Eigenständige Sicherheitskonzepte für mobiles Arbeiten

Sicherheit in der Cloud

Die Zukunft der Arbeit ist mobil. Mit der künftigen Mobilität der Mitarbeiter müssen auch die Unternehmensanwendungen mithalten – Cloud Computing dient dabei als wichtigste Schlüsseltechnologie. Besonders geeignet sind Lösungen, die als Public Platform as a Service (PaaS) und Mobile Software as a Service (SaaS) angeboten werden und auf hybriden Cloud-Infrastrukturen lauffähig sind. Für den mobilen Arbeitsplatz müssen diese jedoch sorgfältig abgesichert werden.

AUTOR: DANIEL LIEBHART

Bereits heute bieten mehr als ein Viertel aller Unternehmen ihren Mitarbeitenden mobile Arbeitsplätze an. Laut der Studie „Workplace of the Future“ der Firma Citrix möchten 89 Prozent der befragten Unternehmen diese Art des Arbeitens bis ins Jahr 2020 zulassen. Die Vorteile liegen auf der Hand: Mobil Arbeitende sind produktiver, flexibler und erzeugen weniger Kosten. Die Zahlen der regelmäßig veröffentlichten Mobile Workforce Reports der Firma iPass, die sich unter anderem auf Statistiken des U.S. Bureau of Labor Statistics beziehen, belegen diese Vorteile auf eindrückliche Art und Weise. Der mobile Arbeitsplatz setzt eine technische Infrastruktur voraus, die einen sicheren Betrieb von Businessanwendungen auch über die Unternehmensgrenzen hinaus erlaubt – im Idealfall rund um die Uhr. Betriebliche Informationssysteme müssen zudem so ausgebaut werden, dass sie von überall einfachen, schnellen und sicheren Zugriff auf Unternehmensdaten zulassen. Das bedeutet im Klartext: Die Zeit der ausschließlich intern betriebenen Insellösungen ist spätestens mit Einführung des mobilen Arbeitsplatzes endgültig vorbei.

CLOUD COMPUTING ALS MOBILES BACKEND

Sollen bestehende IT-Systeme mobile Arbeitsplätze unterstützen, ist eine neue Flexibilität gefragt. Die dazu notwendige IT-Infrastruktur wird vom Chief Analyst Frank Gens der IDC unter dem Begriff „Dritte Plattform“ zusammengefasst. Im Gegensatz zur klassischen Mainframe-Technologie (1. Plattform) und Desktopunterstützung (2. Plattform) bildet sie das Fundament für mobile Anwendungen, die auf einer Kombination von Cloud-Computing-Services, sozialen Netzwerkmechanismen, mobilen Netzwerken und zentralen unternehmenseigenen IT-Infrastrukturen basieren. Analysten von Forrester teilen diese Ansicht: Sie nennen diese Entwicklung „Cloud & Mobile become one“ und halten sie für die ideale Lösung, um den sich ständig verändernden Anforderungen mobiler Unternehmensanwendungen gerecht zu werden. Deshalb sind in den nächsten Jahren eine starke Zunahme der PaaS-Angebote und eine Anpassung von mobilen Cloud-basierten SaaS-Branchenangeboten zu erwarten. Auf dieser Basis werden Unternehmen schon in Kürze flexible mobile Infrastruk-

turen bereitstellen können, die weit über die bisherigen Grenzen traditioneller IT-Systeme hinausgehen.

HYBRID CLOUD ALS ZUKUNFT

Die Grenzen der Unternehmens-IT zu erweitern, bedeutet im Idealfall, eine Kombination aus internen und externen Diensten und Anwendungen einzusetzen. Nur so können Mitarbeitende direkt auf geschäftsrelevante Daten zugreifen und überall produktiv arbeiten. Als Lösung für eine solche Kombination drängt sich die hybride Cloud beinahe auf. Zahlen des Cloud Monitor 2013 des BITKOM für Deutschland zeigen jedoch, dass sich die Mischform aus Private und Public Cloud noch nicht als Plattform etabliert hat. Während jedes dritte Unternehmen bereits Private-Cloud-Lösungen einsetzt, werden jedoch erst von 10 Prozent der Unternehmen Public-Cloud-Angebote genutzt. Trotz zahlreicher Vorteile haben rund ein Drittel der befragten Unternehmen nach wie vor starke Sicherheitsbedenken – insbesondere in Sachen Datenschutz. Dennoch liegen die Vorteile auf der Hand: Geringerer Implementierungs-, Betriebs- und Wartungsaufwand, Skalierbarkeit und flexibler Zugriff auf geografisch verteilte IT-Ressourcen.

