

Link: <https://www.computerwoche.de/a/die-9-groessten-cloud-gefahren,2542253>

Datenpanne, Account-Kidnapping & böartige Insider

Die 9 größten Cloud-Gefahren

Datum: 15.07.2013

Autor(en): Werner Kurzlechner

Die Cloud Security Alliance hat die neun größten Gefahrenherde beim Cloud Computing ermittelt. Datenpannen und -verluste stehen ganz oben im Ranking der Sicherheitsrisiken.



Foto: Iakov Kalinin - Fotolia.com

Cloud Computing wird immer beliebter, weil die Vorzüge offensichtlich sind: Flexibilität, Skalierbarkeit, Kostenersparnisse. Dass manche Anwender mit der Daten-Migration in die Wolke immer noch zögern, liegt traditionellerweise an Sicherheitsbedenken. Zwar arbeiten die Cloud-Anbieter beständig an der Behebung der Probleme. Und neue Security-Lösungen aus der Cloud gewinnen immer mehr an Gewicht. Nichtsdestotrotz wäre es fahrlässig, die Existenz spezifischer Sicherheitsprobleme in der Wolke zu leugnen. Welche das tatsächlich sind, hat die **Cloud Security Alliance**¹ (CSA) im Rahmen einer Studie ermittelt. Der nichtkommerzielle Verbund von Anbietern und IT-Experten identifizierte die neun wichtigsten Problemherde.

1. Datenpannen: Die CSA veranschaulicht das Risikopotenzial an einem Beispiel: So könnte eine Virtual Machine (VM) Timing-Informationen dazu benutzen, die privaten kryptographischen Schlüssel zu extrahieren, die von anderen VMs auf dem gleichen Server verwendet werden. Wenn eine Cloud Service-Datenbank nicht ordentlich gestaltet ist, könnten Hacker mit einem Einbruch in die Anwendungen eines Kunden zugleich an die Daten aller anderen Kunden gelangen.

Die Herausforderung bei dieser Art von Datenverlust liegt laut CSA darin, dass Maßnahmen zur Minimierung des Risikos andere Probleme verschärfen können. So verringere Verschlüsselung zwar die Auswirkungen von Datenpannen. Aber wer die Encryption-Schlüssel verliert, sei zugleich seiner Daten verlustig geworden. Wer sich dagegen wiederum durch Offline-Backups absichert, macht sich laut CSA zugleich wieder anfälliger für neue Datenpannen.

2. Datenverlust: Wertvolle Daten verschwinden spurlos im Äther, so das CSA-Szenario. Die Ursachen dafür können vielfältig sein: ein löschwütiger Hacker, ein sorgloser Cloud-Provider oder eine Naturkatastrophe wie Feuer, Erdbeben oder Flut. Vor Diebstahl kann man sich durch Verschlüsselung schützen – wenngleich mit den bereits genannten möglichen Nebenwirkungen. Riskant ist Datenverlust laut CSA aber nicht alleine im Hinblick auf die Kundenbeziehung, sondern auch wegen der zu erfüllenden Compliance-Vorschriften.

3. Entführung von Accounts und Service Traffic: eine jenseits der Wolke unbekannt Gefahr, so die CSA. Gelangen Hacker an Berechtigungen, können sie Transaktionen und Aktivitäten ausspähen, Daten manipulieren, falsche Informationen streuen und unter falschem Namen auf dubiose Seiten navigieren. Die Angreifer können sich den guten Ruf des Opfers einverleiben, um Folgeattacken zu reiten. Dagegen hilft es nur, sorgfältig auf die Berechtigungen aufzupassen. „Unternehmen sollten darauf achten, einen Account-Austausch zwischen Usern und Services zu unterbinden“, so die CSA. „Und sie sollten die starke Authentifizierung mit zwei Faktoren einsetzen, wo das möglich ist.“

4. Unsichere Interfaces und APIs: IT-Administratoren vertrauen bei Provisioning, Orchestrierung und Monitoring auf Interfaces. APIs sind entscheidend für die Sicherheit und Zugänglichkeit von allgemeinen Cloud-Diensten. Die Komplexität wächst allerdings, wenn Dritte über die Interfaces Add-On-Services einbauen. Die CSA rät deshalb dazu, sich die möglichen Risiken schwacher Interfaces und APIs zu vergegenwärtigen.

Ausfallzeiten können Provider Kunden kosten

5. Denial of Service (DoS): Im Zeitalter des Cloud Computings können durch Hacker verursachte Ausfallzeiten die Provider Kunden Kosten – und die Anwender Geld. Dann nämlich, wenn die Rechnungen auf Compute Cycles und Verbrauch an Speicherplatz basieren. Sogar wenn es den Angreifern nicht gelingt, den Service komplett zur Strecke zu bringen, kann das teuer werden, mahnt die CSA.

6. Böartige Insider: In einem schlecht ausgestalteten Cloud-Szenario, können böswillige Mitarbeiter, Zulieferer und Geschäftspartner laut CSA besonders großen Schaden anrichten. Von Infrastructure-as-a-Service (IaaS) über Platform-as-a-Service (PaaS) zu Software-as-a-Service (SaaS) stehen auf verschiedenen Ebenen Zugänge zu kritischen Systemen und Daten offen. Besonders hoch sei das Risiko, wenn der Cloud-Provider alleine für die Sicherheit verantwortlich ist. Das gelte umso mehr, wenn Verschlüsselungs-Codes nicht auch im eigenen Unternehmen vorhanden seien.

7. Cloud-Missbrauch: Damit sind Attacken gemeint, bei denen beispielsweise Cloud-Services zum Knacken von Encryption-Keys benutzt werden oder Cloud-Server als Einfallstor für Schadsoftware dienen. Die Aufgabe der Provider ist laut CSA, Missbrauch zu definieren und Prozesse zur Identifizierung aufzusetzen.

Ausreichende Ressourcen-Ausstattung hilft Cloud-Risiken zu verstehen

8. Ungenügende Due Diligence: Mängel in der Risikoprüfung treten laut CSA auf, wenn Unternehmen das Cloud-Umfeld und die damit verbundenen Risiken nicht umfänglich verstehen. So könnten sich vertragliche Fragen zu Haftung und Transparenz auf Seiten des Providers auf tun. Hinzu könnten betriebliche und architektonische Fragen kommen, wenn das eigene Entwickler-Team nicht vertraut genug mit der Cloud-Technologie ist. Die CSA empfiehlt, für eine ausreichende Ressourcen-Ausstattung zu sorgen und vor dem Abflug in die Wolke alle Umstände sorgfältig zu prüfen.

9. Bedrohungen durch Shared Technology: Zuletzt weist die CSA darauf hin, dass die Provider in der Cloud Infrastruktur, Plattformen und Anwendungen miteinander teilen. Im Cloud-Liefermodell bestehe deshalb die Gefahr, mit Problemen an irgendeiner Stelle dieser geteilten Technologie konfrontiert zu werden. Empfohlen wird eine defensive und vertiefte Strategie, die eine gründliche Sicherung und ein umfassendes Monitoring beinhaltet.

Links im Artikel:

¹ <https://cloudsecurityalliance.org/>

IDG Tech Media GmbH
Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.