Die Wahl eines Cloud-Anbieters ist Vertrauenssache

Einen vertrauenswürdigen Cloud-Anbieter erkennen Sie am SSL-Zertifikat von Thawte.

Die Wahl eines Cloud-Anbieters ist Vertrauenssache

Einleitung

Cloud-Computing verändert die IT-Landschaft zusehends und Unternehmen stellen sich nicht mehr die Frage, *ob* sie Cloud-Computing einführen sollten, sondern *wann*. Besonders interessant sind hier sogenannte öffentliche Cloud-Lösungen von externen Anbietern, durch die Unternehmen ihre Kosten senken und ihre Flexibilität erhöhen können. Diese Cloud-Angebote bringen zwar enorme wirtschaftliche Vorteile, stellen auf der anderen Seite aber auch ein erhebliches Risiko für Unternehmen dar, die unternehmensinterne Daten schützen und unzählige Vorschriften von Gesetzgebern und Branchenverbänden einhalten müssen.

Viele Cloud-Anbieter können jedoch die von Unternehmen gestellten Sicherheitsanforderungen erfüllen. Hierbei spielen SSL-Zertifikate eine bedeutende Rolle. Das SSL-Protokoll (SSL = Secure Sockets Layer) schützt Daten während der Übertragung. Dieses Whitepaper soll als Leitfaden für die objektive Entscheidungsfindung dienen, wenn es um das Pro und Contra von Cloud-Lösungen geht. Dazu haben wir einige Fragen zusammengestellt, die Sie vor der Auswahl eines Anbieters mit den verschiedenen Kandidaten besprechen sollten. Außerdem wird erläutert, wie SSL-Zertifikate von einer vertrauenswürdigen Zertifizierungsstelle (CA) die sichere und unbedenkliche Nutzung der Cloud für geschäftliche Vorgänge ermöglichen.

Cloud-Computing: neue Möglichkeiten, neue Sicherheitsrisiken

Die meisten Unternehmen betrachten Kosteneinsparungen als den wichtigsten unmittelbaren Vorteil von Cloud-Computing. Sie profitieren von geringeren Aufwendungen für Investitionen und Betriebskosten im IT-Bereich, bedarfsabhängig verfügbaren Kapazitäten im Selbstbedienungsbetrieb und nutzungsabhängigen Abrechnungsmodellen – und werden dadurch flexibler und wendiger. Der Service-Anbieter wiederum kann durch die Kombination von standardisierten Ressourcen und einer großen Kundenzahl enorme Kosteneinsparungen aufgrund der gebündelten Größenvorteile erzielen. Viele auf die Anforderungen von Unternehmen ausgerichtete Hosting-Anbieter sind bereits gut am Markt etabliert und verfügen mit ihren Mitarbeitern, ihren Prozessen und der eingesetzten Technik über die zentralen Kompetenzen, die nötig sind, um das Potenzial von Cloud-Computing auszuschöpfen.

Trotz der unbestreitbaren wirtschaftlichen Vorteile bleiben Unternehmen aufgrund von Vorbehalten auf den Gebieten Sicherheit, Compliance und Datenschutz noch zurückhaltend bei der Umstellung auf Cloud-Dienste. Eine IDC-Umfrage unter IT-Verantwortlichen ergab, dass Cloud-Dienste vor allem mit Sicherheitsbedenken zu kämpfen haben.[1] Das Marktforschungsunternehmen Gartner Research nennt sieben Bereiche[2], in denen Unternehmen beim Einsatz von Cloud-Computing mit Sicherheitsrisiken rechnen müssen. Gartner empfiehlt Unternehmen, bei der Auswahl eines Cloud-Anbieters auf die folgenden Aspekte zu achten:

- **Zugriffsrechte:** Cloud-Anbieter sollten belegen können, dass sie die gebotene Sorgfalt bei der Auswahl ihrer Mitarbeiter, der Aufsicht und der Durchsetzung von Zugangsbeschränkungen walten lassen.

- **Einhaltung gesetzlicher Vorschriften (Compliance):** Unternehmen behalten die Verantwortung für ihre Daten auch dann, wenn diese in einer öffentlichen Cloud abgelegt sind. Sie sollten daher sicherstellen, dass die Provider bereit sind, sich einem Audit zu unterziehen.

