Bericht

Blauer Himmel oder dunkle Wolken?

Der Stand der Dinge bei der Migration zur Cloud

intel Security

Inhalt

Wir bedanken uns bei den 1.200 Teilnehmern der Kernumfrage für ihre Mitarbeit und insbesondere bei diesen Führungskräften, die wir für diesen Bericht zu ihren Erfahrungen und Ansichten befragen durften:

- Brent Conran, Vice President und Chief Information Security Officer, Intel
- Brian Dye, Corporate Vice President, Intel Security
- Dimitra Liveri, Network and Information Security Officer, European Network and Information Security Agency (ENISA)
- Vanessa Pegueros, Chief Information Security Officer, DocuSign, Inc.
- Jim Reavis, Chief Executive Officer, Cloud Security Alliance
- Dave Shackleford, SANS-Analyst und Chief Executive Officer, Voodoo Security
- Timothy Youngblood, Chief Information Security Officer, Kimberly-Clark

Eine Cloud für jedes Wetter? Eine Frage des Vertrauens

Mittlerweile führt beinahe jedes Einschalten eines elektronischen Geräts zu einem Verarbeitungsvorgang in der Cloud. Die Cloud-basierten Services von Amazon Web Services, Microsoft Azure und anderen Cloud-Anbietern kommen in allen Bereichen von Heimautomatisierung bis zu gewinnbringenden Geschäftsanwendungen zum Einsatz. Die aktuelle Entwicklung sowie die Zukunftsprognosen dieser Verarbeitungsplattform sind eindeutig: Cloud Computing wird zunehmen. Und die Abhängigkeit von der Cloud wird für Verbraucher wie für Unternehmen gleichermaßen erhebliche Auswirkungen haben. Laut unserer Umfrage wird in den nächsten 12 bis 18 Monaten ein großer Teil der Unternehmens-IT-Budgets für öffentliche Cloud-Ressourcen ausgegeben. Einige Fachleute bezeichnen dies als Wendepunkt in der IT.

Doch was bedeutet dieser Wechsel? Erstens muss die Kompetenz der Technologieexperten in diesen Unternehmen erheblich verbessert werden. Zweitens muss das Vertrauen in die Cloud zunehmen, was allerdings auch für die Transparenz der Vorgänge gilt, die unabdingbar ist, damit wir dieses Vertrauen aufbauen können.

Die Cloud wird heute zwar bereits eingesetzt, doch in Zukunft werden ihre Möglichkeiten steigen. So wären wir nicht überrascht, wenn früher oder später kritische Infrastrukturanwendungen sowie -Services in die Cloud wechseln. Wir halten es tatsächlich für möglich, dass abseits von Diskussionen über das Rechenzentrum der Zukunft der „Cloud First"-Ansatz (eine vorrangige Nutzung der Cloud) für viele Anwendungen zur Standardeinstellung wird, während die lokale Bereitstellung zur Ausnahme wird (und nur dort stattfindet, wo sie sinnvoll ist).

Sobald die notwendige Sicherheit gewährleistet ist, können die Möglichkeiten des Cloud Computing für die Unterstützung neuer Anwendungen und fortschrittlicher Unternehmens-Tools zur Produktivitätssteigerung genutzt werden. Unsere Umfrage zeigt jedoch, dass Unternehmen auch weiterhin Zweifel an der Vertrauenswürdigkeit und Sicherheit dieser Verarbeitungsplattform haben.

Durch den zunehmenden Einsatz dieser Plattform haben wir die Möglichkeit, die Vertrauenswürdigkeit entsprechend den Erwartungen von Unternehmen und Verbrauchern zu verbessern. Die ehrenamtlich geführte Cloud Security Alliance, eine der führenden Organisationen bei der Forschung im Bereich Cloud-Sicherheit, wirbt für die Teilnahme anderer Organisationen und ihrer Partner bei diesem grundlegenden Wandel.

– Raj Samani, EMEA Chief Technology Officer, Intel Security
– Jim Reavis, Chief Executive Officer, Cloud Security Alliance

Einführung

Die Anforderungen an moderne Unternehmen zwingen diese dazu, sich nicht mehr auf Pilotprogramme und kleinere Projekte zu beschränken, sondern Cloud Computing immer umfassender einzusetzen. Doch welchen wichtigen Trends sowie Problemen müssen sie dabei Rechnung tragen? Wie können Unternehmen die Vorteile der Cloud nutzen, ohne Sicherheit und Kontrolle zu gefährden?

Für unsere Umfrage, die wir in acht Ländern durchführten, befragten wir 1.200 Entscheidungsträger aus dem IT-Bereich, die in ihrem Unternehmen für die Cloud-Sicherheit verantwortlich sind. Dabei wollten wir wissen, welche Pläne sie bezüglich des Cloud-Einsatzes haben, auf welche Probleme sie stoßen und wie ihre Investitionsprioritäten für das kommende Jahr aussehen.

In diesem Bericht betrachten wir die Entwicklungen bei der Migration von Unternehmen zur Cloud und die Unterschiede zwischen Modellen wie Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Security-as-a-Service sowie öffentlicher, privater oder Hybrid-Cloud. Wir untersuchen auch, auf welche Weise Unternehmen in stärker regulierten Branchen Compliance-Probleme beim Einsatz von Cloud Computing überwinden.

Wir werden Mythos und Realität der größten Cloud-Sicherheitsprobleme aufzeigen, mit denen Unternehmen rechnen müssen. Außerdem betrachten wir die Effektivität von Investitionen in Cloud-Sicherheitstechnologien wie Verschlüsselung und Schutz vor Datenkompromittierung.

Wir untersuchen auch, wie Unternehmen die Probleme von Clouds in der Schatten-IT angehen und gleichzeitig Mitarbeitern sowie Abteilungen Zugang zu benötigten Diensten gewähren, ohne dabei den Schutz geschäftlicher Informationen zu vernachlässigen. In diesem Bericht analysieren wir auch das Bewusstsein von Unternehmensführungen für Cloud-Sicherheitsrisiken.

