Quelle: https://blogs.technet.microsoft.com/germany/2016/04/20/die-zwlf-grten-sicherheitsrisiken-in-der-cloud/

Michael Kranawetter – NSO vom 20. April 2016

Die zwölf größten Sicherheitsrisiken in der Cloud

Cloud-Computing wird von immer mehr Unternehmen eingesetzt, um die eigene IT ausfallsicherer und effizienter zu machen. Doch häufig wird dabei übersehen, dass es auch hier Risiken für die Datensicherheit gibt. So stellte die Cloud Security Alliance (CSA) The Treacherous 12 zusammen, eine Beschreibung der zwölf größten Sicherheitsrisiken für Daten in der Cloud. Das Dokument richtet sich in erster Linie an die Betreiber von Cloud-Services, hält aber auch etliche Tipps für Kunden bereit.

1. **Datenverluste**
   Cloud-Provider sind zum Einhalten bestimmter Sicherheitsstandards verpflichtet. Werden sie nicht eingehalten und es kommt zu Datenverlusten, drohen hohe Strafen und empfindliche Reputationsverluste. Allerdings sind nicht nur die Provider für den Schutz der Daten verantwortlich, sondern auch die Anwender. Empfohlen werden eine Multifaktor-Authentifizierung und Verschlüsselung.
2. **Unzureichendes Identitäts-, Zugangs- und Zugriffsmanagement**
   Datenverluste und Hackerangriffe werden begünstigt durch ein fehlendes oder mangelhaftes skalierbares Identitätsmanagement-System, das Fehlen einer Multifaktor-Authentifizierung, die Verwendung schwacher Passwörter und den Verzicht auf den automatischen Austausch von Schlüsseln, Kennwörtern und Zertifikaten.
3. **Unsichere Bedienoberflächen und APIs**
   Schnittstellen sind besonders gefährdet, da sie zum einen die Verbindung zur Software von Drittanbietern herstellen und zum anderen meist übers Internet erreichbar sind. Die erste Verteidigungslinie muss daher die Kontrolle des Codes und eine kontinuierliche Überwachung umfassen.
4. **Systemschwachstellen**
   Sicherheitslücken sind ein bekanntes Phänomen, in der Cloud werden ihre Auswirkungen potenziert. Die CSA empfiehlt regelmäßige Scans auf Schwachstellen, eine schnelle Reaktion auf bekanntgewordene Bugs und die sofortige Installation von Security-Patches und Updates.
5. **Account Hijacking**
   Der Diebstahl von Account-Daten birgt bei Cloud-Diensten zusätzliche Gefahren in sich, da die Angreifer die Aktivitäten und Transaktionen des rechtmäßigen Besitzers überwachen, Daten verändern, falsche Informationen verbreiten und ihn auf manipulierte Seiten führen können. Notwendig ist ein kontinuierliches Monitoring der Benutzeraktivitäten, das gilt auch für die Service-Accounts.
6. **Kriminelle Insider**
   Sie können in einer Cloud-Umgebung besonders viel Schaden anrichten. Die CSA

empfiehlt, dass Cloud-Kunden die Datenverschlüsselung unter eigener Kontrolle behalten und Zuständigkeiten auf mehrere Personen aufteilen.

7. **Advanced Persistent Threads**
   Angriffe, bei denen Unternehmen über längere Zeit hinweg ausgespäht werden, haben in den vergangenen Jahren zugenommen. Cloud-Kunden sollten sich kontinuierlich über aktuelle Bedrohungen informieren und ihre Mitarbeiter entsprechend schulen.
8. **Datenverluste**
   Daten können nicht nur durch Hackerattacken verlorengehen, sondern auch durch versehentliche Löschungen, Naturkatastrophen und ähnliches. Anwender sollten sich über die Sicherheitsmaßnahmen ihres Providers informieren und bei besonders kritischen Daten eventuell das Vorhalten einer lokalen Kopie erwägen.
9. **Nicht erfüllte Sorgfaltspflicht**
   Unter diesem Punkt fasst die CSA die mangelhafte Recherche der Kunden über die Rahmenbedingungen des Cloud-Computing zusammen.
10. **Missbrauch von Cloud-Services**
    Aufgrund der hohen Rechenleistung und des nahezu unbegrenzten Speicherplatzes werden Cloud-Services gerne auch für kriminelle Aktivitäten verwendet, wie etwa das Knacken von Passwörtern oder DDoS-Attacken. Cloud-Provider benötigen daher Mechanismen, um solchen Missbrauch zu entdecken, sowie eine Möglichkeit, damit Kunden und andere Anwender entsprechendes Feedback liefern können.
11. **DoS-Attacken**
    Denial-of-Service-Angriffe können ganze Cloud-Systeme abbremsen oder sogar komplett in die Knie zwingen. Umso wichtiger sind ein Monitoring der Systeme sowie bereits vorbereitete und ständig erreichbare Abwehrmaßnahmen.
12. **Schwachstellen in geteilten Systemen**
    In der Cloud teilen sich mehrere Anwender die gleiche Infrastruktur, Plattform oder Applikation. Eine Schwachstelle kann daher das gesamte Cloud-Angebot eines Providers betreffen. Notwendig sind daher eine umfassende Sicherheitsstrategie sowie Maßnahmen wie eine Multifaktor-Authentifizierung sowie host- und netzwerkbasierte Intrusion-Detection-Systeme.