud Computing zum Speichern und Weiterleiten von Daten. Atmos vereint eine hohe Skalierbarkeit und Mandantenfähigkeit sowie verschiedene Zugangsmöglichkeiten. So erhalten Unternehmen äußerste Flexibilität, wenn es um die Nutzung von Web-Service-APIs für Cloud-basierte Anwendungen oder ältere Protokolle für dateibasierte Systeme geht. Zusammen mit der RSA Data Loss Prevention Suite wird EMC Atmos zu einer intelligenten, datenbewussten Storage-Cloud und ist in der Lage, richtlinienbasierte Verwaltung durchzuführen, um Daten automatisch an verschiedene Standorte weiterzuleiten.



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC

RSA, RSA Security, eFraudNetwork, FraudAction, SecurID und enVision sind eingetragene Warenzeichen von RSA Security Inc. in den Vereinigten Staaten oder anderen Ländern. VMware, vCenter und ESX sind Warenzeichen oder eingetragene Warenzeichen von VMware, Inc. in den Vereinigten Staaten oder anderen Ländern. EMC und Atmos sind Warenzeichen oder eingetragene Warenzeichen der EMC Corporation. Alle weiteren hier angeführten Produkte und Services sind Warenzeichen ihrer jeweiligen Inhaber. ©2009 RSA Security Inc. Alle Rechte vorbehalten.

CLWD BRF1009