Wachsendes Vertrauen in die Cloud

Cloud-Dienste gehören mittlerweile zum festen Bestandteil der IT-Abläufe und sind bei mehr als 90 % aller Unternehmen weltweit im Einsatz. Vielfach setzen Unternehmen auf das „Cloud First"-Prinzip und implementieren interne Dienste nur dann, wenn keine entsprechende Cloud-Variante verfügbar ist. Aus diesem Grund findet bei IT-Architekturen ein rapider Wandel hin zum hybriden Modell mit öffentlichen und privaten Cloud-Komponenten statt: Die Umfrageteilnehmer gehen davon aus, dass 80 % ihres IT-Budgets innerhalb von 15 Monaten (Durchschnittswert) für Cloud-basierte Lösungen ausgegeben werden.

93 %

aller Unternehmen **nutzen Cloud-Dienste** in irgendeiner Form.

49 %

der Umfrageteilnehmer haben wegen fehlender Cyber-Sicherheitskompetenzen **ihre Cloud-Implementierung verlangsamt**.

62 %

der befragten Unternehmen **speichern persönliche Kundendaten** in öffentlichen Clouds.

Für diesen Jahresbericht zum Stand der Dinge bei der Migration zur Cloud führte Intel Security im September 2016 eine Umfrage unter mehr als 2.000 IT-Experten aus unterschiedlichen Branchen und Ländern sowie Unternehmen verschiedenster Größen durch. Einer der Schwerpunkte des diesjährigen Berichts war die Auswirkung des anhaltenden Mangels an qualifizierten Sicherheitsexperten auf die Cloud-Implementierung. Andere Ziele umfassten das Verständnis der Implementierung verschiedener Cloud-Nutzungsmodelle, die Identifizierung der größten Sorgen im Zusammenhang mit öffentlichen und privaten Cloud-Diensten sowie die Untersuchung der zunehmenden Auswirkungen der Schatten-IT.

Durchgeführt wurde die Umfrage unter hochrangigen IT-Entscheidungsträgern bei kleinen (500 bis 1.000 Mitarbeiter), mittleren (1.000 bis 5.000 Mitarbeiter) und großen Unternehmen (mehr als 5.000 Mitarbeiter) aus Australien, Brasilien, Deutschland, Frankreich, Großbritannien, Japan, Kanada, Mexiko, Singapur und den USA sowie den Golfstaaten Saudi-Arabien und Vereinigte Arabische Emirate.

Die Fakten

- Cloud-Dienste werden bei 93 % aller Unternehmen eingesetzt, wobei Software-, Infrastructure- oder Platform-as-a-Service-Angebote zum Einsatz kommen.
- Die durchschnittliche Anzahl an Cloud-Diensten, die bei Unternehmen verwendet werden, fiel von 43 im Jahr 2015 auf 29 im Jahr 2016 – ein Indiz dafür, dass eine Konsolidierung der Cloud-Anbieter oder -Lösungen stattfindet. Auch die Cloud-Architekturen haben sich stark verändert. Waren im Jahr 2015 noch in erster Linie rein private Clouds vertreten, gewinnen mittlerweile öffentliche Clouds immer mehr an Bedeutung, sodass im Jahr 2016 vorrangig hybride öffentlich/private Infrastrukturen eingesetzt wurden.
- Beinahe die Hälfte (49 %) der befragten Experten gab an, dass die Cloud-Implementierung bei ihnen aufgrund fehlender Cyber-Sicherheitskompetenzen gebremst wird. Dieser Mangel ist insbesondere in Japan, Mexiko und den Golfstaaten zu spüren.
- Die Vertrauenswürdigkeit und das Ansehen öffentlicher Cloud-Dienste wird von Jahr zu Jahr besser. Die meisten Unternehmen stufen öffentliche Cloud-Dienste als sicherer als private Clouds ein und trauen ihnen eher zu, die Gesamtbetriebskosten zu senken und die allgemeine Datentransparenz zu verbessern. Das Verhältnis von Führungskräften, die öffentlichen Clouds vertrauen bzw. ihnen misstrauen, liegt mittlerweile bei mehr als 2:1.

intel Security

Kurzfassung

52 %

der Teilnehmer konnten eine **Malware-Infektion zu einer SaaS-Anwendung zurückverfolgen**.

40 %

aller Cloud-Dienste werden **ohne Beteiligung der IT-Abteilung bereitgestellt**.

65 %

der befragten IT-Experten meinen, dass die Absicherung der Cloud durch **„Schatten-Clouds" erschwert** wird.

2 Jahre

Die Zeit, in der die Teilnehmer mit der Implementierung eines vollständig **Software-definierten Rechenzentrums** rechnen.

