Microservices und Sicherheit

Seminar Komponenten, Agenten und Workflows in verteilten Systemen

Felix Ortmann und Konstantin Möllers
{0ortmann,1kmoelle}@informatik.uni-hamburg.de

Universität Hamburg
Fachbereich Informatik
Vogt-Kölln-Straße 30
22527 Hamburg

Zusammenfassung. Mit der stetig zunehmenden Diversifikation von Informationssystemen im Internet ist ein Bedarf für eine verteilte und skalierbare Architektur aufgekommen. So entstand etwa der neue Trend zur Microservice-Infrastruktur. Allerdings birgt diese Risiken in Bezug auf Sicherheit, da sowohl Architektur als auch Kommunikation eines Microservice-Netzwerks Sicherheitsprobleme aufwerfen können. In diesem Aufsatz gehen wir daher auf diese Probleme ein und zeigen für drei Schutzziele Lösungsmöglichkeiten auf. Es wird gezeigt, dass es bereits Möglichkeiten und neuartige Technologie gibt um sich vor Angriffen zu schützen.

1 Einführung

2 Microservice-Architekturen und Sicherheit

3 Kommunikation und Sicherheit

4 Schutzziele

Nachdem wir bisher auf die Architektur und die Kommunikation von Microservices eingegangen sind, betrachten wir im folgenden Abschnitt Angriffspunkte einer solchen Infrastruktur. Explizit werden drei Schutzziele der Informationssicherheit betrachtet, welche eine besondere Relevanz in verteilten Systemen spielen. Zunächst gehen wir auf das der Vertraulichkeit in Unterabschnitt 4.1 ein. Weitergehend setzt sich Unterabschnitt 4.2 mit der Verfügbarkeit und zuletzt **??** mit der Integrität von Informationen innerhalb eines Microservice-Netzwerks auseinander.

4.1 Vertraulichkeit

„Informationsvertraulichkeit ist bei einem IT-System gewährleistet, wenn die darin enthaltenen Informationen nur Befugten zugänglich sind. Dies bedeutet, dass die sicherheitsrelevanten Elemente nur einem definierten Personenkreis bekannt werden. Dazu sind Maßnahmen zur Festlegung sowie zur Kontrolle zulässiger Informationsflüsse zwischen den Subjekten des Systems nötig (Zugriffsschutz und Zugriffsrechte), sodass ausgeschlossen werden kann, dass Informationen zu unautorisierten Subjekten ‚durchsickern'." (Bedner & Ackermann, 2010)

Handshake-basierte Authentifikation

Token-basierte Authentifikation

4.2 Verfügbarkeit

„Die Verfügbarkeit betrifft sowohl informationstechnische Systeme als auch die darin verarbeiteten Daten und bedeutet, dass die Systeme jederzeit betriebsbereit sind und auf die Daten wie vorgesehen zugegriffen werden kann. Zum einen muss die Datenverarbeitung inhaltlich korrekt sein und zum anderen müssen alle Informationen und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden." (Bedner & Ackermann, 2010)

Redundanz und Lastverteilung

Client-seitige Lastverteilung

Kontinuierliches und unabhängiges Deployment

4.3 Integrität

„Integrität oder Unversehrtheit bedeutet zweierlei, nämlich die Vollständigkeit und Korrektheit der Daten (Datenintegrität) und die korrekte Funktionsweise des Systems (Systemintegrität). Vollständig bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Daten, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben. Die Integrität bedeutet, dass Daten im Laufe der Verarbeitung oder Übertragung mittels des Systems nicht beschädigt oder durch Nichtberechtigte unbefugt verändert werden können. Beschädigungs- oder Veränderungsmöglichkeiten sind das Ersetzen, Einfügen und Löschen von Daten oder Teilen davon.“ (Bedner & Ackermann, 2010)

Verschlüsselungsverfahren

5 Zusammenfassung

Literatur

Bedner, M. & Ackermann, T. (2010). Schutzziele der IT-Sicherheit. *Datenschutz und Datensicherheit*, *5*, 323 - 328.

Fowler, M. & Lewis, J. (2014, März). Microservices. A definition of this new architectural term.