RISIKOFAKTOREN DER CLOUD

Will ein Unternehmen mobile Arbeitsplätze einführen, bereitet den Verantwortlichen neben der Sicherheit der Anwendungen und mobilen Endgeräte vor allem die Absicherung der Cloud reichlich Kopfzerbrechen. Der Grund: Die Einhaltung der Sicherheitsvorschriften muss auch vom Cloud-Anbieter gewährleistet werden. Der Security Officer des Unternehmens hat darüber keine Kontrolle – wenn auch nur scheinbar. Nach Angaben der Cloud Security Alliance (CAS), einer Vereinigung von Anbietern von Cloud-Services, sind es neun Risiken, die einer breiten Akzeptanz von Cloud-Angeboten im Wege stehen. Im Report „The Notorious Nine: Cloud Computing Top Threats in 2013“ werden diese nach Sicherheitsrelevanz geordnet aufgelistet und entsprechende Gegenmaßnahmen formuliert. Datendiebstahl, Datenverlust, Missbrauch von Nutzerprofilen, unsichere Schnittstellen (API) und die Angst vor Denial-of-Service-Attacken gehören dabei zu den wichtigsten.

RISIKO NUMMER 1: DATENDIEBSTAHL

Der Datendiebstahl gilt als größtes Risiko, das sich aus Sicht der Unternehmen in den letzten drei Jahren stark erhöht hat. Das kritischste Szenario ist dabei, dass sensible Informationen unberechtigt in die Hände von Mitbewerbern fallen. Nach Angaben der Deutschen Handelskammer entsteht allein durch daraus resultierende Plagiate ein jährlicher Schaden von über 30 Milliarden Euro. Im Extremfall kann das geschädigte Unternehmen durch Datendiebstahl sogar vollständig vom Markt verdrängt werden. Das Marktforschungsinstitut Valid Research hat letztes Jahr im Auftrag der Firma Ernst & Young 400 Führungskräfte deutscher Unternehmen zum Thema Datendiebstahl befragt und ermittelt, dass das Risiko als stark steigend empfunden wird. Über 90 Prozent aller Unternehmen rechnen damit, dass konkurrierende Unternehmen (42 Prozent), Geheimdienste (17 Prozent), ehemalige oder eigene Mitarbeitende (15 Prozent) oder Onlineplattformen (15 Prozent) als Täterschaft in Frage kommen. Um dem Datendiebstahl zuvor zu kommen, schlägt die Cloud Security Alliance ein Paket von nicht weniger als elf verschiedenen Maßnahmen vor. Sie sind Bestandteil der so genannten „CSA Cloud Control Matrix“, einer detaillierten Checkliste, die eine systematische Vermeidung und Absicherung von Risiken im Cloud-Umfeld erlaubt. Sie liegt aktuell in der Version 3 vor und kann über die CAS-Website [1] bezogen werden.

RISIKO NUMMER 2: DATENVERLUST

An zweiter Stelle steht laut CAS das Risiko des direkten Datenverlusts in der Cloud. Ganz gleich ob versehentliches Löschen durch den Anbieter, ausgelöst durch Naturkatastrophen, Ausfälle in Rechenzentren, verlorene Kryptografieschlüssel oder absichtliche Löschung: Wichtige Daten gehen verloren. Dagegen existieren heute gut etablierte und durchgängige Technologien, die eine vollständige und automatische Überwachung der Datenmanipulation in- und außerhalb des Unternehmens unter Einhaltung der gesetzlichen Vorgaben erlauben. Diese Technologien werden unter dem Begriff Data Loss Prevention (DLP) zusammengefasst. Die grundlegende Idee des Ansatzes besteht darin, sämtliche Daten so zu beobachten, dass sie keine unkontrollierten Wege gehen können. Und dies auf den drei Ebenen Bewegungsdaten (über das Netzwerk aus dem Unternehmen heraus via Internet transferierte Daten), gespeicherte Daten (in Dateisystemen, Datenbanken und mittels anderen Speichermethoden abgelegte Daten) und Daten auf dem Endgerät (Laptop, USB-Stick, MP3 Player, Smartphones etc.). In einer Cloud-Umgebung sind die beiden Aspekte Bewegungsdaten und gespeicherte Daten zentral. Aus diesem Grund spielt beispielsweise auch der Speicherort eine entscheidende Rolle. Deutsche Unternehmen wollen ihre Daten am liebsten in Deutschland aufbewahrt wissen und stehen der Nutzung von Servern ausländischer Rechenzentren sehr kritisch gegenüber.

