Cloud Account Hijacking: Best Practices gegen Kontenmissbrauch durch Cyberkriminelle

Die Cloud bringt eine Fülle von Vorteilen für Unternehmen mit sich, darunter reduzierte Kosten und flexible Skalierung, bietet Cyberkriminellen jedoch auch eine große Angriffsfläche, da enorme Datenmengen an einem Ort gespeichert sind. Cloud Account Hijacking auf Unternehmensebene ist besonders verheerend, wenn dadurch vertrauliche oder geschäftskritische Daten durchsickern oder gefälscht werden. Dies kann erhebliche Kosten, rechtliche Konsequenzen und Reputationsschäden verursachen.

Cloud Account Hijacking ist eine gängige Taktik, bei der Cyberkriminelle gestohlene Kontoinformationen eines Opfers missbrauchen. Beispielsweise für das Auspionieren von Unternehmensaktivitäten und Finanztransaktionen, Datenmanipulation und Datendiebstahl sowie weiterführende Spear Phishing-Angriffe auf Kollegen und Geschäftspartner.

Proaktive Maßnahmen bereits bei der Auswahl von Cloud Service Providern
Unternehmen sollten deshalb bereits bei der Auswahl von Cloud Service Providern proaktive Maßnahmen ergreifen: Diese beinhalten die sorgfältige Überprüfung potenzieller Verträge und der Vergleich der Cloud-Sicherheits- und Datenintegritätssysteme verschiedener Provider. Auch sollte bei der Bewertung die Anzahl der Datenverluste, Störungen und Ausfallzeiten, die ein Cloud Service Provider erlebt hat, miteinbezogen werden und auf welche Weise er Schwachstellen überwacht und verwaltet.

Grundlegende Maßnahmen gegen Cloud Account Hijacking

• Multifaktor-Authentifizierung und starke Passwörter: Konten mit starken, nicht mehrfach verwendeten Passwörtern zu schützen, ist eine bewährte Best Practice. Unternehmen sollten ihre Mitarbeiter über die Standards zur Generierung starker Passwörter aufklären und gegebenenfalls zusätzlich sichere Passwortmanager nutzen. Darüber hinaus gibt es verschiedene Multifaktor-Authentifizierungs-Tools, die von den Usern die Eingabe von statischen Passwörtern sowie dynamischen Einmalpasswörtern verlangen, die per SMS, Hardware-Token, Biometrie oder anderen Verfahren bereitgestellt werden können.

• Einschränkung der IP-Adressen, die für den Zugriff auf Cloud-Anwendungen zugelassen sind: Einige Cloud-Anwendungen bieten Tools zum Festlegen zulässiger IP-Bereiche und zwingen Benutzer, nur über Unternehmensnetzwerke oder VPNs auf die Anwendung zuzugreifen.

• Verschlüsselung von sensiblen Daten, bevor sie in die Cloud gelangen.

• Backups: Zudem sollte sichergestellt werden, dass alle Daten gesichert sind, falls Daten in der Cloud verloren gehen.

• Mitarbeiterschulungen: Da Cyberkriminelle häufig über Social-Engineering-Angriffe Account-Daten erschleichen, ist es wichtig, die Mitarbeiter umfassend über Phishing- und Spear-Phishing-Taktiken aufzuklären. Phishing-E-Mails beinhalten häufig bösartige Anhänge zur Verbreitung von Malware oder Links zu gefälschten Webseiten, die Account-Daten abgreifen. Eine umfassende Aufklärung der Mitarbeiter, wie sie betrügerische Nachrichten erkennen können, trägt wesentlich dazu bei, diesen gängigen Bedrohungsvektor zu entschärfen. Zudem sollten Angestellte darüber informiert werden, welche Konsequenzen bei einem möglichen Datendiebstahl oder bei Datenmanipulation drohen.

Datenzentrierte Sicherheitslösungen gegen Cloud Account Hijacking

Für einen erweiterten Schutz vor Datendiebstahl sollten Unternehmen Sicherheitsplattformen wählen, die sich bis in die Cloud und ins Mobilfunknetz erstrecken. Diese Art von Datensicherheitsplattformen sollte Cloud-Security-Funktionen wie End-to-End-Verschlüsselung, Anwendungskontrolle, kontinuierliche Datenüberwachung und die Möglichkeit beinhalten, riskante Datenaktivitäten basierend auf Verhaltens- und Kontextfaktoren, die den Benutzer-, Ereignis- und Datenzugriffstyp betreffen, zu kontrollieren oder zu blockieren.

Data Loss Prevention-Tools (DLP) überwachen und steuern Endpunkt-Aktivitäten, überwachen Daten in der Cloud und filtern Datenströme in Unternehmensnetzwerken, um diese sowohl im Ruhezustand, in Bewegung sowie bei Verwendung zu schützen – selbst im Fall eines Sicherheitsverstoßes. Sobald Verstöße erkannt werden, verhindern DLP-Lösungen durch Warnmeldungen, Verschlüsselung und andere Schutzmaßnahmen, dass Angreifer unternehmenskritische Daten stehlen oder Mitarbeiter diese versehentlich teilen und dadurch die Unternehmenssicherheit gefährden.

Dieser datenorientierte und mehrschichtige Ansatz aus Best Practices und Technologien ermöglicht es Unternehmen, Cloud-Sicherheitsrisiken effektiv zu managen und gleichzeitig die Vorteile der Wolke voll auszuschöpfen.