„Wir sind schon lange keine Early Adopter mehr – also solche, die Cloud-Bereitstellungen testen und im Piloteinsatz betreiben – sondern setzen verschiedene Cloud-Typen im großen Maßstab ein. In allen Bereichen können wir sehen, dass dies die Zukunft der IT ist und Datenverarbeitung zu einer Dienstleistung werden lässt."

– Jim Reavis, CEO, Cloud Security Alliance

„Unsere Geschäftspartner nutzen die Dynamik der Cloud, die höhere Geschwindigkeit, bessere Zusammenarbeit sowie die Flexibilität der Dienste – alles attraktive Vorteile der Cloud – und bauen ihren Einsatz noch weiter aus, da sie sonst ins Hintertreffen geraten. Als Sicherheitsexperten müssen wir Engagement zeigen und beweisen, dass Cloud und Sicherheit zusammenpassen."

– Timothy Youngblood, CISO, Kimberly-Clark

Unternehmens-IT steigert Cloud-Investitionen

Verbraucher nutzen die Cloud bereits aktiv für ihre täglichen Aufgaben, z. B. zum Hochladen von Fotos, Abrufen von E-Mails oder zur Datensicherung. Unsere Umfrage zeigt, dass wir jetzt an einem ähnlichen Wendepunkt angelangt sind, an dem sich die Unternehmens-IT in erster Linie auf Cloud Computing konzentrieren wird.

Während der zunehmende Einsatz der Cloud durch Unternehmen sowie Investitionen keine Überraschung sein dürften, lässt das rasante Tempo dieser Entwicklung aufhorchen. Unsere Umfrage zeigt, dass ein entscheidender Wandel in der Unternehmens-IT stattfindet – in weniger als eineinhalb Jahren (und in manchen Ländern noch eher) werden die IT-Budgets der Unternehmen überwiegend für Cloud-Dienste eingesetzt (siehe Abbildung 1). Die Umfrageteilnehmer erwarten, dass in 16 Monaten 80 Prozent des IT-Budgets ihres Unternehmens für Cloud-Computing-Dienstleistungen ausgegeben wird. Unternehmen in Brasilien und Australien gehen sogar davon aus, dass sie diese 80-Prozent-Marke innerhalb eines Jahres erreichen werden.

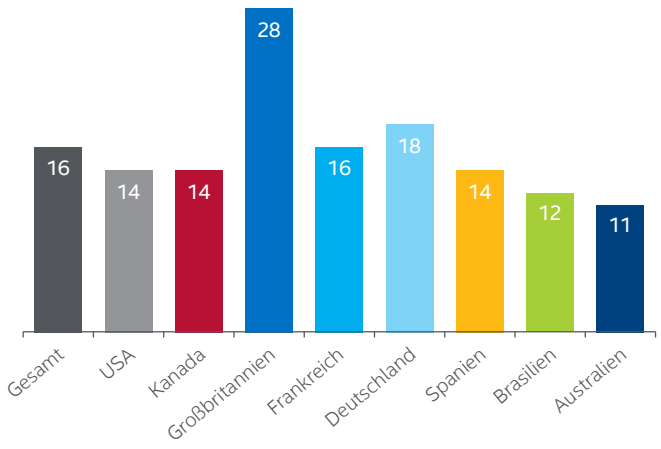

Abbildung 1. Durchschnittliche Anzahl von Monaten, bis das IT-Budget der Unternehmen der Umfrageteilnehmer zu 80 Prozent für Cloud-Computing-Services ausgegeben wird (nach Land aufgeteilt).

Die von den Umfrageteilnehmern genannte Migration zu Cloud-Diensten gilt sowohl für private und öffentliche Cloud-Bereitstellungen. Laut unserer Umfrage ist die private Cloud mit 51 Prozent das von den Unternehmen am häufigsten eingesetzte Cloud-Modell. Die öffentliche Cloud macht dagegen maximal 30 Prozent aus, während Hybrid-Cloud-Kunden auf einen Anteil von 19 Prozent kommen. Wenn wir betrachten, wie viele Monate es dauert, bis 80 Prozent des IT-Budgets eines Unternehmens für Cloud Computing ausgegeben wird, schrumpft der Zeitraum für die private Cloud auf nur noch 15 Monate.

Wir sehen den Beweis, dass der Einsatz von Cloud-Diensten am Wendepunkt angelangt ist. Unternehmen setzen heute im Durchschnitt 43 Cloud-Dienste ein, wobei einige regionale Unterschiede bestehen (Abbildung 2). Bei der Cloud-Einführung ist Großbritannien beispielsweise am langsamsten (im Mittel nur 29 Cloud-Dienste pro Unternehmen), während brasilianische Unternehmen sie am stärksten einsetzen (55 Cloud-Dienste pro Unternehmen).

„Wir bei DocuSign setzen auf das 'Cloud First'-Prinzip und haben festgestellt, dass auch viele unserer Kunden aus den verschiedensten Branchen diesen Ansatz nutzen. Bei Unternehmen aus regulierten Branchen wie Finanzdienstleistungen und Gesundheitswesen dauert dieser Schritt länger. Die IT-Abteilungen dieser Unternehmen sind hier in einer schwierigen Lage, da die Regulierungsbehörden noch vor der Implementierung Nachweise dazu fordern, dass die notwendigen Sicherheitsmaßnahmen umgesetzt werden. Auf den IT-Verantwortlichen lastet also großer Druck, da sie einerseits in aller Ruhe diesen Nachweis erbringen sollen, andererseits ihr Unternehmen jedoch mehr Effizienz und Flexibilität fordert – und natürlich mehr Geschwindigkeit."

– Vanessa Pegueros, CISO, DocuSign, Inc.

„Machen Sie sich bewusst, welche Informationen in der Cloud gespeichert werden können. Wenn Informationen wertvoll für das Unternehmen sind, sollten sie innerhalb der Unternehmensgrenzen in einer privaten Cloud bleiben."

