Wachsendes Vertrauen in die Cloud

Weltweite Ansichten von Unternehmen aus dem Gesundheitswesen

Cloud-Dienste werden im Gesundheitswesen mit 96 % etwas häufiger genutzt als im weltweiten Branchendurchschnitt (93 %). Gründe dafür können Möglichkeiten zur Kostensenkung sowie die schnelle Digitalisierung medizinischer Informationen sein. Ebenso wie Unternehmen in anderen Branchen setzen 81 % der Gesundheitsunternehmen 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 im Gesundheitswesen ein allmählicher Wechsel von privaten Cloud-Rechenzentruminfrastrukturen zu einem hybriden Modell mit öffentlichen und privaten Cloud-Komponenten statt. Befragte Unternehmen gehen davon aus, dass 80 % ihres IT-Budgets innerhalb von 15 Monaten (Durchschnittswert) für Cloud-basierte Lösungen ausgegeben werden.

Diese Analyse der Implementierung von Cloud-Diensten im Gesundheitswesen sowie die damit zusammenhängenden Sorgen und Zukunftspläne wurden der **Intel Security-Cloud-Umfrage für 2016** entnommen. Bei den Umfrageteilnehmern handelte es sich um hochrangige Entscheidungsträger im IT-Sicherheitsbereich aus Ländern wie Australien, Brasilien, Deutschland, Frankreich, den Golfanrainerstaaten (Saudi-Arabien und Vereinigte Arabische Emirate), Großbritannien, Japan, Kanada, Mexiko, Singapur und den USA.

Die wichtigsten Erkenntnisse zu Gesundheitsunternehmen

Laut unserer Umfrage nehmen Unternehmen im Gesundheitswesen unter den Branchen, in denen am häufigsten Cloud-Dienste genutzt werden, mit 96 % Platz 3 ein. Diese Liste wird von Finanzdienstleistern und Technologiefirmen (mit jeweils 99 %) angeführt. Die durchschnittliche Anzahl von Cloud-Diensten bei Gesundheitsunternehmen sank von 41 (2015) auf 33 (2016). Dieser Rückgang fällt dabei geringer aus als beim gesamten Branchendurchschnitt (43 auf 29 Dienste). In jeden Fall ist dies ein Hinweis auf die potenzielle Konsolidierung der Cloud-Anbieter oder -Dienste.

Cloud-Architekturen haben sich erheblich gewandelt – von hauptsächlich privaten Clouds im Jahr 2015 zu vorrangig öffentlich-privaten Hybrid-Architekturen, bei denen Unternehmen im Gesundheitswesen jedoch den geringsten Anteil haben. Überraschend ist, dass Gesundheitsunternehmen mit 24 % zu den stärksten Nutzern rein öffentlicher Cloud-Dienste (SaaS, IaaS oder PaaS) gehören (weltweiter Durchschnitt: 19 %). Leitende IT-Verantwortliche in der Gesundheitsbranche meldeten, dass sie beinahe zweimal häufiger SaaS- als IaaS- oder PaaS-Angebote nutzen. Der Hauptschwerpunkt wird im kommenden Jahr bei SaaS liegen: 67 % der Unternehmen wollen ihre Investitionen in diese Dienste steigern.

96 %

der Gesundheitsunternehmen nutzen die Cloud, zudem gehören sie zu den **Top 3-Branchen** unter den Cloud-Nutzern.

24 %

der Unternehmen im Gesundheitswesen verwenden **rein öffentliche** Cloud-Dienste (SaaS, IaaS oder PaaS).

intel Security

Kurzfassung

46 %

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

60 % 

der Gesundheitsunternehmen speichern **Kundendaten (Patienteninformationen)** in öffentlichen Clouds.

52 % 

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

38 %

der Cloud-Dienste im Gesundheitswesen werden **ohne Einbeziehung der IT-Abteilung implementiert**, und die IT überblickt nur die Hälfte dieser Dienste.

Fast die Hälfte (46 %) der befragten Experten aus dem Gesundheitswesen gab an, dass sich die Implementierung von Cloud-Diensten aufgrund des Fachkräftemangels im Cyber-Sicherheitsbereich verlangsamt hätte. Dieses Problem wurde insbesondere im Zusammenhang mit IaaS-Sorgen genannt. Umfrageteilnehmer aus dem Gesundheitswesen nannten Kompetenzen, die von IT-Sicherheitsverantwortlichen gefordert werden, als größte Sorge bei IaaS. Hier kamen einheitliche und integrierte Sicherheitskontrollen, die weltweit größte Sorge im Zusammenhang mit IaaS, erst an zweiter Stelle.

Auch wenn fehlende Sicherheitskompetenzen die Implementierung verlangsamen, steigen das Vertrauen und die Aufmerksamkeit für öffentliche Cloud-Dienste im Gesundheitswesen von Jahr zu Jahr. Die meisten dieser Unternehmen halten öffentliche Cloud-Dienste für sicherer als private Clouds und trauen ihnen eher zu, die Gesamtbetriebskosten zu senken sowie die allgemeine Datentransparenz zu verbessern. Das Verhältnis von Führungskräften, die öffentlichen Clouds vertrauen bzw. ihnen misstrauen, liegt mittlerweile bei mehr als 2:1. Die größere Vertrauenswürdigkeit und das höhere Ansehen öffentlicher Cloud-Dienste sowie das bessere Verständnis der Risiken bei hochrangigen Führungskräften ermutigt mehr Unternehmen im Gesundheitswesen, vertrauliche Daten in der öffentlichen Cloud zu speichern. Der Grund dafür kann die überdurchschnittliche Sorge über nicht autorisierten Zugriff auf vertrauliche Daten in einer privaten Cloud sein (37 % gegenüber dem weltweiten Durchschnitt von 30 %). Möglicherweise aufgrund von elektronischen Krankenakten und der Vernetzung im Gesundheitswesen gehören diese Unternehmen zu den Branchen, die sehr wahrscheinlich Daten (teilweise oder vollständig) in öffentlichen Clouds speichern. Dies gilt insbesondere für Kundendaten (Patienteninformationen) mit 60 % sowie Mitarbeiterdaten mit 54 %.