- Die größere Vertrauenswürdigkeit und das höhere Ansehen öffentlicher Cloud-Dienste sowie das bessere Verständnis der Risiken bei hochrangigen Führungskräften ermutigt mehr Unternehmen, vertrauliche Daten in der öffentlichen Cloud zu speichern. Persönliche Kundendaten werden am häufigsten in öffentlichen Clouds gespeichert (bei 62 % der Befragten).
- Cloud-Anwendungen werden auch weiterhin für Cyber-Attacken missbraucht, und mehr als die Hälfte (52 %) der Umfrageteilnehmer gab an, dass sie definitiv eine Malware-Infektion zu einer SaaS-Anwendung zurückverfolgen konnten.
- Schatten-IT ist eine wachsende Sorge für die IT-Abteilung. Aufgrund der langsameren Implementierung der IT bei gleichzeitig breiter Akzeptanz der Cloud werden beinahe 40 % der Cloud-Dienste ohne die Einbeziehung der IT-Abteilung bereitgestellt. Deshalb glauben 65 % der befragten IT-Experten, dass dieses Phänomen sie daran hindert, die Cloud entsprechend abzusichern.
- Die Virtualisierung privater Rechenzentrumarchitekturen schreitet voran. Im Durchschnitt sind 52 % aller unternehmenseigenen Rechenzentrum-Server virtualisiert, und die meisten Befragten rechnen damit, dass die Umwandlung zum vollständig Software-definierten Rechenzentrum innerhalb von zwei Jahren abgeschlossen sein wird.

Schlussfolgerungen und Empfehlungen

Unternehmen vertrauen Cloud-Diensten ein breites Spektrum von Anwendungen und Daten an, die zum größten Teil vertraulich oder geschäftskritisch sind. Die Daten werden dorthin verlagert, wo sie benötigt werden und am effektivsten sowie effizientesten eingesetzt werden können. Die Sicherheitsmaßnahmen müssen jedoch bereits an den entsprechenden Stellen implementiert sein, um Bedrohungen schnell zu erkennen, das Unternehmen zu schützen und Datenkompromittierungsversuche abzuwehren. Cloud-Dienste ermöglichen erhebliche Kostensenkungen sowie Ressourcen-Einsparungen, und angesichts des breiten Spektrums an Angeboten können Sie die optimale Lösung für das eigene Unternehmen auswählen. Sicherheitsanbieter stellen Tools bereit, mit denen grundlegende Sicherheitsprobleme gelöst werden können, beispielsweise der Schutz übertragener Daten, die Verwaltung des Benutzerzugriffs sowie die Festlegung konsistenter Richtlinien für verschiedene Dienste.

Die Verlagerung vertraulicher Daten in die öffentliche Cloud kann Cyber-Kriminelle anlocken. Angreifer suchen stets nach dem leichtesten Opfer, ganz gleich, wo sich dieses befindet. Integrierte oder einheitliche Sicherheitslösungen sind ein starker Schutz vor diesen Bedrohungen und geben den Sicherheitsverantwortlichen einen Überblick über alle Dienste, die das Unternehmen nutzt, sowie darüber, welche Datensätze mit diesen Diensten ausgetauscht werden dürfen.

Der Missbrauch von Anmeldeinformationen der Benutzer, insbesondere der Administratoren, wird die wahrscheinlichste Angriffsform darstellen. Unternehmen sollten daher sicherstellen, dass sie stets die empfohlenen Vorgehensweisen für die Authentifizierung befolgen, d. h. individuelle Kennwörter, mehrstufige Authentifizierung und – sofern verfügbar – biometrische Kennungen.

Obwohl die Mehrheit davon ausgeht, dass Schatten-IT das Unternehmen gefährdet, werden Sicherheitstechnologien wie Schutz vor Datenkompromittierung (DLP), Verschlüsselung sowie Cloud Access Security Broker (CASB) immer noch zu wenig eingesetzt. Die Integration dieser Tools in ein bestehendes Sicherheitssystem verbessert den Überblick, ermöglicht die Entdeckung von „Schatten-Diensten" und bietet Möglichkeiten zur automatischen Absicherung gespeicherter sowie übertragener Daten in heterogenen Umgebungen.

Sie können zwar Arbeitsschritte an verschiedene Drittanbieter auslagern, doch für die Risiken gilt das leider nicht. Aus diesem Grund müssen Unternehmen bei der Informationssicherheit Kapazitäten zur Risikoverwaltung und -beseitigung aufbauen. Sie sollten eine „Cloud First"-Strategie implementieren, um die Implementierung von Cloud-Diensten für Kostensenkung und Flexibilitätssteigerung zu erleichtern. Gleichzeitig ist es notwendig, die bislang reaktiven Sicherheitsprozesse in proaktive umzuwandeln.

Den vollständigen Bericht können Sie **hier** herunterladen.

intel Security

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com