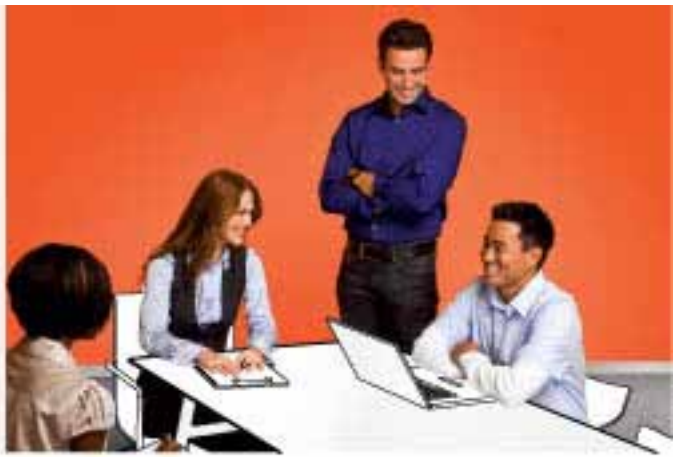
STRATEGIEPAPIER



Auswahl eines vertrauenswürdigen Cloud-Anbieters

SSL ist eine sichere Brücke zur Cloud

GeoTrust®

Zusammenfassender Überblick

Die IT-Landschaft verändert sich durch das Cloud Computing in rasantem Tempo, und bei Gesprächen über die Akzeptanz der Cloud-Technologie geht es nicht mehr um das "Falls", sondern das "Wann". Unternehmen haben ein starkes Interesse an ausgelagerten ("öffentlichen") Cloud-Angeboten, die zur Kosteneinsparung beitragen und den Handlungsspielraum des Unternehmens vergrößern können. Diese Cloud-Services bieten enorme wirtschaftliche Vorteile. Sie stellen für Unternehmen, die firmeneigene Datenbestände sichern müssen und gleichzeitig unzählige Branchenrichtlinien und behördliche Richtlinien einhalten müssen, jedoch auch erhebliche potenzielle Risiken dar.

Viele Cloud-Service-Provider können die von Unternehmen benötigte Sicherheit bieten, und SSL (Secure Sockets Layer)-Zertifikate sind ein Bestandteil der Lösung. SSL ist genauer gesagt die Lösung zum Sichern von Daten, wenn diese übertragen befinden.

Dieses Strategiepapier möchte Unternehmen darin unterstützen, pragmatische Entscheidungen zu treffen, wo und wann Cloud-Lösungen verwendet werden können, indem auf spezielle Probleme eingegangen wird, die Unternehmen mit Hosting Providern besprechen sollten, bevor sie einen Anbieter wählen, und indem betont wird, wie SSL von einer vertrauenswürdigen Zertifizierungsstelle Unternehmen darin unterstützen kann, Geschäfte in der Cloud vertrauenswürdig abzuwickeln.

Bereit oder nicht, hier kommt die Cloud

Cloud Computing wird manchmal als der bedeutsamste Paradigmenwechsel seit dem Aufkommen des Internets bezeichnet. Andere halten es nur für eine Modeerscheinung. Eines ist jedoch sicher: Cloud-Technologie hat es rasch an die Spitze der Prioritätsliste jedes IT-Managers geschafft.[1] Organisationen bauen die Nutzung von Cloud-Services aus, und Industrieanalysten, wie Gartner Research, schätzen, dass Unternehmen weltweit in den nächsten 5 Jahren zusammen 112 Milliarden US-Dollar für Cloud-Services ausgeben werden.[2]

Neue Geschäftsideen

Die meisten Organisationen nennen Kosteneinsparungen als den unmittelbarsten Vorteil von Cloud Computing. Für das Unternehmen bieten Cloud-Services niedrigere IT-Investitions- und Betriebskosten, bedarfsorientierte Kapazität mit Selbstbedienungsbereitstellung und nutzungsabhängige (Pay-per-Use) Preismodelle für größere Flexibilität und größeren Handlungsspielraum. Der Service-Provider erreicht wiederum exponentiell größere Skalierungseffekte, indem er einem großen Kundenstamm eine standardisierte Palette von Computing-Ressourcen zur Verfügung stellt. Viele Hosting Provider für Unternehmen sind auf dem Markt bereits gut positioniert und verfügen über die Kernkompetenzen (Personal, Prozesse, Technologie), um dem Unternehmen Cloud Computing anbieten zu können.