An Cloud-Computing führt kein Weg vorbei

„Manche sind der Ansicht, dass Cloud-Computing der bedeutendste Paradigmenwechsel seit der Erfindung des Internets ist. Andere halten es lediglich für eine Modeerscheinung. Eines ist jedenfalls sicher: Die Cloud-Technologie hat sich schnell den ersten Platz auf der Prioritätenliste jedes IT-Chefs erobert."

– Quelle: Gartner EXP Worldwide Survey (http://www.gartner.com/it/ page.jsp?id=1283413)

„Immer mehr Unternehmen strömen in die Cloud und Marktforscher wie Gartner Research schätzen, dass Unternehmen aus allen Ländern in den nächsten fünf Jahren insgesamt 112 Milliarden US-Dollar für Cloud-Dienste ausgeben werden."

– Quelle: Gartner Research (http://www. gartner.com/it/page.jsp?id=1389313)

---

1. Quelle: IDC eXchange (http://blogs.idc.com/ie/?p=730)

2. „Assessing the Security Risks of Cloud Computing" (http://www.gartner.com/DisplayDocument?id=685308) Gartner, 3. Juni 2008

- **Speicherort der Daten:** Der Anbieter sollte angeben, wo sich seine Rechenzentren befinden und ob er bestimmte Anforderungen bei der Datensicherheit garantieren kann.

- **Datenabschottung:** Da die meisten öffentlichen Clouds von mehreren Kunden gemeinsam genutzte Umgebungen sind, muss der Hosting-Anbieter hundertprozentig garantieren können, dass die Daten der verschiedenen Kunden voneinander getrennt bleiben.

- **Datenwiederherstellung:** Es muss gewährleistet sein, dass der Hosting-Anbieter die Daten im Notfall vollständig wiederherstellen kann.

- **Überwachung und Berichte:** Es ist nicht einfach, Vorgänge in einer öffentlichen Cloud zu überwachen und zu protokollieren. Unternehmen sollten sich daher von ihrem Hosting-Anbieter zusichern lassen, dass dieser sie bei Untersuchungen unterstützen kann.

- **Datenverfügbarkeit:** Firmenpleiten kommen vor. Unternehmen, die in Cloud-Computing einsteigen möchten, sollten sich daher eingehend nach der Portabilität ihrer Daten erkundigen, damit sie weiterhin darauf zugreifen und ihre Daten auf anderen Plattformen nutzen können, falls der Anbieter vom Markt verschwindet.

Um die Vorteile von Cloud-Computing auszunutzen, ohne die Gefahr für Sicherheit und Compliance zu erhöhen, kommt es für Unternehmen auf die Wahl des richtigen Anbieters an: Dieser muss unbedingt verantwortungsvoll mit Sicherheitsrisiken beim Cloud-Computing wie den oben aufgeführten umgehen. Wenn das Unternehmen nicht mehr nur einen Cloud-Dienst, sondern mehrere Dienste von verschiedenen Anbietern nutzt, muss es sich bei jedem einzelnen Anbieter um alle diese Kriterien kümmern. Und jeder Anbieter hat seine eigene Infrastruktur, seine eigenen Richtlinien, sein eigenes Sicherheitsprofil. Die Anforderungen an die Vertrauenswürdigkeit werden damit so komplex, dass ein überall verfügbares und äußerst zuverlässiges Verfahren notwendig ist, das die Sicherheit der Daten beim Verschieben in die Cloud, innerhalb der Cloud und aus der Cloud gewährleistet.

SSL – der Schlüssel zum sicheren Cloud-Computing für Unternehmen

SSL ist ein Sicherheitsprotokoll, das Browser und Webserver verwenden, um die Daten der Benutzer während der Übertragung zu schützen. Dieses Sicherheitsprotokoll ist der Standard für den vertrauensvollen Datenaustausch im Internet. Ohne das überall einsetzbare SSL-Protokoll gäbe es keine Vertrauenswürdigkeit im Internet. Bei jeder Datenübertragung kommt SSL ins Spiel. Wenn ein Unternehmen Daten in der Cloud ablegt, ist der sichere Netzwerkzugriff auf diese Daten wichtig. Ferner kann man davon ausgehen, dass die Daten bei routinemäßigen Verwaltungsarbeiten des Anbieters zwischen verschiedenen Servern innerhalb der Cloud verschoben werden. Egal, ob die Daten zwischen Server und Browser oder zwischen zwei Servern verschoben werden – mit SSL sind sie geschützt.