– Eric Knapp, Global Director of Cybersecurity, Honeywell

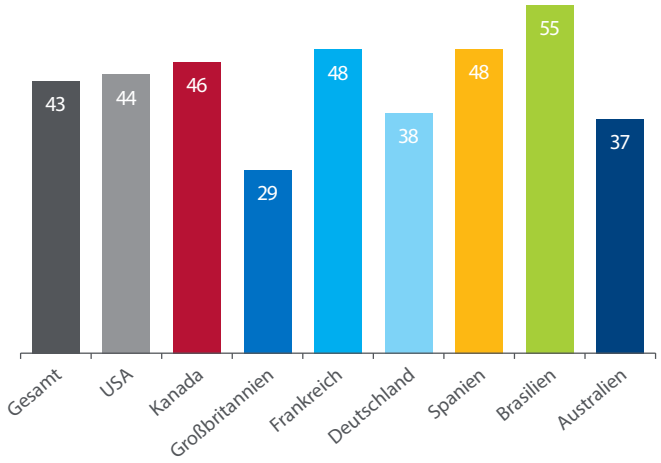

Abbildung 2. Die durchschnittliche Anzahl der von Unternehmen genutzten Cloud-Dienste (nach Land aufgeteilt).

Natürlich gibt es Unterschiede beim Einsatz der verschiedenen Cloud-Plattformen, seien es öffentliche, private und hybride oder verwaltete Clouds oder SaaS, IaaS und PaaS. Gleichzeitig ist dies auch ein Beweis dafür, dass der Umfang des Cloud-Einsatzes von der Branche abhängt. In stark regulierten Branchen (z. B. im Finanzsektor) sind die Unternehmen gegenüber Cloud noch vorsichtig, und auch Behörden sowie der öffentliche Sektor liegen auf den hinteren Plätzen.

In Anbetracht der Entwicklungen beim Cloud-Einsatz zeigt sich, dass wir SaaS nicht isoliert betrachten dürfen. Tatsächlich zeigt unsere Umfrage, dass die Mehrzahl der Unternehmen in alle Cloud-Dienstmodelle investieren möchte, wobei 81 Prozent (möglicherweise überraschend) an IaaS gehen, während SaaS mit nur 60 Prozent das Schlusslicht bildet (siehe Abbildung 3). Den zweiten Platz auf der Rangliste nimmt ganz knapp Security-as-a-Service ein (78 Prozent) ein. Und sogar die geplanten Investitionen in PaaS liegen mit 69 Prozent höher als SaaS.

Diese Zahlen werden gestützt vom SANS-Bericht, der ebenfalls zeigt, dass IaaS im nächsten Jahr der Bereich mit dem größten Wachstum bei Cloud-Bereitstellungen für Unternehmen sein wird.

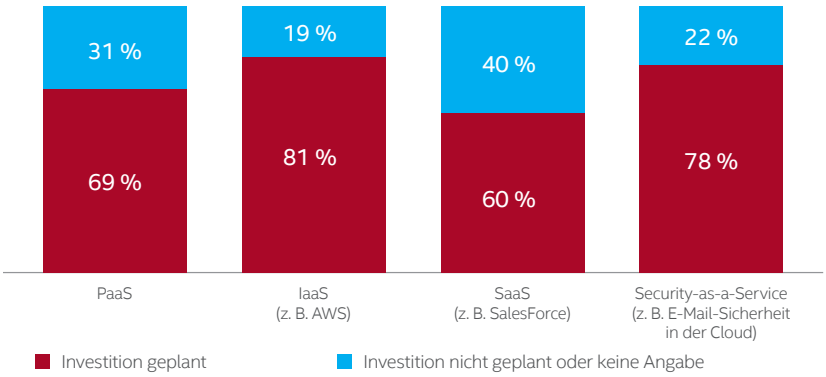

Abbildung 3. In welche Cloud-Bereitstellungen möchte Ihr Unternehmen investieren?

„Fehlender Einblick in die Arbeitsweise und Abläufe beim Cloud-Dienstanbieter erschwert die Risikoanalyse sowie die Entscheidungen zur Risikoverwaltung. Zahlreiche Vorschriften wurden noch vor dem Aufkommen der Cloud erlassen, wobei angenommen wurde, dass ein Unternehmen vollständige Kontrolle über die Datenverarbeitungstechnologie hat. Dies ist in einer Cloud nicht mehr der Fall."

– Jim Reavis, CEO, Cloud Security Alliance

„Wir kennen die Sorgen im Zusammenhang mit Datenkompromittierungen. Häufig kommt es zu einem Angriff auf die Anmeldeinformationen von Benutzern mit legitimen Zugang zum Cloud-Dienst, sodass die Informationen auf diese Weise exfiltriert werden können."

– Jim Reavis, CEO, Cloud Security Alliance

Sicherheit und Compliance: Der Bedarf nach größerer Transparenz

Welche Folgen wird dieser zunehmende Cloud-Einsatz für die Unternehmenssicherheit haben? Wir halten es für möglich, dass noch mehr wichtige und vertrauliche Daten in der Cloud gehostet werden. Etwa 40 Prozent der Teilnehmer der SANS-Umfrage **Orchestrating Security in the Cloud** (Durchsetzung von Sicherheit in der Cloud) gaben an, dass sie vertrauliche Daten in der Cloud verarbeiten oder speichern.[1] Die häufigsten Datentypen, die in der Cloud gespeichert werden, sind Business Intelligence (52 Prozent), Finanzbuchhaltung (52 Prozent), Mitarbeiterdaten (48 Prozent) und personenbezogene Kundendaten (40 Prozent). Sorgen bereiten uns jene 13 Prozent der befragten Unternehmen, die nicht wissen, ob sie die Cloud für vertrauliche Daten nutzen. Viele Sicherheitsexperten (besonders von großen Unternehmen) gehen davon aus, dass der Anteil tatsächlich viel größer ist. Das liegt zum Teil daran, dass einige Unternehmen nicht zugeben möchten, dass sie es nicht wissen, während bei anderen die Geschäftsprozesse und Unternehmenseinheiten über die ganze Welt verstreut sind, sodass sie schlicht keine Ahnung haben, ob sie gefährdet sind.

Für 72 Prozent der SANS-Umfrageteilnehmer bereitet die Einhaltung von Compliance-Vorgaben in der Cloud die größte Sorge. Das eigentliche Problem hierbei ist die Transparenz: Mehr als die Hälfte (58 Prozent) der SANS-Umfrageteilnehmer nennt fehlenden Einblick in die Abläufe des Cloud-Anbieters als größtes Problem.