Neue Sicherheitsherausforderungen für IT

Trotz der eindeutigen wirtschaftlichen Vorteile der Nutzung von Cloud-Services bremsten Bedenken hinsichtlich Sicherheit, Compliance und Datenschutz die Akzeptanz durch Unternehmen. Eine IDC-Umfrage unter IT-Managern kam zu dem Ergebnis, dass Sicherheit das Thema Nummer 1 bei IT-Cloud-Services ist.[3] Gartner Research hat sieben konkrete Sicherheitsrisikobereiche[4] im Zusammenhang mit Cloud Computing für Unternehmen identifiziert und empfiehlt Organisationen, bei der Auswahl des Anbieters einige wichtige Punkte anzusprechen:

1. **Zugriffsrechte** – Cloud-Service-Provider sollten nachweisen können, dass sie angemessene Einstellungs-, Aufsichts- und Zugriffssteuerungspraktiken umsetzen, um eine Verwaltungsdelegierung durchzusetzen.
2. **Einhaltung gesetzlicher Bestimmungen** – Unternehmen sind für ihre eigenen Daten verantwortlich, auch wenn sich diese in einer öffentlichen Cloud befinden, und sollten sicherstellen, dass ihre Anbieter bereit und willens sind, sich Prüfungen zu unterziehen.
3. **Datenspeicherort** – Bei der Auswahl eines Hosting Providers sollte unbedingt die Frage gestellt werden, wo sich deren Rechenzentren befinden, und ob sie folgende konkrete Anforderungen an den Datenschutz erfüllen.
4. **Datensegregation** – Die meisten öffentlichen Clouds sind gemeinsam genutzte Umgebungen, und es ist unabdingbar, dass Hosting Provider die vollständige Datensegregation für sichere Mehrinstanzenfähigkeit garantieren können.
5. **Datenwiederherstellung** – Das Unternehmen muss sicherstellen, dass sein Hosting Provider bei einem Systemausfall die Daten vollständig wiederherstellen kann.
6. **Überwachung und Berichterstellung** – Die Überwachung und Protokollierung der Aktivitäten in öffentlichen Clouds erweisen sich als schwierig. Unternehmen sollten deshalb einen Nachweis verlangen, dass ihre Hosting Provider Ermittlungen unterstützen können.
7. **Gewährleistung der geschäftlichen Verfügbarkeit** – Firmen kommen und gehen, und Unternehmen sollten kritische Fragen zur Portabilität ihrer Daten stellen, um eine fehlende Kompatibilität und einen möglichen Verlust ihrer Daten zu vermeiden, falls die Firma den Betrieb einstellt.

Um von den Vorteilen des Cloud Computing profitieren zu können, ohne Sicherheits- und Compliance-Risiken zu erhöhen, dürfen Unternehmen nur mit vertrauenswürdigen Service-Providern zusammenarbeiten, die mit diesen und anderen Herausforderungen der Cloud-Sicherheit umgehen können. Wenn Unternehmen außerdem von der Nutzung nur eines Cloud-basierten Diensts auf die Nutzung von mehreren verschiedenen Anbietern übergehen, müssen sie alle diese Probleme über mehrere Operatoren hinweg verwalten, wobei diese jeweils unterschiedliche Infrastrukturen, Betriebsrichtlinien und Sicherheitskenntnisse aufweisen. Durch diese Komplexität der Vertrauensanforderungen wächst der Bedarf an einem generell verfügbaren und sehr zuverlässigen Verfahren zur Sicherung Ihrer Daten, wenn diese an die Cloud, aus dieser heraus und innerhalb der Cloud übertragen werden.

1. Quelle: Gartner EXP Worldwide Survey (http://www.gartner.com/it/page.jsp?id=1283413)
2. Quelle: Gartner Research (http://www.gartner.com/it/page.jsp?id=1389313)
3. Quelle: IDC eXchange (http://blogs.idc.com/ie/?p=730)
4. "Assessing the Security Risks of Cloud Computing" (http://www.gartner.com/DisplayDocument?id=685308) Gartner, 3. Juni 2008.