Zwei Bestandteile von SSL sind es, die einige der Sicherheitsprobleme beim Cloud-Computing lösen: zuerst einmal die SSL-Verschlüsselung, die vertrauliche Daten während der Übertragung von einem Server zu anderen Servern oder zu Browsern vor unbefugten Mitlesern schützt. Der zweite Vorteil ist vielleicht sogar noch wichtiger: SSL legt fest, dass bestimmte Server und Domänen als vertrauenswürdig gelten. Ein SSL-Zertifikat kann belegen, dass ein bestimmter Server bzw. eine bestimmte Domäne in der Tat zu der Person bzw. dem Unternehmen gehört, die als Eigentümer angegeben werden. Um diesen Vorteil nutzen zu können, muss der Cloud-Anbieter SSL-Zertifikate von einer anerkannten Zertifizierungsstelle (CA) beziehen.

Abschottung der Daten und sicherer Zugriff auf Cloud-Services

Daten in der Cloud abzulegen, bringt grundsätzlich das Problem der Abschottung dieser Daten mit sich. Bei Daten, die auf herkömmliche Weise im Unternehmen gespeichert werden, hat das Unternehmen nicht nur die volle Kontrolle über den Aufbewahrungsort, sondern auch über die Zugriffsberechtigungen. In einer Cloud-Umgebung dagegen ist das ganz anders, denn hier ist es der Cloud-Anbieter, der über den Serverstandort und den Speicherort der Daten bestimmt. Eine fachgerecht implementierte SSL-Lösung kann vertrauliche Daten aber beim Verschieben innerhalb der Cloud, zwischen Servern des Cloud-Anbieters und zu den Browsern der Benutzer schützen.

Verschlüsselung

Unternehmen sollten von ihrem Cloud-Anbieter eine Kombination von SSL und Servern verlangen, die die Verschlüsselung von Sitzungen mit 256 Bit unterstützen. Damit sind ihre Daten während des Verschiebens mit mindestens der gängigen Verschlüsselungsstärke geschützt, so dass unbefugt abgefangene Daten unlesbar sind.

Authentifizierung

Bevor auch nur ein Datenbit in die Cloud verschoben wird, sollten Unternehmen außerdem zur Bedingung machen, dass der Eigentümer der Server authentifiziert ist. Selbstsignierte SSL-Zertifikate stellen keine ausreichende Authentifizierung dar. Nur von einer unabhängigen, vertrauenswürdigen Stelle ausgestellte SSL-Zertifikate können den Eigentümer wirksam authentifizieren. Das Bestehen auf einem von einer anerkannten und unabhängigen Zertifizierungsstelle ausgestellten SSL-Zertifikat zur Authentifizierung des Servers macht es praktisch unmöglich, dass ein unberechtigter Server Zugang zur Umgebung des Cloud-Anbieters erhält.

Gültigkeit des Zertifikats

Nach der Authentifizierung eines Servers und einer Domäne bleibt das dafür ausgestellte SSL-Zertifikat für eine bestimmte Dauer gültig. Um auch den seltenen Fall zu berücksichtigen, dass ein Zertifikat aus irgendeinem Grund kompromittiert wird, lässt sich zweifelsfrei feststellen, ob das Zertifikat seit seiner Ausstellung widerrufen wurde: Bei jedem „Handshake“ zu einer SSL-Sitzung wird überprüft, ob das SSL-Zertifikat in einer aktuellen Datenbank mit widerrufenen Zertifikaten enthalten ist.

Für diese Überprüfung gibt es derzeit zwei Standardverfahren: OCSP (Online Certificates Status Protocol) und CRL (Certificate Revocation List). Beim OCSP-Verfahren wird die Zertifizierungsstelle gefragt, ob das Zertifikat widerrufen wurde. Ist dies nicht der Fall, ist die Bahn frei für den „Handshake“. Beim CRL-Verfahren muss der Browser die aktuelle Widerrufsliste von der Zertifizierungsstelle abrufen und selbst überprüfen, ob das fragliche Zertifikat darin enthalten ist.

