Attack Simulation Tools for Amazon Web Services (AWS)

Studiengang: MAS Cyber Security

Die unverzichtbare Rolle von Security Testing in modernen IT-Strukturen: Eine tiefgreifende Untersuchung mit Fokus auf Cloud Computing und Open-Source-Lösungen.

Einleitung

In der heutigen digitalen Ära hat sich Cloud Computing als ein fundamentaler Baustein moderner IT-Infrastrukturen etabliert. Amazon Web Services (AWS), revolutioniert als marktführender Anbieter die Bereitstellung skalierbarer Ressourcen, gekoppelt mit einer transparenten Kostenstruktur. Diese Entwicklung birgt jedoch bei omnipräsenter Internetverbindung das erhöhte Risiko von Cyberangriffen, sofern sie ohne Implementierung nicht adäquater Sicherheitsmechanismen einhergeht.

Ausgangslage

AWS offeriert ein umfangreiches Spektrum an cloudbasierten Dienstleistungen, die von Unternehmen weltweit genutzt werden. Trotz eines robusten Sicherheitsrahmenwerks sind immer wieder neue Schwachstellen erkennbar, die potenziell von Cyberkriminalität ausgenutzt werden können. Dies unterstreicht den fortwährenden Bedarf an Verstärkung von Sicherheitsvorkehrungen, um Daten und Anwendungen wirksam zu schützen.

Ziel

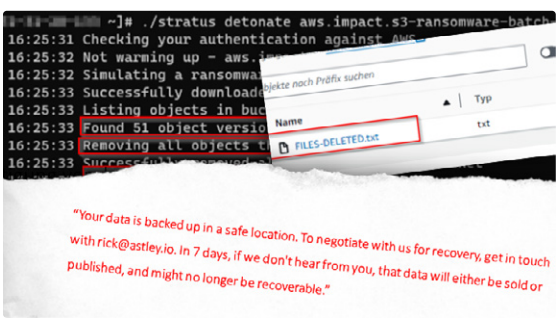
Das Hauptziel dieser Arbeit besteht darin, eine umfassende Vergleichsanalyse von Open-Source-Softwarelösungen durchzuführen, die speziell darauf ausgelegt sind, Schwachstellen in Cloud-Umgebungen zu identifizieren, und deren Kompatibilität mit AWS zu evaluieren. Durch eine methodische Untersuchung werden zwei herausragende Tools ausgewählt, um deren Effektivität in einer kontrollierten AWS-Sandbox-Umgebung zu testen. Dabei wird besonderes Augenmerk auf etablierte Cyber-Sicherheitsstandards, einschliesslich des renommierten MITRE ATT&CK Frameworks, gelegt. Ziel ist es, die Wirksamkeit der vorhandenen Erkennungssysteme für Angriffsszenarien signifikant zu verbessern.

Abschluss und Ausblick

Die Wahrung der Sicherheit in Cloud-Umgebungen stellt einen kontinuierlichen Prozess dar, der regelmässige Überprüfung und Aktualisierung erfordert. Diese Arbeit befasst sich mit der Untersuchung und Bewertung von Open-Source-Tools zur Unterstützung der Sicherheitsmassnahmen in Cloud-Infrastrukturen. Durch die Optimierung bestehender Sicherheitssysteme kann die Widerstandsfähigkeit gegenüber Cyberbedrohungen verbessert werden, was zu einer verstärkten Sicherheit der digitalen Ressourcen des Unternehmens beiträgt.

Beispiel anhand eines Use-Cases: Die Risiken durch nachlässige und inkonsistente Prüfungen IAM-Richtlinien aufzeigen

Ein einziger Konfigurationsfehler in den IAM-Richtlinien kann unerwartet die Sicherheitsschleusen öffnen und Angreifern ermöglichen, unbemerkt tiefgreifende Kontrolle über fast die gesamte Cloud-Infrastruktur zu erlangen. Dieser Use-Case beleuchtet, wie durch unsachgemässe Konfigurationen von IAM-Richtlinien Sicherheitslücken entstehen, die Cyberkriminelle mit Open-Source-Software ausnutzen können, um erhöhte Berechtigungen zu erlangen. Durch das Erlangen des Administratorzugriffs können Angreifer kritische Aktionen ausführen, allen voran das Erstellen von Zugangsschlüsseln, das Auslesen vertraulicher Informationen und das Initiieren schädlicher Operationen.



Beispiel eines Use-Cases

Kiatbodin Koetsuk
MAS Cyber Security