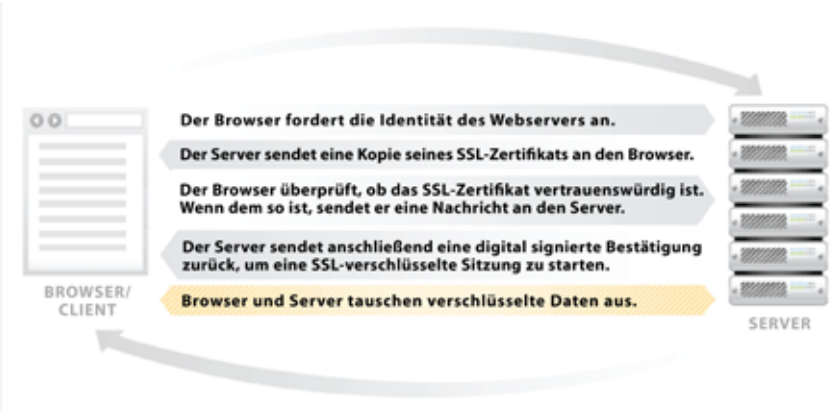
SSL ist eine Brücke zu sicheren Daten in der Cloud

SSL ist ein von Webbrowsern und Webservern verwendetes Sicherheitsprotokoll, das Benutzern hilft, ihre Daten während der Übertragung zu schützen. SSL ist der Standard zum Einrichten eines vertrauenswürdigen Informationsaustauschs über das Internet. Ohne die Ubiquität von SSL wäre jegliches Vertrauen im Internet schlichtweg unmöglich. SSL kommt immer dann ins Spiel, wenn der Speicherort von Daten geändert wird. Wenn ein Unternehmen seine Daten in der Cloud verwaltet, spielt der sichere Netzwerkzugriff auf die Daten eine wichtige Rolle. Diese Daten werden außerdem wahrscheinlich zwischen Servern in der Cloud übertragen, wenn der Service-Provider routinegemäß Verwaltungsaufgaben durchführt. Unabhängig davon, ob Daten zwischen Server und Browser oder zwischen Server und Server übertragen werden, trägt SSL zur Sicherung der Daten bei.

SSL bietet zwei Dienste an, um mit einige Probleme im Zusammenhang mit der Cloud-Sicherheit zu beseitigen. Erstens verhindert die SSL-Verschlüsselung, dass private Daten von nicht autorisierten Benutzern gelesen werden, wenn sie zwischen Servern sowie zwischen Server und Browser übertragen werden. Der zweite und möglicherweise wichtigere Vorteil liegt darin, dass einem bestimmten Server und einer bestimmten Domäne vertraut werden kann. Mit einem SSL-Zertifikat kann authentifiziert werden, dass ein bestimmter Server und eine bestimmte Domäne der Person oder Organisation gehören, die er/sie zu repräsentieren vorgibt. Hierfür muss der Hosting Provider SSL von einer Drittanbieter-Zertifizierungsstelle (CA) verwenden.

Wie funktioniert SSL?

Ein SSL-Zertifikat enthält ein öffentliches und privates Schlüsselpaar sowie geprüfte Kennungsinformationen. Wenn ein Browser (oder Client) auf eine gesicherte Domäne verweist, teilt der Server seinen öffentlichen Schlüssel (über das SSL-Zertifikat) mit dem Client, um ein Verschlüsselungsverfahren und einen eindeutigen Codierungsschlüssel für die Sitzung einzurichten. Der Client bestätigt, dass er den Aussteller des SSL-Zertifikats erkennt und ihm vertraut. Dieser Prozess, der auf einer hochentwickelten Backend-Architektur mit doppelten Sicherheitsprüfungen basiert, ist als "SSL-Handshake" bekannt und kann eine sichere Sitzung starten, bei der der Datenschutz und die Datenintegrität eingehalten werden.



Sicherstellung von Datensegregation und sicherem Zugriff

Bei der Cloud-Speicherung sind Datensegregationsrisiken immer präsent. Bei traditioneller Onsite-Speicherung kontrolliert der Eigentümer des Unternehmens genau, wo sich die Daten befinden, und wer genau darauf zugreifen kann. In einer Cloud-Umgebung ist dies ganz anders, da der Cloud-Service-Anbieter kontrolliert, wo sich die Server und die Daten befinden. Mit einer ordnungsgemäßen SSL-Implementierung können vertrauliche Daten jedoch gesichert werden, wenn sie in der Cloud zwischen Speicherorten und zwischen Cloud-Anbieter-Servern und Endbenutzern in Browsern übertragen werden.