Dunkle Wolken voraus? Bedrohungen für das 21. Jahrhundert

Unsere Umfrage legt nahe, dass angesichts der Lücke zwischen Wahrnehmung und Realität eine Neubewertung der realen Cloud-Bedrohungen notwendig ist.

In den meisten Ländern bereiten Datensicherheitsvorfälle die größte Sorge in Bezug auf SaaS – mehr als ein Fünftel der Teilnehmer (22 Prozent) nennen diese Befürchtung. Datenkompromittierungen zählen ebenfalls zu den größten Sorgen bei IaaS und privaten Clouds. Es gibt einige regionale Unterschiede, vor allem in Australien, wo Ausfallzeiten die größte Sorge darstellen.

Doch wie sieht die Realität wirklich aus?

Bei weiterführenden Fragen gab weniger als ein Viertel der befragten Unternehmen (23 Prozent) an, dass sie bei ihrem Cloud-Dienstanbieter tatsächlich Datenverluste oder -kompromittierungen erlebt hatten, und nur bei einem Fünftel hatte ein Angreifer nicht autorisierten Zugriff auf Daten oder Services. Die SANS-Umfrage zeigt eine noch niedrigere Anzahl von Cloud-Datenkompromittierungen: Hier gaben nur 9 Prozent der Teilnehmer an, dass sie in öffentlichen Clouds oder in ihren SaaS- bzw. Privat-Cloud-Anwendungen einen Zwischenfall erlebt hatten.

Die am häufigsten genannten Cloud-Dienst-bezogenen Vorfälle und Probleme der Umfrageteilnehmer waren die Migration von Services und Daten, hohe Kosten und schlechter Mehrwert oder fehlende Einblicke in die Abläufe des Cloud-Anbieters (Abbildung 4).

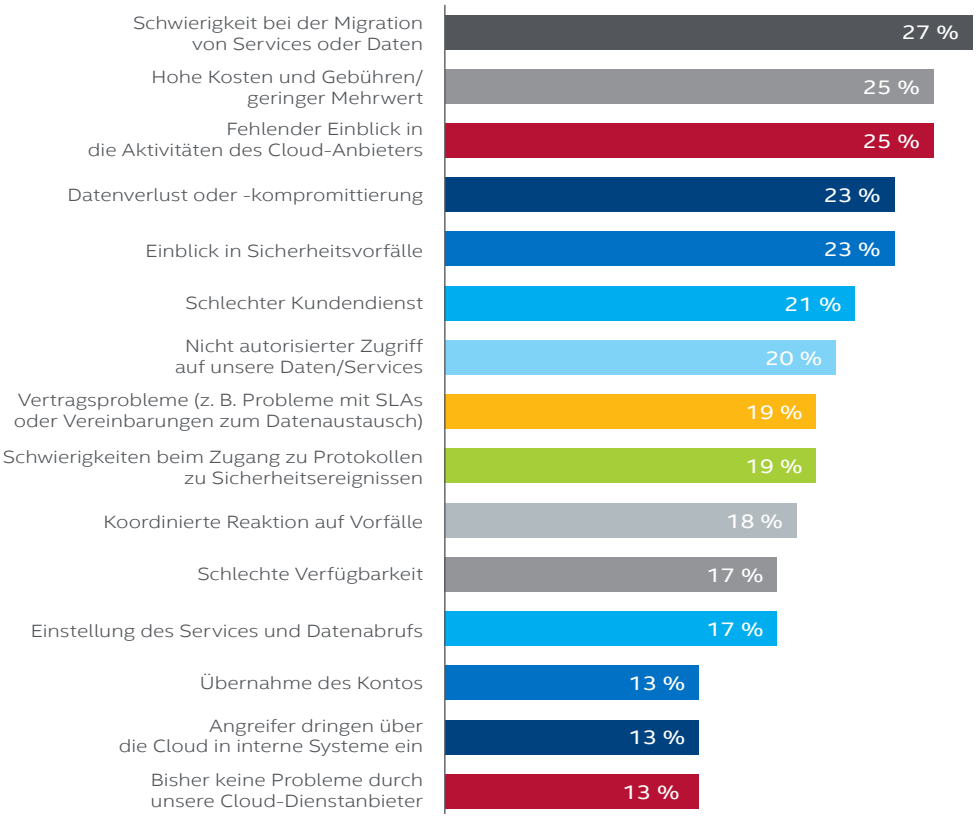

Abbildung 4. Welche Probleme hatte Ihr Unternehmen mit Cloud-Dienstanbietern in Bezug auf Cloud-Sicherheit?

Beim Blick auf die einzelnen von den Umfrageteilnehmern genannten Sicherheitsbedrohungen für die Cloud zeigt sich, dass Malware und Botnets das größte Problem für private Cloud-Bereitstellungen darstellen (33 Prozent), während Denial-of-Service-Angriffe als größte Bedrohung für öffentliche Clouds wahrgenommen werden (36 Prozent).

„Unternehmen müssen Sicherheitskonzepte und -maßnahmen in DevOps integrieren, und die zwei wichtigsten Elemente sind dabei kontinuierliche Überwachung und Änderungserkennung.“

– Dave Shackleford, SANS-Analyst und CEO, Voodoo Security

Andere Cloud-Sicherheitsrisiken entstehen potenziell durch die vertikale Skalierung oder die Konsolidierung von Diensten, obwohl dies eher eine Frage der Verfügbarkeit und des störungsfreien Geschäftsbetriebs ist, was entsprechende Planungen des Unternehmens erfordert. Eine weitere wichtige Eigenschaft des Cloud-Einsatzes ist die Zunahme von „DevOps“ – die immer schnelleren Zyklen bei Entwicklung, Test und Bereitstellung von Anwendungen. Um mit diesen rasanten Entwicklungen Schritt zu halten und bei damit zusammenhängenden potenziellen Sicherheitsrisiken gewarnt zu werden, ist die Integration zuverlässiger Sicherheitsfunktionen in die kontinuierliche Entwicklungsumgebung unabdingbar.

