

HOCHSCHULE DER MEDIEN

BACHELORARBEIT

Sicherheitsbetrachtungen von Applikations-Containersystemen in Cloud-Infrastrukturen am Beispiel Docker

Moritz Hoffmann

Studiengang: Mobile Medien

Matrikelnummer: 26135

E-Mail: mh203@hdm-stuttgart.de

Dezember 2015

Erstbetreuer:

Prof. Dr. Joachim Charzinski
Hochschule der Medien

Zweitbetreuer:

Patrick Fröger
ITI/GN, Daimler AG

Sicherheitsbetrachtungen von Applikations-Containersystemen in Cloud-Infrastrukturen am Beispiel Docker

Moritz Hoffmann
Studiengang Mobile Medien,
Hochschule der Medien
`mh203@hdm-stuttgart.de`

Dezember 2015

Eidesstattliche Erklärung

„Hiermit versichere ich, Moritz Hoffmann, ehrenwörtlich, dass ich die vorliegende Bachelorarbeit mit dem Titel: „Sicherheitsbetrachtungen von Applikations-Containersystemen in Cloud-Infrastrukturen am Beispiel Docker“ selbstständig und ohne fremde Hilfe verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Arbeit, die dem Wortlaut oder dem Sinn nach anderen Werken entnommen wurden, sind in jedem Fall unter Angabe der Quelle kenntlich gemacht. Die Arbeit ist noch nicht veröffentlicht oder in anderer Form als Prüfungsleistung vorgelegt worden. Ich habe die Bedeutung der ehrenwörtlichen Versicherung und die prüfungsrechtlichen Folgen (§26 Abs. 2 Bachelor-SPO (6 Semester), § 24 Abs. 2 Bachelor-SPO (7 Semester), § 23 Abs. 2 Master-SPO (3 Semester) bzw. § 19 Abs. 2 Master-SPO (4 Semester und berufsbegleitend) der HdM) einer unrichtigen oder unvollständigen ehrenwörtlichen Versicherung zur Kenntnis genommen.“

Unterschrift

Datum

Abstract

English version:

....
..

Deutsche Version:

....
...
.
..

Inhaltsverzeichnis

1	Überblick	5
1.1	Arten von Virtualisierungen	5
1.1.1	Einordnung Docker	5
1.2	Einführung in Docker	5
2	Ziel der Arbeit/Forschungsfrage	6
3	Security aus Linux Kernel-Features	7
3.1	Isolierung	7
3.1.1	namespaces	7
3.1.1.1	user namespaces	7
3.1.2	capabilities	7
3.1.2.1	Beispiele, /proc-Verzeichnis, (Un-)Mounten des Host-Filesystems	7
3.1.3	Mandatory Access Control (MAC)	7
3.1.3.1	Beispiel SELinux	7
3.2	Ressourcenverwaltung	7
3.2.1	cgroups	7
3.3	Docker im Vergleich zu anderen Containerlösungen	7
4	Security im Docker-Ökosystem	8
4.1	Docker Images und Repositories	9
4.1.1	neues Signierungs-Feature	9
4.2	Docker Daemon	9
4.2.1	REST-API	9
4.2.2	Support von Zertifikaten	9
4.3	Docker Cache	9
4.4	privileged Container	9
4.5	Networking	9
4.5.1	bridge Netzwerk	9
4.5.2	overlay Netzwerk	9
4.5.3	DNS	9
4.5.4	Portmapping	9

4.6	Daten-Container	9
4.7	Docker mit VMs	9
4.8	Tools rund um Docker	9
4.8.1	Docker Swarm	9
4.8.2	Docker Compose	9
4.8.3	Nautilus Project	9
4.8.4	Vagrant	9
4.8.5	Kubernetes	9
5	Docker in Unternehmen/Cloud-Infrastrukturen	10
6	Fazit/Ausblick	11

Abbildungsverzeichnis

1	Awesome Image	4
---	-------------------------	---

Tabellenverzeichnis

Hallo One more line joooooo [?]



Abbildung 1: Awesome Image

lkasjdflkj asldkjf lasjkdfkadsjf ladksjflkjsldkf dslfjklaks df a sdfjaldsfj
ladksjf lkjlakjsd f asdf aljsdflkjasldfjalsdfj l adskjflj d f dslkfjalksdjf sd fljsdf-
kjsld f

dieser text ist kursiv

asdfasdfasdfasdlkvalrkgjval asdkfj sldkfjlsdjfa adaher is kes ji lkaskdj
ladskj a ldksfjll aldkfj lkj afsdlfkjl alsdkf jaldskfj la sdflaldsflas df sadfl sf

das hier ist monotype

Kapitel 1

Überblick

1.1 Arten von Virtualisierungen

1.1.1 Einordnung Docker

1.2 Einführung in Docker

Kapitel 2

Ziel der Arbeit/Forschungsfrage

Kapitel 3

Security aus Linux Kernel-Features

3.1 Isolierung

3.1.1 namespaces

3.1.1.1 user namespaces

3.1.2 capabilities

3.1.2.1 Beispiele, /proc-Verzeichnis, (Un-)Mounten des Host-Filesystems

3.1.3 Mandatory Access Control (MAC)

3.1.3.1 Beispiel SELinux

3.2 Ressourcenverwaltung

3.2.1 cgroups

3.3 Docker im Vergleich zu anderen Containerlösungen

Kapitel 4

Security im Docker-Ökosystem

4.1 Docker Images und Repositories

4.1.1 neues Signierungs-Feature

4.2 Docker Daemon

4.2.1 REST-API

4.2.2 Support von Zertifikaten

4.3 Docker Cache

4.4 privileged Container

4.5 Networking

4.5.1 bridge Netzwerk

4.5.2 overlay Netzwerk

4.5.3 DNS

4.5.4 Portmapping

4.6 Daten-Container

4.7 Docker mit VMs

4.8 Tools rund um Docker

4.8.1 Docker Swarm

4.8.2 Docker Compose

4.8.3 Nautilus Project

4.8.4 Vagrant

4.8.5 Kubernetes

Kapitel 5

Docker in Unternehmen/Cloud- Infrastrukturen

Kapitel 6

Fazit/Ausblick

Literaturverzeichnis