Publication: it&t business (A)
Publishing House: IT Media
Publication date: 11.11.2011
Page: 32

Cloud-Sicherheit ist machbar

Die Sicherheitsrisiken einer Zusammenarbeit von Unternehmen und Behörden in der öffentlichen Cloud sind beherrschbar, meint *Franz Kaiser*

Cloud-basierte Services haben ihre Vorteile: Selbstbedienung bei Bedarf, universeller Zugang zu Ressourcen und große Flexibilität. Die Kehrseite der Medaille ist jedoch die Anfälligkeit für Attacken, die von außerhalb der Cloud kommen. Daten laufen über öffentliche Netzwerke, und Risiken wie etwa Dateninfektion oder -verlust fallen höher aus als in klassischen, internen IT-Netzwerken.

Die größten Schäden werden oft gar nicht von Hackern oder Cyberkriminellen verursacht, sondern passieren auf dem „Transportweg", der über eine Cloud-basierte Infrastruktur führt. Um einem möglichen Schaden vorzubeugen gehört in erster Linie ein konsequentes Sicherheitsmodell aus definierten Zugangsrichtlinien, klarer Aufgabentrennung und unumstößlichen Protokollierungsverfahren definiert. Und es muss Technik eingesetzt werden.

Der Autor Franz Kaiser ist Regional Director Austria & Switzerland bei Fortinet

Daten-Infektion in der Cloud. Öffentliche Cloud-Infrastrukturen sind eine technische Herausforderung für Netzwerkmanager. Öffentliche Organisationen müssen ihre Schutzmechanismen überprüfen, bevor sie Daten in der Cloud ablegen, zirkulieren oder wieder in das eigene Netzwerk integrieren. Hier sind unter anderem Applikationskontrolle, Verschlüsselung, SSL-Inspektion, Data Leakage Protection und Anti-Virus zu nennen. Daten, die in der Cloud lediglich abgelegt sind, aber nicht zirkulieren, so genannte Data-at-Rest, können durch Verschlüsselungsverfahren vor nicht autorisierten Angriffen geschützt werden. Daten im Umlauf (Data-in-Motion) dagegen werden in der Cloud nicht unbedingt geprüft oder gereinigt. Es besteht also das Risiko, dass bereits in der Cloud infizierte Daten ins eigene Netzwerk gelangen können.

Speicher- und Transportsicherheit. Datentransfer und Zusammenarbeit in der Cloud setzen ein gut durchdachtes Konzept voraus. Als erstes sollte die Sicherheit der in der Cloud gespeicherten Daten bedacht werden. Diese hängt eng mit der Leistung der Cloud Hosting Service Provider zusammen, ob diese zum Beispiel Sicherheitsrichtlinien für die Zugangskontrolle haben und Maßnahmen zur Vermeidung undichter Stellen im Netzwerk treffen. Auch die Einhaltung rechtlicher Vorschriften seitens des Cloud-Anbieters muss vor der Auftragserteilung gründlich überprüft werden.

Im nächsten Schritt muss für die Sicherheit der Daten auf dem Transportweg gesorgt werden. Das Scannen von Applikationsinhalten auf Malware ist hier ebenso zu nennen wie deren Verschlüsselung und die gezielte Suche nach Bedrohungen bei der Überschreitung der Netzwerkgrenze.

Aber auch wenn alle diese Kriterien der Cloud-Sicherheit erfüllt sind, bleibt die Möglichkeit, dass Hacker ihre Angriffe auf eine bestimmte Organisation abzielen und Datenspionage oder Datendiebstahl erfolgreich durchführen.

Vergiftete Dokumente. Dateien mit hohen Zirkulationsraten sind für Cyberkriminelle besonders attraktiv. Jedes Dateiformat braucht eine Anwendungssoftware für die Anzeige und die Bearbeitung der Datei. „Vergiftete" Dateien (Poisoned Documents) entstehen dann, wenn eine „gesunde" Datei nach einer Modifizierung mit einer bösartigen Byte-Serie geladen wird. Ein solcher Angriff zielt auf ein bestimmtes Programm – etwa das Leseprogramm Adobe Reader (PDF) – ab, muss aber deshalb nicht auch bei einem alternativen Anwendungsprogramm (etwa dem FoxIT Reader) funktionieren. Auch unterschiedliche Versionen eines Programmes können den Angriffserfolg beeinflussen.

„Poisoned Document"-Angriffe können Massenangriffe sein, bei denen es einfach nur darum geht, möglichst viele User zu treffen.

Gezielte Attacken haben hingegen bestimmte Empfänger im Visier, sind effektiver – und werden häufiger. Dabei werden E-Mails verschickt, die auf den ersten Blick überzeugen, weil sie auf Ereignisse verweisen, mit denen der Empfänger vertraut ist. Wird die Datei geöffnet, installiert sich der bösartige Code und schleust auf dem Rechner Daten ein, die nach Systemstart die Kontrolle übernehmen, wie etwa Spy-

Trojaner oder die zur Bildung von Botnets führen. In der Regel wird zuerst ein Botnet-Agent installiert, der dem Angreifer berichtet und Malware (meistens ein Remote Administration Tool) herunterlädt. Einmal auf dem Rechner kann das Tool Files herunterladen, Screenshots machen und sogar die Webcam aktivieren.

Gegenmaßnahmen. Gegen solche Attacken lässt sich wappnen. Zeitnahes Patchen von Software-Updates ist hier genauso zu nennen wie konsequentes Identity-Management. Von Vorteil ist eine stets topaktuelle Sicherheitslösung, die zudem mehrschichtig aufgebaut ist und Anti-Virus, Intrusion Prevention, Web Filtering, Anti-Spam und Application Control-Optionen umfasst. Mit diesen Maßnahmen wird auch das Sicherheitsrisiko beim Einsatz von Cloud-Services beherrschbar. ■

Fortinet
www.fortinet.de