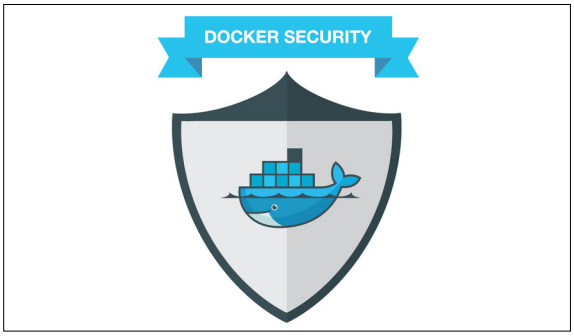
Fabio
Caspani

Container Security



Docker Security Logo
docker.com

Ausgangslage: In dieser Arbeit wurde eine Software entwickelt, um Sicherheitsrisiken von Applikationscontainern zu veranschaulichen, da in den letzten Jahren die Container stark an Bedeutung gewonnen haben. Einige der häufigsten Sicherheitsrisiken von Docker Containern werden in einer Demonstrationssoftware aufgezeigt. Der Umfang der Demonstrationssoftware wurde in einer Vorstudie beleuchtet und eingegrenzt. Im Zusammenhang mit der Demonstrationsumgebung wurde das automatisierte Container Auditing Programm «Docker Bench for Security» untersucht.

Ergebnis: Die entwickelte Demonstrationssoftware umfasst sieben allgemeine Sicherheitsrisiken, von unsicheren Netzwerken bis zu Ausbrüchen aus dem Container, welchen Docker Container ausgesetzt sein können. Der Anwender kann in der Software jeweils die Vulnerabilität ausnutzen und die Sicherheitslücke anschliessend beheben. Das Container Auditing Programm «Docker Bench for Security» erwies sich in dieser Form als ungeeignet für die Sicherheitsprüfung von Containern. Da alle Container eines Hosts gleichzeitig statisch analysiert werden, entfällt die Möglichkeit, auf die Sicherheitsanforderungen der einzelnen Container einzugehen. Die Audit Software macht zudem auch keine Gewichtung der einzelnen Tests. Dies kann zu einer massiven Verfälschung des Gesamtergebnisses führen. Ebenfalls wird die Auswertung unübersichtlich, da eine visuelle Unterscheidung fehlt. Sowohl betreffend Prioritäten wie auch Kategorien der Testfälle. Es wird deshalb empfohlen, eigene Sicherheitsstandards zu entwerfen und diese den Bedürfnissen des Projekts anzupassen. In der Zukunft ist es möglich, die Demonstrations-software weiter auszubauen oder eine Gewichtung in die Audit Software zu implementieren.