Verschlüsselung

Unternehmen sollten von ihrem Cloud-Anbieter die Verwendung einer Kombination aus SSL und Servern fordern, die mindestens 128-Bit-Sitzungsverschlüsselung (oder vorzugsweise die leistungsfähigere 256-Bit-Verschlüsselung) unterstützen. Auf diese Weise werden ihre Daten mit den der Industrienorm entsprechenden oder besseren Verschlüsselungsstufe gesichert, wenn sie zwischen Servern oder zwischen Server und Browser übertragen werden, wodurch abgefangene Daten nicht gelesen werden können.

Authentifizierung

Unternehmen sollten auch verlangen, dass die Eigentumsverhältnisse des Servers authentifiziert werden, bevor auch nur 1 Bit Daten zwischen Servern übertragen wird. Selbstsignierte Zertifikate bieten keine Authentifizierung. Nur unabhängige SSL-Zertifikate von Drittanbietern ermöglichen eine legitime Eigentumsauthentifizierung. Die Forderung nach einem kommerziell ausgestellten SSL-Zertifikat von einer Drittanbieter-Zertifizierungsstelle, die den Server authentifiziert hat, macht es praktisch unmöglich, einen nicht autorisierten Server zu erstellen, der die Umgebung des Cloud-Anbieters unterwandern kann.

Gültigkeit des Zertifikats

Nachdem Server und Domäne authentifiziert wurden, gilt das für das jeweilige Gerät ausgestellte SSL-Zertifikat für eine festgelegte Zeitdauer. Wenn in seltenen Fällen ein SSL-Zertifikat in irgendeiner Weise kompromittiert wurde, kann mit einer ausfallsicheren Prüfung verifiziert werden, dass das Zertifikat seit der ursprünglichen Ausstellung nicht widerrufen wurde. Immer, wenn ein Handshake für eine SSL-Sitzung initiiert wird, wird das SSL-Zertifikat mit einer aktuellen Datenbank für widerrufenen Zertifikate verglichen.

Für diese Validitätsprüfung werden zurzeit zwei Normen eingesetzt, Online Certificates Status Protocol (OCSP) und Zertifikatswiderrufsliste (CRL). Bei OCSP wird eine Abfrage an die Zertifizierungsstelle gesendet, in der angefragt wird, ob dieses Zertifikat widerrufen wurde. Die Zertifizierungsstelle antwortet mit ja oder nein. Falls die Antwort nein ist, wird der Handshake eingeleitet. Für CRL muss andererseits der Browser die aktuellste Liste der widerrufenen Zertifikate von der Zertifizierungsstelle herunterladen und die Liste selbst auf das Vorhandensein des Zertifikats prüfen.

Die Online Certificate Status Profile (OCSP)-Norm wird weithin als zuverlässiger angesehen, weil sie aktueller ist und weniger zu Zeitüberschreitungen infolge des Netzwerkdatenverkehrs neigt. SSL-Zertifikate, die sich nur auf die CRL-Norm verlassen, sind weniger wünschenswert, weil bei hohem Netzwerkdatenverkehr folgender Schritt ausfallen kann: Einige Browser interpretieren eine unvollständige CRL-Prüfung fälschlicherweise als Bestätigung, dass ein Zertifikat nicht in der Zertifikatswiderrufsliste vorhanden ist, vollführen demzufolge einen Handshake und leiten eine Sitzung basierend auf einem widerrufenen SSL-Zertifikat ein. In einem solchen Szenario könnte ein nicht autorisierter Server ein widerrufenes Zertifikat nutzen, um sich erfolgreich als legitimer Server auszugeben, wodurch eine hinreichende Grundlage für eine Datenverletzung gegeben ist.

