Wachsendes Vertrauen in die Cloud

Weltweite Ansichten von Finanzdienstleistern

Laut unserer Umfrage setzen Finanzdienstleister häufiger als alle anderen Branchen auf Cloud-Dienste. In 99 % der Unternehmen werden Cloud-Funktionen genutzt, während der Durchschnitt aller Branchen bei 93 % liegt. Die Finanzbranche gehört zu den Branchen, die besonders häufig auf das „Cloud First"-Prinzip setzen, d. h. interne Dienste nur dann implementieren, wenn keine entsprechende Cloud-Variante verfügbar ist. Dieser Ansatz wird von 87 % verfolgt (weltweiter Durchschnitt: 82 %). Zudem stellten wir fest, dass bei den IT-Architekturen für Finanzdienstleister ein rapider Wandel von privaten Cloud-Rechenzentruminfrastrukturen hin zum hybriden Modell mit öffentlichen und privaten Cloud-Komponenten stattfindet: Die Umfrageteilnehmer gehen davon aus, dass 80 % ihres IT-Budgets innerhalb von 14 Monaten (Durchschnittswert) für Cloud-basierte Lösungen ausgegeben werden.

99 %

der Finanzdienstleister **setzen eine beliebige Form von Cloud-Diensten ein**.

57 %

der Finanzdienstleister verwenden **Hybrid-Lösungen mit öffentlichen und privaten Komponenten**.

48 %

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

Diese Analyse der Implementierung von Cloud-Diensten bei Finanzdienstleistern 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 Finanzdienstleistern

Finanzdienstleister liegen bei der Implementierung von Cloud-Diensten an erster Stelle (99 % der befragten Unternehmen) – gemeinsam mit Technologie-Unternehmen, die ebenso häufig auf beliebige Cloud-Dienste setzen. Die Cloud-Architekturen dieser Unternehmen haben sich im vergangenen Jahr stark geändert. Der Anteil der Unternehmen mit rein privaten Cloud-Diensten fiel von 50 % (2015) auf 26 % (2016), da viele Firmen zu hybriden Lösungen mit privaten und öffentlichen Cloud-Diensten wechselten, die jetzt von 57 % der Finanzdienstleister genutzt werden.

Fast die Hälfte (48 %) der befragten Experten im Finanzbereich gab an, dass sich die Implementierung von Cloud-Diensten aufgrund des Fachkräftemangels im Cyber-Sicherheitsbereich verlangsamt hätte. Auch wenn fehlende Sicherheitskompetenzen und Sorgen die Implementierung verlangsamen, steigen das Vertrauen und die Aufmerksamkeit für öffentliche Cloud-Dienste von Jahr zu Jahr. Die meisten Finanzdienstleister halten öffentliche Cloud-Dienste für sicherer als private Clouds und trauen ihnen

Kurzfassung

54 %

der Befragten aus dem Finanzwesen konnten eine **Malware-Infektion zu einer SaaS-Anwendung zurückverfolgen**.

64 %

der Finanzdienstleister **speichern einige oder alle vertraulichen Kundendaten** in öffentlichen Clouds.

39 %

der Cloud-Dienste werden **ohne Einbeziehung der IT-Abteilung implementiert**, und **die IT überblickt nur 45 % dieser Dienste**.

eher zu, die Gesamtbetriebskosten zu senken sowie die Datentransparenz zu verbessern. Der einzige Vorteil der privaten vor der öffentlichen Cloud liegt nach Meinung der befragten Experten im Finanzbereich im wahrscheinlich besseren Schutz vor Hackern.

Cloud-Anwendungen werden auch weiterhin für Cyber-Attacken missbraucht, und mehr als die Hälfte (54 %) der Umfrageteilnehmer gab an, dass sie definitiv eine Malware-Infektion zu einer SaaS-Anwendung zurückverfolgen konnten. Gleichzeitig gehört die Finanzdienstleistungsbranche zu den Branchen mit dem geringsten Anteil an Unternehmen, die bereits ein Datenleck oder eine Kompromittierung verzeichnet haben (19 %; weltweiter Durchschnitt: 22 %).

Das Verhältnis von Finanzdienstleistern, 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, vertrauliche Daten in der öffentlichen Cloud zu speichern. Möglicherweise aufgrund der Tatsache, dass so viele Finanztransaktionen und andere Dienste online abgewickelt werden, gehören Finanzdienstleister zu den Unternehmen, die am häufigsten einige oder alle vertraulichen Kundendaten in der öffentlichen Cloud speichern (64 %).