Wir sollten uns angesichts der Umfrageergebnisse keinesfalls der Vorstellung hingeben, dass Cloud-Datenkompromittierungen keine ernsthafte Sicherheitsbedrohung sind oder nie vorkommen. Deshalb sollten wir die Möglichkeit in Betracht ziehen, dass Datenkompromittierungen nicht erfasst werden, wenn sie Strafverfolgungsbehörden oder Regulierern nicht gemeldet werden. Und natürlich sind die Konsequenzen von Cloud-Datenkompromittierungen, wenn sie denn doch einmal vorkommen, häufig schwerwiegend. Während die Lücke zwischen der wahrgenommenen Cloud-Sicherheitsbedrohung und der Realität geschlossen werden muss, deuten die Umfrageergebnisse darauf hin, dass bei der Investition und Planung rund um die Behebung schwerwiegender Kompromittierungen auch gewöhnlichere, alltäglichere Gefahren für Unternehmenssysteme und Daten in der Cloud berücksichtigt werden müssen. Dazu gehören Migrationsprobleme, schlechter Kundendienst und Vertragsstreitigkeiten sowie konkrete Sicherheitsbedrohungen wie Denial-of-Service-Angriffe, Malware und das Hacken von Konten.

Cloud-Sicherheit und Risiken: Der blinde Fleck der Unternehmensführung

Unsere Umfrage zeigt eine starke Beteiligung hochrangiger Führungskräfte an Entscheidungen zur Cloud-Sicherheit. Dies gilt nicht nur für den Leiter IT, sondern auch für den CIO und CISO sowie häufig auch für den CEO und CFO. Aber versteht die Unternehmensführung die Sicherheitsrisiken auch vollständig?

„Ein Großteil der Vorstände und Führungskräfte erkennt mittlerweile, dass Cloud-Sicherheit ein wichtiges Element für jedes Unternehmen ist und entsprechende Aufmerksamkeit benötigt."

– Vanessa Pegueros, CISO, DocuSign, Inc.

In Bezug auf öffentliche Clouds scheint es bei der Unternehmensführung eine Besorgnis erregende Lücke bei der Wahrnehmung der Sicherheitsprobleme im Zusammenhang mit der Speicherung vertraulicher Daten in der öffentlichen Cloud zu geben (siehe Abbildung 5). Nur 34 Prozent der Teilnehmer gaben an, dass die hochrangigen Führungskräfte in ihrem Unternehmen die Probleme wirklich verstehen, während ein Fünftel der Meinung ist, dass Führungskräfte der obersten Ebene keine Ahnung haben oder die Risiken nur teilweise kennen. Die Lücke ist in Großbritannien noch größer: Hier gehen nur 15 Prozent der Befragten davon aus, dass die Führungskräfte in ihrem Unternehmen die mit der Speicherung von Daten in der öffentlichen Cloud verbundenen Risiken umfassend verstehen. Das ist ein erheblicher Unterschied zu Brasilien (49 Prozent) und Australien (47 Prozent), wo die Unternehmensführung den Problemen deutlich mehr Aufmerksamkeit widmet.

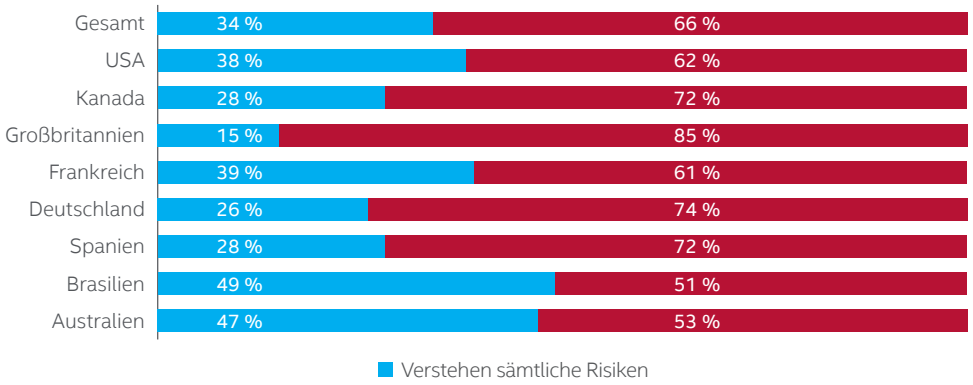

Abbildung 5. Glauben Sie, dass die Unternehmensführung/Führungskräfte in Ihrem eigenen Unternehmen die Sicherheitsprobleme im Zusammenhang mit der Speicherung vertraulicher Daten in der öffentlichen Cloud verstehen?

„Wissen ist Macht, und Schulung ist Wissen. Wir haben ein sehr intensives Programm zur Förderung des Sicherheits-bewusstseins, das darauf ausgerichtet ist, allen unseren Mitarbeitern den Wert von Informationen zu verdeutlichen. Das bezeichnen wir als unsere 'menschliche Firewall'."

– Timothy Youngblood, CISO, Kimberly-Clark

Obwohl schwerwiegende Datenkompromittierungen und finanzielle sowie rufschädigende Konsequenzen die Datensicherheit zu einem wichtigen Thema für viele CEOs und Führungskräfte gemacht haben, ist es immer noch wichtig, die Aufmerksamkeit durch Informationen zu steigern und ein Verständnis der Risiken zu vermitteln, die mit der Speicherung vertraulicher Daten in der Cloud zusammenhängen.

Schatten-IT: Bedrohung oder Chance?

Ein Großteil der Teilnehmer unserer Umfrage gab an, dass Schatten-IT die Möglichkeiten ihres Unternehmens zur Absicherung und dem Schutz von Cloud-Diensten negativ beeinflusst. Dabei waren 10 Prozent der Meinung, dass ihr Unternehmen erheblichen Risiken ausgesetzt ist.

Die Absicherung der Schatten-IT ist auch weiterhin ein großes Problem: 52 Prozent der Branchen erwarten immer noch von der IT-Abteilung, dass diese die nicht autorisierten Cloud-Dienste in ihrer Abteilung absichert. Hinzu kommt, dass beinahe ein Viertel der Umfrageteilnehmer (23 Prozent) anmerkte, dass diese Abteilungen die Absicherung selbst übernehmen, ohne die IT-Abteilung einzubeziehen.