Erleichtern der Einhaltung gesetzlicher Bestimmungen

Als nächstes gibt es die Risiken bei der Einhaltung gesetzlicher Bestimmungen. Wenn es um sichere und vertrauliche Daten geht, werden Unternehmen zahlreiche Vorschriften aufgebürdet. Diese reichen von Gesetzen wie dem Sarbanes-Oxley (SOX) Act, der nur öffentliche Unternehmen betrifft, bis zu dem Sicherheitsstandard der Payment Card Industry (PCI-DSS), der jede Firma betrifft, die Kartenzahlung akzeptiert, bis zu dem Health Insurance Portability and Accountability Act (HIPAA), der jedes Unternehmen betrifft, bei dem auch nur die geringste Wahrscheinlichkeit besteht, dass es mit Patientendaten zu tun haben könnte. In Europa gelten die Datenschutzrichtlinien der EU, und Kanada verfügt über ein gleichwertiges Gesetz zum Schutz personenbezogener Daten und elektronischer Dokumente (Personal Information Protection and electronic Documents Act, PIPEDA).

Wenn eine Organisation ein IT-Outsourcing an einen Cloud-Service-Anbieter durchführt, ist die Organisation nach wie vor für die Compliance mit SOX, PCI, HIPAA und anderen geltenden Gesetzen verantwortlich – und möglicherweise darüber hinaus, je nachdem, wo sich die Server und Daten in einem gegebenen Zeitraum befinden. Infolgedessen ist das Unternehmen auch im Falle des Outsourcings für die Sicherheit und Integrität der Daten dann verantwortlich. Die IT-Manager des Unternehmens können sich nicht nur darauf verlassen, dass der Cloud-Anbieter diese Anforderungen erfüllt. Deshalb muss das Unternehmen dafür sorgen, dass der Cloud-Anbieter sich um einen Überblick über die Compliance bemüht. Cloud-Computing-Anbieter, die sich externen Prüfungen und Sicherheitszertifizierungen entziehen, "signalisieren, dass sie von Kunden nur für die trivialsten Funktionen genutzt werden können", gibt Gartner zu verstehen.

Technologische Änderungen an der Cloud-Computing-Umgebung können die Compliance der Kunden eines Cloud-Computing-Anbieters unwissentlich reduzieren. Funktions-Upgrades, wie Änderungen der Berechtigung, neue Funktionen, Einführung von Mobilgeräten sowie Netzwerkänderungen können die Compliance ebenfalls beeinflussen. [5] In diesem Fall und bei der Datensegregation verhindert die SSL-Verschlüsselung die versehentliche Veröffentlichung geschützter oder privater Daten, da die gesetzlich geforderte Sorgfalt und der Datenzugriff automatisiert sind. Die SSL-Verschlüsselung macht alle vertraulichen Daten für Drittanbieter, die diese abfangen oder anzeigen, nutzlos.

Fernhalten von Daten an unerwünschten Speicherorten

SSL kümmert sich um den dritten Risikobereich, den Datenspeicherort, auf die gleiche Weise. Ein öffentliche Cloud ist mit einer Blackbox vergleichbar. Obwohl sie von überall aus Zugriff auf Daten ermöglichen, verschleiern sie den physikalischen Ort der Server und Daten. Wenn ein Cloud-Anbieter jedoch zur Verschlüsselung der Daten bei deren Standortänderung SSL verwendet, hat ein Unternehmen die Gewissheit, dass seine Daten sicher sind, wenn sie in der Cloud übertragen werden. Zusätzlich stellen legitime SSL-Drittanbieter, wie GeoTrust oder VeriSign, einem Server in einem Staat mit schlechtem Leumund, wie Nordkorea und Iran, kein SSL-Zertifikat aus. Solange der Cloud-Anbieter auf allen seinen Servern über SSL von einer diese Praxis einhaltenden Zertifizierungsstelle vertrauenswürdige Authentifizierung und Verschlüsselung fordert, weiß ein Unternehmen, dass der Cloud-Anbieter seine Daten nicht auf IT-Hardware in diesen Ländern speichert.

Andere Bereiche, in denen SSL hilfreich ist

Das Unternehmen muss wissen, wie sein Cloud-Anbieter mit weltweit installierten Servern seine Daten im Falle eines Systemausfalls sichert. Gartner erklärt, dass "jedes Angebot, bei dem die Daten und die Infrastruktur der Anwendung nicht auf mehrere Sites repliziert werden, zum Totalausfall führen kann", und dass jedes Unternehmen in der Cloud wissen muss, ob der Cloud-Anbieter die Daten mithilfe von Backups oder Duplikaten vollständig wiederherstellen kann, und wie lange dies dauert.