Leitende IT-Verantwortliche im Finanzbereich berichten, dass sie am häufigsten SaaS (64 %) einsetzen, dicht gefolgt von IaaS (57 %) und PaaS mit großem Abstand (38 %). Die Investitionspläne für das kommende Jahr neigen jedoch mehr in Richtung IaaS: 69 % möchten ihre Aktivitäten in diesem Bereich verstärken, zunehmende Investitionen in SaaS sind bei 60 % und in PaaS bei 52 % geplant.

Als größte Sorge in Bezug auf SaaS nannten Finanzdienstleister ebenso wie andere Unternehmen den Schutz vertraulicher Daten bei der Übertragung in die Cloud und aus der Cloud heraus. Bei IaaS-Angeboten bereiten vor allem die Aufrechterhaltung der Compliance sowie die Möglichkeit eines nicht autorisierten Zugriffs in einer öffentlichen Mehrmandanten-Cloud Sorgen, während in anderen Branchen konsistente Sicherheitskontrollen genannt wurden. Die durchschnittliche Anzahl an Cloud-Diensten, die bei Finanzdienstleistern verwendet werden, fiel von 40 im Jahr 2015 auf 29 im Jahr 2016 – ein Indiz dafür, dass eine Konsolidierung der Cloud-Anbieter stattfindet.

Ebenso wie bei den meisten Branchen stellt Schatten-IT die IT-Abteilungen vor Herausforderungen. Experten im Finanzbereich berichten, dass ohne die Einbeziehung der IT implementierte Cloud-Dienste 39 % der Dienstnutzung ausmachen. Zudem haben sie nicht einmal zur Hälfte (45 %) Einblick in diese Anwendungen. Die meisten Finanzdienstleister verlassen sich bei der Überwachung von Cloud-Nutzung, die nicht von der IT bestätigt wurde, vor allem auf Firewalls der nächsten Generation (59 %). Die Reaktion auf gefundene nicht autorisierte Schatten-IT-Anwendungen besteht meist darin, den Zugriff darauf komplett zu blockieren (28 %) oder den Zugriff per Identitäts- und Zugriffsverwaltung zu begrenzen (27 %). In Anbetracht der überdurchschnittlichen Sorgen über den Schutz des Datenverkehrs in und aus der Cloud ist es überraschend, dass die Nutzung von DLP- und Verschlüsselungs-Tools leicht unter dem Durchschnitt liegt. Insgesamt bereitet IT-Verantwortlichen im Finanzbereich die Schatten-IT größere Sorgen als den meisten anderen Branchen: 72 % sind der Meinung, dass dieses Phänomen sie dabei behindert, die Sicherheit der Cloud zu gewährleisten.

Obgleich Finanzdienstleister der öffentlichen Cloud positiv gegenüberstehen, verwenden weiterhin 26 % rein private Cloud-Dienste, während 57 % auf eine Mischung aus öffentlicher und privater Cloud setzen. Bei den privaten Diensten liegt der Anteil virtueller Rechenzentrum-Server über dem weltweiten Durchschnitt (55 % gegenüber 52 %), während das Niveau der Container-Implementierung dem weltweiten Durchschnitt von 80 % entspricht. Die Mehrzahl der Befragten (73 %) erwartet den Wechsel zu einem vollständig Software-definierten Rechenzentrum innerhalb von zwei Jahren.

Schlussfolgerungen und Empfehlungen

Offensichtlich gehören Finanzdienstleister zu den stärksten Nutzern von Cloud-Diensten und ausgereiften Sicherheitslösungen. Sie setzen nicht nur häufiger Cloud-Dienste ein, sondern berichten auch seltener über Kompromittierungen als Unternehmen anderer Branchen.

Clouds werden auf Dauer bleiben, und die Sicherheitsverantwortlichen im Finanzbereich sind den anderen Branchen bei der Cloud-Implementierung einen Schritt voraus. Dank der Vielzahl der verfügbaren 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.

Finanzdienstleister verfügen über wertvolle Datensätze zu Finanztransaktionen und befinden sich schon lange im Visier von Cyber-Kriminellen. Angreifer suchen stets nach dem leichtesten Opfer, ganz gleich, ob sich dieses in öffentlichen, privaten oder hybriden Clouds 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. Sollten Sie noch nicht auf die „Cloud First“-Strategie setzen, sollten Sie diese implementieren, um den Wechsel zu 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