Dürfen GMP-Daten in die Cloud?

Potenzielle Risiken der Cloud-Nutzung

Unzureichendes Identitäts-, Berechtigungs- und Zugriffsmanagement
Die Zugänglichkeit der Cloud, die Remote-Arbeiten von überall mit einer Internetverbindung ermöglicht, ist eines ihrer (vielen) Verkaufsargumente. Wenn dieses Potenzial, sich aus der Ferne mit Netzwerken und Plattformen zu verbinden, jedoch genutzt wird, kann es Sicherheitsrisiken bergen. Hacker können sich als legitime Benutzer ausgeben, um Zugang zu Cloud-Ressourcen und -Systemen zu erhalten und diese zu nutzen.

Unsichere Schnittstellen und Anwendungsprogrammierschnittstellen
APIs bieten Benutzern die Möglichkeit, ihre Cloud-Umgebung zu verwalten, zu entwickeln und anzupassen. Diese sehr offene und zugängliche Natur kann jedoch eine Bedrohung für die Cloud-Sicherheit darstellen, denn wenn Einzelpersonen und Unternehmen Cloud-Dienste an ihre Bedürfnisse anpassen, gibt es Raum für Fehler und Fehlkonfigurationen. Schnittstellen sind in der Regel auch der am stärksten exponierte Teil einer Cloud-Umgebung, möglicherweise mit einer öffentlichen IP-Adresse, was es wichtig macht, diese entsprechend zu sichern.

Fehlkonfigurationen und unzureichende Änderungskontrolle

Fehlkonfigurationen sind die falsche oder suboptimale Einrichtung von Computer-ressourcen, die sie anfällig für Fehler machen können. Eine unzureichende Änderungs-kontrolle in Cloud-Umgebungen kann zu falschen Konfigurationen führen und verhindern, dass Fehlkonfigurationen behoben werden.

Fehlende Cloud-Sicherheitsarchitektur und -strategie
Cloud-Sicherheitsstrategie und -Sicherheitsarchitektur umfasst die Berücksichtigung und Auswahl von Cloud-Bereitstellungsmodellen, Cloud-Service-Modellen, Cloud-Service-Providern (CSPs), Service-Region-Verfügbarkeitszonen und spezifischen Cloud-Diensten. Unternehmen sollten vorab Geschäftsziele, Risiken, Sicherheitsbedrohungen und die Einhaltung gesetzlicher Vorschriften bei der Gestaltung und Entscheidung von Cloud-Services und -Infrastrukturen berücksichtigen.

Unsichere Softwareentwicklung
Cloud-Technologien erhöhen die Komplexität von Software. Dadurch können unbeabsichtigte Funktionen entstehen, die die Erstellung von „Exploits" (Programme, die Sicherheitslücken ausfindig machen und ausnutzen) und wahrscheinlichen Fehlkonfigurationen ermöglichen könnten. Dank der Zugänglichkeit der Cloud können Angreifer diese „Funktionen" einfacher als je zuvor nutzen.

Quelle: Cloud Security Alliance (CSA), Report 2022 "Top Threats to Cloud Computing – Pandemic Eleven", Erläuterung und Übersetzung der Begriffe: Dr. Peter Schober

GMP VERLAG Peither

Unsichere Drittanbieter-Ressourcen
Eine Ressource eines Drittanbieters kann bedeuten: Open-Source-Code über SaaS-Produkte und API-Risiken bis hin zu einem managed Service eines Cloud-Anbieters. Risiken, die von Ressourcen Dritter ausgehen, bestehen in Schwachstellen für Exploits und hackbaren Konfigurationen.

Systemschwachstellen
Das sind Fehler in Cloud-Service-Plattformen. Sie können ausgenutzt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gefährden und den Dienstbetrieb zu stören. Alle Cloud-Komponenten können Schwachstellen enthalten, die Cloud-Dienste anfällig für Angriffe machen können.

Versehentliche Offenlegung von Daten in der Cloud
Die zunehmende Anzahl von Konfigurationen für Cloud-Ressourcen führt dazu, dass Fehlkonfigurationen häufiger auftreten. Mangelhafte Transparenz im Cloud-Inventar und eine entsprechende Netzwerkgefährdung können zu unbeabsichtigten Datenlecks führen. Darüber hinaus verwenden z. B. viele Datenbanken schwache Passwörter oder benötigen keine Authentifizierung, was sie zu einem leichten Ziel für Angreifer macht.

Fehlkonfiguration und Nutzung von Serverless und Container-Workloads
Serverless (zu Deutsch: Serverlos, ohne Server) ist ein Ausführungsmodell, bei dem der Cloud-Anbieter (z. B. AWS, Azure oder Google Cloud) für die Ausführung von Code verantwortlich ist, indem er die Ressourcen dynamisch zuweist. Der Code wird normalerweise in sogenannten „Containern" (zu Deutsch: Programmhüllen ohne Langzeitspeicher) ausgeführt. Eine spezifische Konfiguration dieser Container kann unter bestimmten Bedingungen zum unerwünschten Einfallstor für Schadsoftware (sog. Malware) werden.

Organisiertes Verbrechen, Hacker und hochentwickelte anhaltende Cyber-Bedrohungen
Damit sind kriminelle oder politisch motivierte Angriffe gemeint, die professionell ausgeführt werden zum Zwecke von Erpressung, Raub, Sabotage oder Spionage.

Exfiltration (kopieren, übertragen, abrufen) von Daten aus der Cloud
Das betrifft sensible, geschützte oder vertrauliche Informationen. Diese Daten können von einer Person außerhalb der Organisation freigegeben, angezeigt, gestohlen oder verwendet werden. Datenexfiltration kann das primäre Ziel eines gezielten Angriffs sein. Das kann aus einer ausgenutzten Schwachstelle resultieren oder aufgrund von Fehlkonfigurationen, Anwendungsschwachstellen oder schlechten Sicherheitspraktiken.

Quelle: Cloud Security Alliance (CSA), Report 2022 "Top Threats to Cloud Computing – Pandemic Eleven", Erläuterung und Übersetzung der Begriffe: Dr. Peter Schober