Zur Vermeidung von Datenverlust sollten Cloud-Service-Anbieter Backup-Daten-Repositorys verwalten. Bei einem Absturz versuchen die Cloud-Hosts, die Daten von Backup-Servern wiederherzustellen. SSL sichert den Backup- und Wiederherstellungsprozess eines Unternehmens mit einer zusätzlichen Sicherheitsschicht. Dadurch wird sichergestellt, dass Daten, auf die von Backup- oder Duplikatservern zugegriffen wird, während der Übertragung verschlüsselt werden, und dass Server, auf die wegen Backup-Daten zugegriffen wird, als legitime Quellen für diese Informationen authentifiziert werden.

5. "Domain 10: Guidance for Application Security V2.1", Cloud Security Alliance, Juli 2010.

Einsatz von SSL zum Aufbau und Bewahren von Vertrauen in die Cloud

Die Verwendung eines Cloud-Service-Anbieters erfordert ein hohes Maß an Vertrauen. Kritische Geschäftsanwendungen dürfen sich nicht auf die Versuchs-und-Irrtums-Methode verlassen. Unternehmen müssen auf entscheidende Zuverlässigkeit bestehen, um Vertrauen aufzubauen, und mit SSL-Zertifikaten ist dies ganz offensichtlich und sofort erkennbar möglich. Fehlendes oder gebrochenes SSL kann dagegen das Vertrauen sofort zunichte machen.

Beispiel: Nehmen wir an, dass ein Unternehmen einen Cloud-Anbieter zum Hosten seiner E-Commerce-Website wählt, der Host jedoch ein Problem mit dem SSL-Zertifikat der Site hat. Ein Benutzer besucht die Site und wird sofort mit der Fehlermeldung "Sichere Verbindung fehlgeschlagen" oder der Meldung "Problem mit dem Sicherheitszertifikat der Website" begrüßt. Wird dieser Benutzer die Browserwarnung ignorieren und sich durchklicken, um eine Transaktion auf einer anscheinend nicht vertrauenswürdigen Site abzuschließen? Wahrscheinlich nicht.

Nicht alle SSL werden gleich erstellt

Die Vertrauenskette erstreckt sich über den Cloud-Anbieter hinaus zu deren Sicherheitsanbieter. Die Sicherheit des Cloud-Anbieters ist nur so gut wie die Verlässlichkeit der von ihm verwendeten Sicherheitstechnologie. Cloud-Anbieter sollten SSL von einer anerkannten, zuverlässigen und sicheren unabhängigen Zertifizierungsstelle verwenden. Ihr SSL sollte mindestens 128-Bit-Sitzungsverschlüsselung und im Optimalfall 256-Bit-Verschlüsselung unterstützen. Außerdem sollte ein strikter Authentifizierungsprozess erforderlich sein.

Unternehmen müssen sicherstellen, dass ihr Cloud-Anbieter ein SSL-Zertifikat verwendet, das nicht geknackt werden kann. Neben der Gewährleistung, dass das SSL von einem autorisierten Drittanbieter stammt, sollte die IT-Organisation des Unternehmens auch die folgenden Sicherheitsanforderungen der SSL-Sicherheit des Cloud-Anbieters verlangen:

- **Eine Zertifizierungsstelle, die ihre globalen Roots** hinter Schichten von industrieüblicher Sicherheit schützt, wobei mehrere Ebenen der elektronischen und physikalischen Sicherheitsmaßnahmen verwendet werden.
- **Eine Zertifizierungsstelle, die für ihre globalen Roots ein Backup für die Notfallwiederherstellung** verwaltet.
- **Globale Roots, die den sichersten neuen Verschlüsselungsstandard nutzen,** der 2048-Bit-RSA-Schlüssel verwendet.
- **Eine verkettete Hierarchie, die ihre SSL-Zertifikate stützt**. Mindestens eine dazwischenliegende Root in der Kette bedeutet eine exponentielle Verbesserung der Verschlüsselungsschutzstufe, um Angriffe auf die globale Root zu verhindern.
- **Sicheres Hashing mithilfe der SHA-1-Norm**, um zu gewährleisten, dass der Inhalt der Zertifikate nicht manipuliert werden kann.