Cloud-Anwendungen werden jedoch auch weiterhin für Cyber-Attacken missbraucht, und mehr als die Hälfte (52 %) der Umfrageteilnehmer im Gesundheitswesen gab an, dass sie definitiv eine Malware-Infektion zu einer SaaS-Anwendung zurückverfolgen konnten. Sie gehören auch zu den Unternehmen, die am häufigsten von Datenlecks (25 % gegenüber weltweit durchschnittlichen 22 %) oder Malware-bezogenen Zwischenfällen (13 % gegenüber 10 %) aufseiten der Cloud-Dienstanbieter betroffen sind.

Ebenso wie bei den meisten Branchen stellt Schatten-IT die IT-Abteilungen vor Herausforderungen. Nicht alle SaaS-Nutzungen bei den Gesundheitsunternehmen werden von der IT genehmigt. Experten im Gesundheitswesen berichten, dass ohne die Einbeziehung der IT implementierte Cloud-Dienste 38 % der Dienstnutzung ausmachen. Zudem haben sie nur zur Hälfte Einblick in diese Anwendungen. Die Reaktion auf gefundene nicht autorisierte Schatten-IT-Anwendungen besteht meist darin, den Zugriff darauf komplett zu blockieren. Insgesamt bereitet die Schatten-IT den IT-Verantwortlichen im Gesundheitswesen recht große Sorgen: 63 % sind der Meinung, dass dieses Phänomen es ihnen erschwert, die Sicherheit der Cloud zu gewährleisten.

Obgleich Gesundheitsunternehmen SaaS positiv gegenüberstehen und häufiger als im Durchschnitt rein öffentliche Cloud-Dienste einsetzen, verwenden 26 % weiterhin ausschließlich private Dienste und 50 % eine Mischung aus öffentlichen sowie privaten Diensten. Bei den privaten Diensten liegt der Anteil virtueller Rechenzentrum-Server nur leicht über dem Durchschnitt (51 % gegenüber 52 %). Zudem gehören die Experten im Gesundheitswesen zu denjenigen, die besonders gern Container nutzen. Die Mehrzahl der Befragten (76 %) erwartet den Wechsel zu einem vollständig Software-definierten Rechenzentrum innerhalb von zwei Jahren.

Schlussfolgerungen und Empfehlungen

Scheinbar nutzen und vertrauen Unternehmen im Gesundheitswesen den SaaS-Anwendungen mehr als andere Branchen. Bei der Verwendung privater Clouds liegen diese Unternehmen im Mittelfeld, während sie bei hybriden Clouds die hinteren Plätze einnehmen. Ob durch die häufige Nutzung der öffentlichen Cloud, den hohen Wert ihrer Daten oder eine Kombination beider Faktoren: Sie verzeichnen mehr Cyber-Angriffe, Malware-Zwischenfälle und Datenlecks als Unternehmen anderer Branchen.

Kurzfassung

Clouds werden auf Dauer bleiben, und die Sicherheitsverantwortlichen im Gesundheitswesen müssen der Entwicklung voraus bleiben, um ihr Unternehmen schützen zu können. Dank der Vielzahl verfügbarer Cloud-Angebote können Unternehmen die am besten passende Lösung finden, die gleichzeitig die gewünschten Kosteneinsparungen bietet und die Sicherheitsanforderungen erfüllt. 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.

Gesundheitsunternehmen verfügen über wertvolle Gesundheitsdaten und mussten im vergangenen Jahr Ransomware-Angriffe hinnehmen. Informationen hierzu finden Sie im **McAfee Labs Threats-Report vom Dezember 2016**. Gleichzeitig führen Unternehmen in dieser Branche aktiv neue Technologien ein, mit denen sich die Qualität und Effektivität der Patientenversorgung verbessern lässt. Angreifer suchen weiterhin stets nach dem leichtesten Opfer, ganz gleich, wo sich dieses befindet. Integrierte oder einheitliche Sicherheitslösungen bieten starken 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.

Laut den **Bedrohungsprognosen von McAfee Labs für 2017** werden für Angriffe besonders häufig Anmeldeinformationen (insbesondere von Administratoren) verwendet. Daher müssen Sie gewährleisten, dass alle Endgeräte (einschließlich Tablets und Smartphones) angemessen geschützt werden. Empfohlene Vorgehensweisen für die Authentifizierung (z. B. individuelle Kennwörter, mehrstufige Authentifizierung sowie – sofern verfügbar – Biometriedaten) sind grundlegende Strategien, mit denen das Risiko für Infektionen oder Kompromittierungen erheblich reduziert werden kann.

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.

Weitere Informationen zu diesem Thema finden Sie im vollständigen Bericht **Wachsendes Vertrauen in die Cloud**.

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