Das OCSP-Verfahren gilt insgesamt als zuverlässiger, da die hierbei verwendeten Daten immer aktuell sind und die Überprüfung mit geringerer Wahrscheinlichkeit aufgrund von zu starkem Datenverkehr im Netzwerk abgebrochen wird. SSL-Zertifikate, die sich nur auf das CRL-Verfahren verlassen, sind weniger empfehlenswert, denn bei hohem Datenverkehr im Netzwerk kann dieser Schritt versehentlich übersprungen werden: Einige Browser interpretieren eine unvollständige CRL-Prüfung als Bestätigung, dass das Zertifikat nicht auf der Widerrufsliste steht, und würden „Handshake“ und Sitzungsstart trotz eines widerrufenen SSL-Zertifikats durchführen. In einer solchen Situation könnte sich ein betrügerisch geführter Server mit einem widerrufenen Zertifikat erfolgreich als authentifizierter Server ausgeben – dem unbefugten Zugriff auf Daten wären damit Tür und Tor geöffnet.

Erleichterung von Compliance

Ein wichtiges Thema ist natürlich auch die Einhaltung gesetzlicher Vorschriften, die Compliance. Zum Thema Datenschutz gibt es eine Fülle gesetzlicher Bestimmungen. Allen voran ist hier das Bundesdatenschutzgesetz zu nennen, das für die Bundesrepublik Deutschland die Erhebung, Speicherung und Weitergabe von Daten genau regelt. Aber damit nicht genug, so gibt es beispielsweise noch auf europäischer Ebene die Datenschutzrichtlinie 95/46/EG, in den USA für Aktiengesellschaften den Sarbanes-Oxley-Act (kurz SOX) und international den „Payment Card Industry Data Security Standard“ (kurz PCI) für Unternehmen, die Zahlungen per Kreditkarte akzeptieren.

Ein Unternehmen kann zwar einem Anbieter von Cloud-Diensten IT-Leistungen übertragen, verantwortlich für die Einhaltung aller maßgeblichen Gesetze, Richtlinien und Vorschriften bleibt dennoch weiterhin das Unternehmen. Und je nachdem, wo sich die Daten und die Server gerade befinden, können auch noch Gesetze anderer Länder ins Spiel kommen. Selbst bei der Auslagerung von

Wie funktioniert SSL?

Ein SSL-Zertifikat enthält einen öffentlichen und einen privaten Schlüssel sowie Angaben zur bestätigten Identität des Inhabers. Wenn ein Browser (der Client) eine mit SSL gesicherte Domäne aufrufen möchte, sendet der Server seinen öffentlichen Schlüssel an den Client, um ein Verschlüsselungsverfahren festzulegen und einen eindeutigen Schlüssel für diese Sitzung zu generieren. Der Client bestätigt, dass er den Aussteller des SSL-Zertifikats anerkennt und ihm vertraut. Dieses Verfahren – bei dem im Hintergrund komplexe Vorgänge und viele Prüfungen ablaufen – bezeichnet man als „SSL-Handshake“. Es steht am Anfang einer sicheren Sitzung, bei der die Sicherheit und Integrität der Daten geschützt sind.

Daten steht also das Unternehmen für die Sicherheit und Unversehrtheit seiner Daten in der Pflicht. Da sich die IT-Leitung des Unternehmens bei der Einhaltung all dieser Anforderungen nicht ausschließlich auf den Cloud-Anbieter verlassen darf, muss das Unternehmen sich von diesem bestätigen lassen, dass die Einhaltung der Anforderungen überprüft wird. Anbieter von Cloud-Diensten, die sich externen Audits und Sicherheitszertifizierungen verweigern, „signalisieren damit, dass Kunden sie nur für allereinfachste Aufgaben nutzen können“, stellte Gartner fest.

Auch technische Änderungen an der Cloud-Computing-Umgebung können die Compliance des Cloud-Kunden unbemerkt schwächen. Ebenso können Aktualisierungsmaßnahmen wie Änderungen der Zugriffsberechtigungen, neue Funktionen, der Umstieg auf Mobilgeräte oder Änderungen an der Netzwerkkonfiguration die Compliance beeinträchtigen.[3] Wie bei der Abschottung von Daten kann auch hier SSL Schutz vor einer unbeabsichtigten Offenlegung geschützter oder vertraulicher Daten bieten, denn die Zugangsverwaltung sowie weitere Maßnahmen im Rahmen der gesetzlich geforderten Sorgfaltspflicht sind automatisiert. Durch die SSL-Verschlüsselung werden alle sensiblen Daten für Dritte, die diese Daten abfangen oder anzeigen, unbrauchbar.