„Schatten-IT ist die neue IT. Das alte Modell verschwindet gerade. Je mehr wir uns dagegen stellen, desto mehr Gelegenheiten verlieren wir, sie abzusichern. Wir müssen akzeptieren, dass Schatten-IT heute Realität ist, und unsere Energie auf ihre sichere Verwaltung konzentrieren.“

– Vanessa Pegueros, CISO, DocuSign, Inc.

Die Übersicht über die Schatten-IT in den einzelnen Geschäftsbereichen ist bei SaaS im Allgemeinen größer als bei IaaS. In allen Fällen weiß jedoch mindestens ein Fünftel der Befragten nicht, ob Schatten-IT in jeder Abteilung ihres Unternehmens eingesetzt wird. Am stärksten vertreten ist die Schatten-IT in den Bereichen Vertrieb, Forschung und Entwicklung sowie im Marketing. Das größte Fragezeichen besteht bei der Rechtsabteilung. Etwa 37 Prozent unserer Umfrageteilnehmer wissen nicht, ob diese Abteilung die Cloud ohne Wissen der IT-Abteilung nutzt.

Wie gehen Unternehmen mit dem Problem der Schatten-IT um? Die häufigsten Methoden sind:

- Überwachung von Datenbankaktivitäten (49 Prozent)
- Firewalls der nächsten Generation (41 Prozent)
- Web-Gateways (37 Prozent)

Eine andere Taktik ist die Zusammenarbeit mit der Finanzabteilung, um benachrichtigt zu werden, wenn Kostenabrechnungen für Cloud-Dienste eingereicht werden.

Es gibt einen spürbaren Unterschied beim Umgang mit Schatten-IT, sobald sie entdeckt wurde. Beinahe die Hälfte der Befragten (46 Prozent) blockiert den Zugang, während 37 Prozent die Schatten-IT in einen zugelassenen Dienst umwandeln.

„Die Angestellten versuchen nur, ihre Arbeit zu erledigen. Wenn wir ihnen diese Möglichkeit nicht geben können, werden sie es auf andere Weise versuchen. Deshalb müssen IT-Abteilung und CIO als Mittler auftreten und gegenüber der Cloud sowie SaaS-Services offen sein.“

– Brent Conran, Vice President und CISO, Intel

Wächst das Vertrauen in die Cloud?

Auf den ersten Blick zeigen die Kennzahlen aus unserer Umfrage ein relativ geringes Vertrauen in Cloud Computing verglichen mit lokal oder intern gehosteter IT. Wenig überraschend ist die öffentliche Cloud das Modell, dem am wenigsten vertraut wird (Abbildung 6).

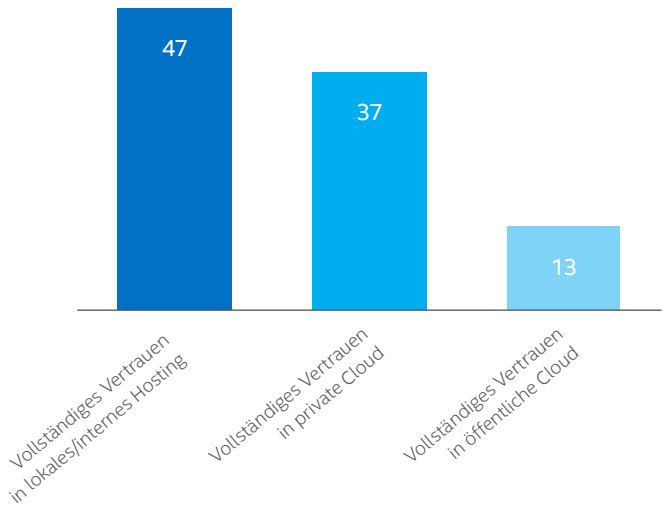

Abbildung 6. Wie sehr vertrauen Sie darauf, dass die folgenden Modelle die Sicherheit der vertraulichen Daten Ihres Unternehmens gewährleisten können?

Insgesamt zeigt sich, dass das Vertrauen in Cloud Computing im letzten Jahr gewachsen ist – 77 Prozent der Befragten gaben an, dass ihr Unternehmen mittlerweile mehr vertraut als noch vor einem Jahr (Abbildung 7).

„Für Cloud-Anbieter bricht gerade ein neues Zeitalter an. Derzeit befinden wir uns in einer Übergangsphase, doch ich gehe davon aus, dass mit diesen neuen Vorschriften Investitionen und Vertrauen in Cloud-Dienste gestärkt werden."

– Dimitra Liveri, Networks and Information Security Officer, European Network and Information Security Agency (ENISA)

„Der erste Schritt bei Unternehmenssicherheit in der öffentlichen Cloud ist die Frage: Wo ist die Grenze des Verantwortungsbereichs? Was können Sie als Unternehmen vollständig kontrollieren, und welche Verwaltungsaufgaben fallen in den Verantwortungsbereich des Cloud-Anbieters? Und Sie müssen die Kontrollen für das vollständige Sicherheitsspektrum bewerten, einschließlich Datensicherheit, Identitätsverwaltung und Richtlinienanwendung. Es gibt Dinge, die Sie nicht mehr kontrollieren können, insbesondere auf Netzwerkebene."

– Dave Shackleford, SANS-Analyst und CEO, Voodoo Security

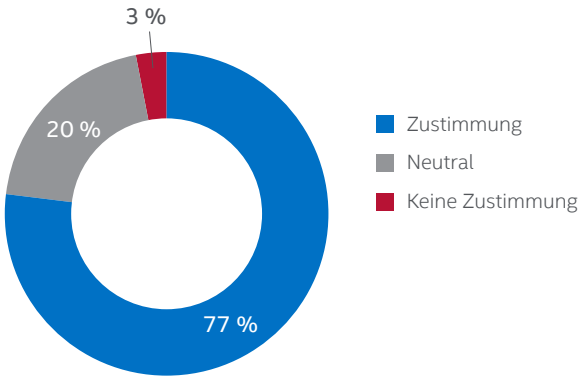

Abbildung 7. Anteil der Befragten, die der Aussage „Mein Unternehmen vertraut Cloud Computing jetzt mehr als noch vor 12 Monaten" zustimmen.