Viele Server verlassen sich zudem auf ein Debian-basiertes Betriebssystem, um ihre SSL-Schlüssel zu generieren. Die fundamentalen Verschlüsselungsfunktionen dieses Systems wurden 2006 bis 2008 angegriffen. Unternehmen sollten darauf achten, dass sich ihr Cloud-Anbieter weder auf Server noch auf SSL-Zertifikate verlässt, die durch diese Sicherheitslücke gefährdet sein könnten. SSL-Zertifikate können mit einer Gültigkeitsdauer von bis zu sechs Jahren ausgestellt werden. Daher ist es möglich, dass SSL mit dieser Sicherheitslücke noch in Gebrauch ist. [6]

Authentifizierung vermittelt Vertrauen in Referenzen

Das Vertrauen in eine Referenz hängt vom Zutrauen zum Aussteller der Referenz ab, weil der Aussteller für die Authentizität der Referenz bürgt. Zertifizierungsstellen verwenden unterschiedliche Authentifizierungsmethoden, um von Organisationen bereitgestellte Informationen zu prüfen. Die beste Wahl ist ein Cloud-Anbieter, der gemäß einer weithin bekannten Zertifizierungsstelle, der Browseranbieter vertrauen, genormt ist, während eine strikte Authentifizierungsmethode und sehr zuverlässige Infrastruktur verwaltet werden.

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

Für SSL gibt es vier Authentifizierungsstufen. Alle ermöglichen einen verschlüsselten Informationsaustausch. Der Unterschied liegt in der Stärke der Server- und Domänenauthentifizierung. Das heißt, welcher Aufwand bei der Validierung der Eigentumsverhältnisse und Kontrolle dieses Servers und der Domäne betrieben wird.

1. **Selbstsignierte Zertifikate** bieten in keiner Weise Authentifizierung, um Verschlüsselung zu ermöglichen. Dieser SSL-Typ bietet nicht die von einem Unternehmen benötigte Sicherheit.
2. **Domänenvalidierte Zertifikate** bieten nur grundlegende Authentifizierung, weil sie lediglich bestätigen, dass der Zertifikatsanforderer zur Verwendung eines bestimmten Domänennamens berechtigt ist. Diese Zertifikate werden für Server-zu-Browser-Verbindungen nicht empfohlen, weil damit die Identität der für diese Domäne oder diesen Server verantwortlichen Organisation nicht überprüft oder angezeigt wird.
3. **Organisationsvalidierte Zertifikate** bieten zuverlässige Authentifizierung für die Cloud, weil damit überprüft wird, dass die für die Domäne oder den Server verantwortliche Organisation tatsächlich existiert und die Person, die das SSL-Zertifikat für diese Domäne oder diesen Server beantragt, ein authentifizierter Vertreter dieser Organisation ist. Diese SSL-Zertifikate sind akzeptable Optionen für Server-zu-Browser-Verbindungen. Sie bieten für den Endbenutzer jedoch nicht die höchste Stufe an vertrauensbildenden Funktionen.
4. **Extended Validation-Zertifikate (EV)** sind die beste Wahl für Server-zu-Browser-Verbindungen, weil sie die höchste Authentifizierungsstufe bieten und damit am eindeutigsten überprüft wird, ob die Verbindung sicher ist. Bei EV-Zertifikaten wird die rechtliche, physikalische und betriebliche Existenz der Organisation geprüft, ebenso wie das Recht dieser Organisation für die Verwendung dieser Domäne. Mit EV ist gewährleistet, dass die Identität der Organisation durch offizielle Unterlagen geprüft wurde, die von einem autorisierten Drittanbieter verwaltet werden, und dass der Zertifikatsanforderer ein autorisierter Vertreter der Organisation ist.