Überwachung der Herkunft der Daten

SSL entschärft auch den dritten wichtigen Punkt: den des Speicherortes. Öffentliche Clouds sind quasi eine Blackbox: Sie ermöglichen zwar einerseits permanenten Datenzugriff von überall, verschleiern auf der anderen Seite aber den konkreten Standort der Server und somit der Daten. Wenn aber der Cloud-Anbieter Daten bei der Übertragung mit SSL verschlüsselt, kann sich das Unternehmen darauf verlassen, dass seine Daten unterwegs sicher sind.

Angesehene unabhängige SSL-Anbieter wie Thawte stellen übrigens keine SSL-Zertifikate für Server in bestimmten Ländern wie Nordkorea und dem Iran aus. Wenn sich also der Cloud-Anbieter für eine Zertifizierungsstelle mit einer solchen Richtlinie

3. „Domain 10: Guidance for Application Security V2.1“, Cloud Security Alliance, Juli 2010.

entscheidet, um eine vertrauenswürdige Authentifizierung und Verschlüsselung auf allen seinen Servern zu erhalten, können die Kunden dieses Anbieters sicher sein, dass er ihre Daten nicht auf Rechnern in diesen Ländern ablegt.

Weitere Vorteile von SSL

Das Unternehmen muss wissen, wie sein Cloud-Anbieter, der rund um den Globus Server betreibt, die Daten vor Verlust schützt. Gartner sagt dazu, dass „bei jedem Angebot, das die Daten und die Anwendungsinfrastruktur nicht an mehreren Standorten repliziert, das Risiko eines totalen Datenverlusts besteht“. Ferner stellt Gartner fest, es sei die Pflicht jedes Unternehmens mit Daten in der Cloud, sich darüber zu informieren, ob der Cloud-Anbieter in der Lage ist, die Daten vollständig von Sicherungskopien oder Replikationen wiederherzustellen, und wie lange dies dauern würde. Zur Vorbeugung von Datenverlusten sollten Anbieter von Cloud-Diensten ein Daten-Repository zu Backup-Zwecken pflegen. Kommt es zu einem Absturz, versuchen die Hosts, die Daten von Backup-Servern wiederherzustellen. Mit SSL werden Backup und Wiederherstellung in zweifacher Hinsicht sicherer für Unternehmen: Erstens sorgt SSL dafür, dass Daten, die von einem Backup oder einem gespiegelten Server abgerufen werden, verschlüsselt übertragen werden. Und zweitens sorgt SSL dafür, dass die Server, von denen die Backup-Daten abgerufen werden, als vertrauenswürdige Datenquellen authentifiziert sind.

SSL-Zertifikate machen die Cloud vertrauenswürdiger

Die Entscheidung für einen Anbieter von Cloud-Diensten erfordert ein hohes Maß an Vertrauen. Wenn es um Anwendungen geht, die eine zentrale Rolle für den Unternehmenserfolg spielen, darf nichts dem Zufall überlassen werden. Unternehmen müssen hierbei auf bestimmten unverzichtbaren Kriterien für die Zuverlässigkeit bestehen und SSL-Zertifikate sind eine gut erkennbare und anerkannte Möglichkeit dafür. Im Gegenzug kann ein fehlender oder nicht funktionierender SSL-Schutz jedes Vertrauen im Handumdrehen zerstören.

Ein Beispiel: Ein Unternehmen entscheidet sich, seinen Online-Shop bei einem Cloud-Anbieter zu betreiben. Leider tritt ein Problem mit dem SSL-Zertifikat der Shop-Website auf. Wer den Online-Shop besucht, sieht daher als erstes beunruhigende Fehlermeldungen wie etwa „Sichere Verbindung fehlgeschlagen“ oder „Problem mit dem Sicherheitszertifikat der Website“. Wird der Besucher daraufhin die Warnung seines Browsers ignorieren und seinen Einkauf in einem scheinbar nicht vertrauenswürdigen Shop fortsetzen? Wohl kaum.