RISIKO NUMMER 3: MISSBRAUCH VON NUTZERPROFILEN

Kaum eine Woche vergeht, in der nicht über einen Diebstahl von Passwörtern berichtet wird. Obwohl in vielen Fällen vorwiegend private E-Mail- oder einfache Onlinenutzerkonten betroffen sind, ist dieses Risiko im Bereich unternehmensrelevanter Anwendungen und Daten zu berücksichtigen. Die Anzahl der Betrugsdelikte mit Zugangsberechtigungen nehmen in der Statistik des Cybercrime zwar nicht den ersten Platz ein, doch sind die Konsequenzen aufgetretener Fälle weitreichend. So können beispielsweise Nutzerprofile missbraucht werden, um einen unbemerkten Informationsdiebstahl zu begehen oder absichtlichen Datenverlust herbeizuführen. Deshalb schlägt die Cloud Security Alliance acht Cloud-Control-Matrix-Maßnahmen vor, die vom einfachen Zugriffsschutz bis hin zur weitreichenden Autorisierungsstrategie reichen.

MOBILE ARBEITSPLÄTZE ERFORDERN INDIVIDUELLE CLOUD-SECURITY-DISPOSITIVE

Der Einsatz hybrider Cloud-Infrastrukturen als zukünftige „Dritte Plattform“ eines Unternehmens sollte mit einer Anpassung der unternehmensinternen Sicherheitsdispositive einhergehen. Dies bedeutet nichts anderes, als bestehende IT-Sicherheitsrichtlinien auf ihre Wirksamkeit in einer Cloud-Umgebung zu prüfen. Anschließend sind die Cloud-Angebote entsprechend auszuwählen sowie bestehende Dienste nötigenfalls zu verändern. Für optimale Sicherheit sollten sämtliche Richtlinien, Standards und Vorgaben der Cloud Security Alliance konsequent umgesetzt werden. Sie bilden eine bis ins Detail durchdachte Basis für die Planung und Durchführung von Maßnahmen zur Risikominimierung. Allerdings ist diese sehr umfangreich: So umfasst alleine die Sicherheitsrichtlinie für kritische Bereiche im Cloud Computing vierzehn Domänen, die in einer „Trusted Cloud“-Referenzarchitektur abgebildet werden können. Doch auch gesunder Pragmatismus kann dabei helfen, die passenden Lösungen zu identifizieren. Das Jericho Cloud Cube Model unterscheidet beispielsweise anhand der vier Kriterien intern/extern, proprietär/offen, innerhalb/außerhalb und insourced/outsourced die Art und Weise, wie Mitarbeitende mobile zusammenarbeiten. Eine solche Klassifikation erlaubt die Zuordnung der Sicherheitsanforderungen an die bevorzugte Arbeitsweise und erleichtert damit die Klassifikation und Auswahl geeigneter Cloud-Infrastrukturen entscheidend.

Unternehmen, die für den Großteil ihrer Mitarbeiter mobile Arbeitsplätze zur Verfügung stellen möchten, kommen jedoch nicht umhin, früher oder später eigene Cloud-Security-Dispositive zu entwickeln. Dennoch können sie sich an den Überlegungen und Strategien aus dem DLP-Bereich orientieren – insbesondere dann, wenn für die mobile Arbeit private Geräte verwendet werden.

Links & Literatur

[1] http://cloudsecurityalliance.org/research/ccm/

Daniel Liebhart

ist Dozent für Informatik an der Hochschule für Technik in Zürich und Solution Manager der Trivadis AG. Er ist Autor des Buchs „SOA goes real“ (Carl Hanser Verlag) und Koautor verschiedener Fachbücher.