Nachdem zwei wichtige Vorschrifteninitiativen die Zustimmung der EU-Kommission erwarten, verspricht 2016 ein gutes Jahr für europäische Cloud-Anbieter und Benutzer zu werden. Bei diesen Vorschriften handelt es sich um die EU-Datenschutz-Grundverordnung und die Richtlinie über Dienste der Netz- und Informationssicherheit (NIS-Richtlinie). Wird damit das Vertrauen in die Cloud-Sicherheit wachsen? Die Fachleute gehen davon aus.

Prioritäten bei Cloud-Sicherheitsinvestitionen

Die Prioritäten bei Sicherheitsinvestitionen unterscheiden sich für die verschiedenen Cloud-Bereitstellungen. Unternehmen nutzen im Durchschnitt drei Sicherheitslösungen, um ihre SaaS-Anwendungen zu schützen. Am häufigsten ist dabei Dateiverschlüsselung (60 Prozent), gefolgt von E-Mail-Sicherheit (55 Prozent).

Bei IaaS nutzen Unternehmen durchschnittlich vier Sicherheitslösungen. Am häufigsten finden sich Firewalls (70 Prozent) und Verschlüsselung (62 Prozent). Die private Cloud nutzt ebenfalls im Durchschnitt vier Sicherheitslösungen, wobei Firewalls am häufigsten eingesetzt werden (67 Prozent).

Die vier Bereiche von Security-as-a-Service, in die Unternehmen investieren wollen, sind die gleichen, in die sie bereits investieren: E-Mail-, Web- und Malware-Schutz sowie Anwendungs-Firewall (Abbildung 8). Diese Entwicklung zeigt, dass Unternehmen die bereits vorhandenen Cloud-basierten Sicherheits-Services verbessern und ausbauen möchten.

Die SANS-Umfrage zeigt auch einige wichtige Bereiche für Cloud-Sicherheitsinvestitionen für die nächsten 18 Monate auf. Dazu gehören Schwachstellen-Scans, mehrstufige Authentifizierung, Schutz vor Datenkompromittierung, Protokollverwaltung, Eindringungserkennungssysteme (IDS) und Eindringungsschutzsysteme (IPS), Sicherheitsinformations- und Ereignis-Management (SIEM) sowie Cloud Access Security Broker (CASB).

Laut dem Gartner-Bericht *Market Guide for Cloud Access Security Brokers* (Marktleitfaden für Cloud Access Security Broker) sind vor allem CASBs ein Bereich mit starkem Wachstum. Gartner sagt voraus, dass „bis zum Jahr 2020 insgesamt 85 Prozent aller großen Unternehmen ein Cloud Access Security Broker-Produkt für ihre Cloud-Dienste nutzen werden – ein Anstieg von aktuell weniger als 5 Prozent".[2] Unsere Umfrage bestätigt das. Obwohl CASBs relativ neu sind, nutzen 36 Prozent aller Unternehmen solche Dienste, um ihre SaaS-Anwendungen zu schützen, und 32 Prozent überwachen damit Cloud-Implementierungen in der Schatten-IT. Beinahe ein Viertel aller Unternehmen (24 Prozent) möchte in Zukunft in einen CASB-as-a-Service investieren.

„Ein Überblick über die Vorgänge in Ihrer Cloud-Umgebung (z. B. zwischen der Benutzerbasis und SalesForce) ist wirklich wichtig, und ich werde den Tools, mit denen das sicher möglich ist, größere Aufmerksamkeit schenken. Wir benötigen außerdem Tools, mit denen wir Prozesse wie die Reaktion auf Zwischenfälle automatisieren und vorhandene Investitionen besser nutzen können.“

– Vanessa Pegueros, CISO, DocuSign, Inc.

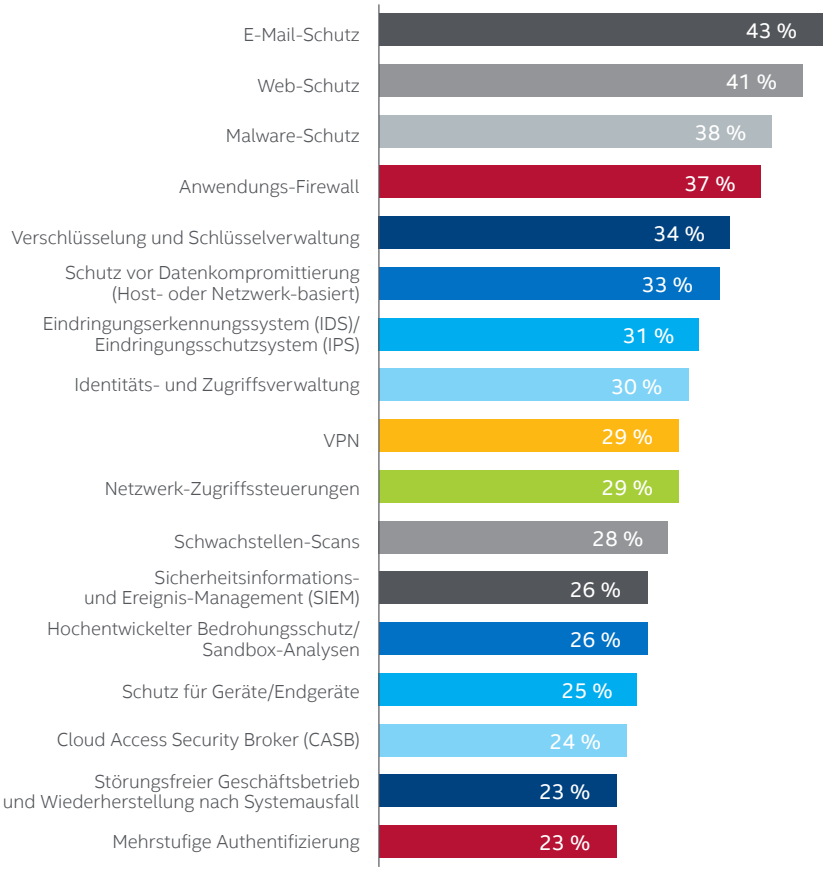

Abbildung 8. In welche Bereiche von Security-as-a-Service möchte Ihr Unternehmen investieren?