Die Kette des Vertrauens reicht also über den Cloud-Anbieter hinaus bis zum Anbieter seiner Sicherheitslösung. Die Sicherheit des Cloud-Dienstes ist nur so zuverlässig wie die verwendete Sicherheitstechnik. Cloud-Anbieter sollten daher SSL-Zertifikate von einer anerkannten, zuverlässigen und unabhängigen Zertifizierungsstelle verwenden. Idealerweise sollten die Zertifikate die Sitzungen mit 256 Bit verschlüsseln und es sollte für eine kompromisslose Authentifizierung gesorgt sein.

Manche Anbieter generieren ihre SSL-Schlüssel auf Servern mit Debian-Betriebssystemen. Aufgrund eines Sicherheitsproblems können Zertifikate, die zwischen 2006 und 2008 auf solchen Systemen erstellt wurden, unsicher sein. Unternehmen sollten sich unbedingt vergewissern, dass ihr Cloud-Anbieter sich weder auf Server noch auf SSL-Zertifikate verlässt, die von diesem Problem betroffen sein können. Da bei SSL-Zertifikaten eine Gültigkeit von bis zu sechs Jahren möglich ist, kann es sein, dass solche unsicheren Zertifikate noch im Einsatz sind.[4]

Authentifizierung schafft Vertrauen in Identitätsbelege

Das Vertrauen in Identitätsbelege steht und fällt mit dem Vertrauen in den Aussteller des Belegs, denn dieser bürgt für dessen Authentizität. Zertifizierungsstellen können mehrere Authentifizierungsverfahren verwenden, um zu überprüfen, ob die Angaben des Zertifikatsinhabers der Wahrheit entsprechen.

Die Wahl sollte daher auf einen Cloud-Anbieter fallen, der mit einer Zertifizierungsstelle zusammenarbeitet, die bekannt ist, das Vertrauen der Browser-Hersteller genießt, bei der Authentifizierung hohe Maßstäbe anlegt und eine äußerst zuverlässige Infrastruktur betreibt. Bei SSL-Zertifikaten ist eine Authentifizierung auf vier Stufen möglich. Zwar ermöglichen sie alle den verschlüsselten Austausch von Daten, aber es gibt große Unterschiede bei der Belastbarkeit der Authentifizierung von Server oder Domäne: Hier geht es um die Sorgfalt, mit der die Eigentümer von Server und Domäne und die Kontrollverhältnisse überprüft werden.

- **Selbstsignierte Zertifikate** ermöglichen nur die Verschlüsselung und sonst nichts. Diese Art von SSL-Zertifikaten erfüllt die Sicherheitsansprüche von Unternehmen nicht.

- **Zertifikate mit Domänenvalidierung** leisten nur eine rudimentäre Authentifizierung, indem sie bestätigen, dass die Person, die das Zertifikat beantragt, die Rechte am betreffenden Domänennamen hat. Diese Zertifikate sind für Server-Browser-Verbindungen nicht empfehlenswert, denn weder wird mit ihnen die Identität des für die Domäne bzw. den Server verantwortlichen Unternehmens überprüft, noch zeigen sie diese an.

4. Quelle: http://voices.washingtonpost.com/securityfix/2008/05/debian_and_ubuntu_users_fix_yo.html

- **SSL-Zertifikate mit Unternehmensvalidierung** bieten eine zuverlässige und für Cloud-Computing geeignete Authentifizierung, denn es wird überprüft, dass das Unternehmen hinter der Domäne bzw. dem Server tatsächlich existiert und dass der Antragsteller ein autorisierter Vertreter dieses Unternehmens ist. Diese SSL-Zertifikate sind für Server-Browser-Verbindungen geeignet, bieten allerdings nicht jene optimalen Leistungsmerkmale, die beim Endbenutzer Vertrauen schaffen.