   Ein SSL-Zertifikat mit dieser höchsten Authentifizierungsstufe kann im Webbrowser eines Endbenutzers eindeutige Kennungen auslösen: eine grüne Adressleiste, die den Namen der Organisation und den Namen der Zertifizierungsstelle anzeigt, von der das SSL ausgestellt wurde. Wenn Endbenutzer die grüne Adressleiste sehen, haben sie die absolute Gewissheit, dass ihre Verbindung sicher ist. Zahlreiche Unternehmen haben nach der Bereitstellung von Extended Validation-SSL deutliche Steigerungen bei den abgeschlossenen Transaktionen (durchschnittlich 18 Prozent für VeriSign-Kunden) beobachtet. EV ist aus diesen und anderen Gründen die bevorzugte Wahl zum Hosten von Anwendungen und Diensten in der Cloud.

Zusammenfassung: Entscheiden Sie sich für das Bekannte

SSL ist eine erprobte Technologie und ein Meilenstein der Cloud-Sicherheit. Wenn ein Unternehmen einen Cloud Computing-Anbieter auswählt, sollte das Unternehmen die von diesem Cloud-Anbieter ausgewählten Sicherheitsoptionen berücksichtigen. Das Wissen, dass ein Cloud-Anbieter SSL von einer vertrauenswürdigen Zertifizierungsstelle verwendet, kann zu einem langfristigen Aufbau von Vertrauen in die Verpflichtung dieses Anbieters führen, die in seinem Besitz befindlichen Daten zu sichern.

Bei der Auswahl eines Cloud-Service-Providers müssen Unternehmen mit ihren Cloud-Partnern die Handhabung und Minimierung von Risikofaktoren, die durch SSL nicht beseitigt werden können, auch sehr offen besprechen. Unternehmen sollten die von Gartner vorgeschlagenen sieben Kategorien bei der Bewertung von Cloud Computing-Lösungen (und insbesondere beim Abschluss von Verträgen) berücksichtigen.

Cloud-Anbieter sollten SSL von einer anerkannten, zuverlässigen und sicheren unabhängigen Zertifizierungsstelle verwenden. Deren SSL sollte mindestens 128-Bit-Verschlüsselung und im Optimalfall 256-Bit-Verschlüsselung basierend auf der neuen globalen 2048-Bit-Root unterstützen. Außerdem sollte ein strikter Authentifizierungsprozess erforderlich sein. Die SSL-Genehmigungsinstanz sollte Rechenzentren mit militärischem Sicherheitsstandard und Notfallwiederherstellungs-Sites, die hinsichtlich Datenschutz und Verfügbarkeit optimiert sind, unterhalten. Die Authentifizierungspraktiken der SSL-Zertifizierungsstelle müssen jährlich von einem vertrauenswürdigen Drittanbieter-Prüfer kontrolliert werden. Die Marken GeoTrust®, Thawte® und VeriSign® SSL bieten SSL-Produkte an, die diese Anforderungen erfüllen.

Weitere Informationen

Einen vertrauenswürdigen Cloud-Service-Provider, der die in diesem Strategiepapier genannten Kriterien erfüllt, finden Sie auf der folgenden Website: http://www.geotrust.com/sell-ssl-certificates/strategic-partners.html.

Über GeoTrust

GeoTrust ist führend in Sicherheitsprodukten und der weltweit zweitgrößte digitale Zertifikataussteller. Über 300.000 Kunden in mehr als 150 Ländern setzen auf GeoTrust, um Online-Transaktionen zu sichern und Geschäfte über das Internet abzuwickeln. Durch unsere Palette von digitalen Zertifikaten und Sicherheitsprodukten können Organisationen jeder Größe die Sicherheit ihrer digitalen Transaktionen kostengünstig maximieren.

Kontakt

www.GeoTrust.com/de

UNTERNEHMENSSITZ
GeoTrust, Inc.
350 Ellis Street, Bldg. J
Mountain View, CA 94043-2202, USA
Gebührenfrei in den USA
+1-866-511-4141
Tel +1-650-426-5010
Fax +1-650-237-8871
enterprisesales@geotrust.com

EMEA VERKAUFSBÜRO
GeoTrust, Inc.
8th Floor Aldwych House
71-91 Aldwych
London, WC2B 4HN, Großbritannien
Tel +44.203.0240907
Fax +44.203.0240958
sales@geotrust.co.uk

APAC VERKAUFSBÜRO
GeoTrust, Inc.
134 Moray Street
South Melbourne VIC 3205
Australien
sales@geotrustaustralia.com

11-08-2011 NT110108