Von den Unternehmen, die einen öffentlichen Cloud-Dienst nutzen, gab etwas mehr als ein Drittel (34 Prozent) an, dass sie eine zentrale Lösung mit vollständiger Integration und zentraler Verwaltung für ihre Hybrid-Cloud und die lokalen Systeme einsetzen. Es gibt hier also noch viele Verbesserungsmöglichkeiten.

Zusammenfassung

Der Einsatz der Cloud im Unternehmen nähert sich mit raschen Schritten einem Wendepunkt – die Unternehmen gaben an, dass sie innerhalb der nächsten 16 Monaten oder noch früher 80 Prozent ihres IT-Budgets für die Cloud ausgeben werden.

Es gibt viele überzeugende Anreize, die Unternehmen zu einem Wechsel in die Cloud motivieren, beispielsweise größere Flexibilität, schnellere Innovation sowie Kosteneffizienz. Eine solche Bandbreite von Cloud-Bereitstellungsmöglichkeiten bringt natürlich auch Sicherheitsprobleme mit sich. Da die Cloud als Repository für so viele wichtige Unternehmensdaten dient oder dienen wird, sollten Unternehmen Folgendes berücksichtigen:

- Für Sicherheitskontrollen und Compliance sind Unternehmen und Cloud-Dienstanbieter gemeinsam verantwortlich. Fragen Sie Ihren Dienstanbieter nach seinen Sicherheitskontrollen, und überprüfen Sie, ob Ihr Service Level Agreement (SLA) auch regelmäßige Berichte umfasst. Das Unternehmen muss jedoch alles absichern, was in der Cloud in seinen Verantwortungsbereich fällt (z. B. Daten, Anwendungen oder Arbeitsabläufe) und seine Cloud-Architektur entsprechend aufbauen.

„Auch wenn Sie Ihre Datenverarbeitung ausgelagert haben und die Cloud nutzen, haben Sie Ihre Verantwortung nicht ausgelagert. Sie können nicht einfach sagen: 'Hey, daran ist Amazon Schuld'.“

– Brent Conran, Vice President und CISO, Intel

- Wichtige Bereiche für Sicherheitsinvestitionen sind Datenverschlüsselung, Identitäts- und Zugangsverwaltung, Schutz vor Datenkompromittierung sowie E-Mail-Schutz. Zunehmend investieren Unternehmen auch in Security-as-a-Service sowie in andere Dienste, mit denen sie die Sicherheit über mehrere Anbieter und Umgebungen hinweg koordinieren können. Dazu zählen insbesondere CASBs.
- Da zur Schatten-IT zählende Cloud-Bereitstellungen aufgrund der Gefahr für Unternehmensdaten auch weiterhin ein Problem darstellen, sollten IT-Abteilungen mit den einzelnen Geschäftsabteilungen zusammenarbeiten, um sicherere Möglichkeiten zur Implementierung eigener Cloud-Bereitstellungen aufzuzeigen. Die IT-Abteilung kann Kontrolle und Überblick zurückerlangen, indem sie als Mittler agiert und den Geschäftsabteilungen sicherere alternative Cloud-Dienste zuweist.
- Obwohl viele Unternehmensführungen stärker an Entscheidungen zur Cloud-Sicherheit beteiligt sind, gibt es eine gefährliche Lücke zwischen ihrem Verständnis und den realen Risiken. Dies zeigt nicht nur, wie wichtig Schulungen sind, sondern auch, dass CIOs und CISOs mehr das Gespräch mit anderen Führungskräften suchen müssen. Die finanziellen Auswirkungen und die Rufschädigung, die Unternehmen im Zuge einiger kürzlich erfolgter schwerwiegender Datenkompromittierungen verkraften mussten, sollten für die Führungskräfte ein großer Anreiz sein, der Datensicherheit – intern oder in der Cloud – größte Priorität einzuräumen.

Methodik

Die Umfrage unter 1.200 IT-Entscheidungsträgern mit Verantwortung für die Cloud-Sicherheit in ihren Unternehmen wurde im Juni 2015 von Vanson Bourne durchgeführt. Die Teilnehmer stammten aus Australien, Brasilien, Deutschland, Frankreich, Großbritannien, Kanada, Spanien sowie den USA und waren bei Unternehmen verschiedenster Größe angestellt, von mittleren Unternehmen mit 251 bis 500 Mitarbeitern bis zu Großunternehmen mit mehr als 5.000 Angestellten.

Über Intel Security

McAfee ist jetzt ein Geschäftsbereich von Intel Security. Durch die Security Connected-Strategie, einen innovativen Ansatz für Hardware-unterstützte Sicherheitslösungen sowie das Global Threat Intelligence-Netzwerk ist Intel Security voll und ganz darauf konzentriert, für die Sicherheit seiner Kunden zu sorgen. Dazu liefert Intel Security präventive, bewährte Lösungen und Dienste, mit denen Systeme, Netzwerke und Mobilgeräte von Privatanwendern und Unternehmen weltweit geschützt werden können. Intel Security verknüpft die Erfahrung und Fachkompetenz von McAfee mit der Innovation und bewährten Leistung von Intel, damit Sicherheit als essentieller Bestandteil jeder Architektur und Computerplattform eingebettet wird. Intel Security hat sich zum Ziel gesetzt, allen – Privatpersonen ebenso wie Unternehmen – die Möglichkeit zu geben, die digitale Welt sicher nutzen zu können. **www.intelsecurity.com**

1. *SANS Institute: Orchestrating Security in the Cloud* (Durchsetzung von Sicherheit in der Cloud), Dave Shackleford, September 2015 (unterstützt von Intel Security).
2. Gartner-Bericht: *Market Guide for Cloud Access Security Brokers* (Marktleitfaden für Cloud Access Security Broker), Craig Lawson, Neil MacDonald und Brian Lowans, 22. Oktober 2015.

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

62260rpt_cloud_0316