- **Zertifikate mit Extended Validation (EV)** sind die beste Wahl für Server-Browser-Verbindungen, denn hier wird die anspruchsvollste Authentifizierung durchgeführt und sie weisen am deutlichsten auf die Sicherheit der Verbindung hin. Mit EV-Zertifikaten wird neben der rechtlichen, physischen und geschäftlichen Existenz des Unternehmens auch das Recht des Unternehmens an der Verwendung des betreffenden Domänennamens überprüft. Ein EV-Zertifikat belegt, dass die Identität des Unternehmens durch offizielle Dokumente Dritter bestätigt wurde und dass es sich bei dem Antragsteller um einen autorisierten Vertreter des Unternehmens handelt.

Nur ein SSL-Zertifikat mit diesem höchsten Authentifizierungsniveau löst bestimmte eindeutige Kennzeichen im Browser des Website-Besuchers aus: In einer grün hinterlegten Adressleiste werden der Name des Unternehmens und der Name der Zertifizierungsstelle, die das SSL-Zertifikat ausgestellt hat, angezeigt. Sieht ein Website-Besucher die grüne Adressleiste, kann er sich darauf verlassen, dass die Verbindung sicher ist. Zahlreiche Unternehmen konnten nach der Einrichtung von Extended Validation SSL einen deutlichen Anstieg der abgeschlossenen Transaktionen verzeichnen. Dies sind nur einige der Gründe, warum EV-Zertifikate bei der Bereitstellung von Anwendungen und Diensten über die Cloud die erste Wahl sind.

Fazit: Verlassen Sie sich auf Bewährtes

SSL ist ein bewährtes Verfahren und der Grundstein für Sicherheit im Cloud-Computing. Bei der Wahl des Cloud-Anbieters sollte ein Unternehmen auch die Sicherheitsoptionen berücksichtigen, für die sich der Cloud-Anbieter entschieden hat. Verwendet dieser zum Beispiel SSL-Zertifikate von einer vertrauenswürdigen Zertifizierungsstelle, ist das bereits ein starkes Indiz für sein ernsthaftes Engagement für den Datenschutz in seiner Cloud-Umgebung. Das Unternehmen sollte dem Cloud-Anbieter gegenüber auch unmissverständlich deutlich machen, dass Handhabung und Eindämmung der Risikofaktoren, für die SSL keine Lösung darstellt, eine große Rolle spielen. Hier sollte sich das Unternehmen bei der Bewertung (und Buchung) von Cloud-Computing-Angeboten an den sieben Kategorien von Gartner orientieren.

Cloud-Anbieter wiederum sollten SSL-Zertifikate von einer anerkannten, zuverlässigen und unabhängigen Zertifizierungsstelle verwenden. Das SSL-Zertifikat sollte 256-Bit-Verschlüsselung mit globalen Root-Zertifikaten mit 2048 Bit bieten. Außerdem sollte für eine kompromisslose Authentifizierung gesorgt sein. Die Rechenzentren der Zertifizierungsstelle, die das SSL-Zertifikat ausstellt, müssen nach militärischen Maßstäben gesichert sein und die Maßnahmen zur Datenwiederherstellung im Notfall müssen optimal auf Datenschutz und -verfügbarkeit ausgerichtet sein. Die SSL-Zertifizierungsstelle muss ihre Authentifizierungsverfahren jährlich von einer vertrauenswürdigen externen Audit-Organisation überprüfen lassen. SSL-Produkte von Thawte erfüllen alle diese Anforderungen.

Falls Sie weitere Fragen haben, wenden Sie sich an einen unserer Verkaufsberater:

- **Telefonisch**
  - **USA: +1 888 484 2983**
  - **Großbritannien: +44 203 450 5486**
  - **Südafrika: +27 21 819 2800**
  - **Deutschland: +49 69 3807 89081**
  - **Frankreich: +33 1 57 32 42 68**
- **Per E-Mail an Enterprisesales@thawte.com**
- **Besuchen Sie unsere Website: http://www.thawte.de/ssl/volume-discount-ssl-certificates/index.html**

Mit den renommierten digitalen Zertifikaten des führenden internationalen Online-Sicherheitsexperten Thawte schützen Sie Ihr Unternehmen und bauen so bei Ihren Kunden Vertrauen auf. Seit 17 Jahren bietet Thawte seinen Kunden Stabilität, Zuverlässigkeit, eine bewährte Infrastruktur und erstklassigen Kunden-Support. Deshalb entscheiden sich Kunden weltweit für Thawte als ihren internationalen Sicherheitspartner.

UID 190/2/13