H. Langweg, M. Meier, B.C. Witt, D. Reinhardt et al. (Hrsg.): Sicherheit 2018,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2018 221

Informationssicherheitskonzept nach IT-Grundschutz für Containervirtualisierung in der Cloud

Erik Buchmann[1] Andreas Hartmann[2] Stephanie Bauer[3]

Abstract:

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit dem IT-Grundschutz eine sichere und wirksame Schutzvorkehrung vor den stetig steigenden Bedrohungen im Kontext der Digitalisierung zur Verfügung. Zwar sind die behandelten BSI-Bausteine herstellerneutral definiert. Gleichwohl beziehen sich die Bausteine auf die sich ändernden Technologien, was eine entsprechende Anpassung erforderlich macht. Mit dem Hintergrund von Cloud basierten IT-Infrastrukturen findet aktuell ein massiver Wandel hinsichtlich eingesetzter Servertechnologien und –dienste hin zu Containervirtualisierung in der Cloud statt. Unternehmen, die ihre IT-Landschaften diesbezüglich transformieren, müssen darum mehr denn je die Sicherheit ihrer Daten gewährleisten. Wir zeigen am Beispiel von Docker Containern, wie der IT-Grundschutz auf diese neuen Herausforderungen anzupassen ist. Wir gehen dabei insbesondere auf die Gefährdungsanalyse, Docker-spezifische Gefährdungen sowie entsprechende Maßnahmen ein.

Keywords: IT-Grundschutz; Digitalisierung; IT-Sicherheit; Docker Container; Cloud Technologien

1 Einleitung

Die Containervirtualisierung, z.B. mit dem Open-Source Projekt Docker [Do17], ermöglicht es durch die Bereitstellung von Containern, innovative und cloudbasierte Anwendungen auf eine agile, kosteneffiziente Weise umzusetzen und bereitzustellen. Um dabei Tempo- und Innovationsvorteile zu realisieren müssen Unternehmen ihre traditionelle IT-Infrastruktur anpassen [Gö17]. Dies ist zwingend mit einer Anpassung des IT-Sicherheitskonzepts verbunden. Wenn das Sicherheitskonzept eines Unternehmens auf dem IT-Grundschutz [Bu11] des Bundesamts für Sicherheit in der Informationstechnik (BSI) beruht oder im Rahmen einer ISO 27001 Zertifizierung auf dem IT-Grundschutz aufgebaut [Bu14] wurde, ist dies schwierig: Ein Baustein für die Containervirtualisierung mittels Docker oder alternativer Produkte existiert derzeit nicht. Allerdings gibt es Grundlagen, z.B. einen Baustein B 3.304 für den sicheren Betrieb von Virtualisierungsservern oder einen Katalog von allgemeingültigen Elementargefährdungen.

In dieser Arbeit untersuchen wir, inwiefern der bestehende IT-Grundschutz nach BSI auf die Containervirtualsierung mit Docker angewendet werden kann, um die Virtualisierungsinfrastruktur vom physischen Server bis zu den Containern abzusichern. Unser wesentlicher

[1] Hochschule für Telekommunikation Leipzig, Deutschland, buchmann@hft-leipzig.de
[2] Hochschule für Telekommunikation Leipzig, Deutschland, hartmann@hft-leipzig.de
[3] T-Systems International GmbH, Nürnberg, Deutschland, stephanie.bauer@telekom.de

doi:10.18420/sicherheit2018_18

Beitrag ist eine Gefährdungsanalyse für alle Komponenten des Docker-Ökosystems, die mit den Bausteinen des BSI nicht ausreichend abgesichert werden. Das heißt, wir beschreiben Docker-spezifische Gefährdungen und entsprechende Maßnahmen zum Umgang mit diesen Gefährdungen, die über die BSI Grundschutz-Kataloge hinausgehen. Zuletzt diskutieren wir, ob diese Aspekten in einen benutzerdefinierten Baustein [Bu17a] für die Containervirtualisierung integriert werden sollten.

Unsere Untersuchung erfolgt für eine On-Premise-Lösung, bei der der Nutzer Eigentümer der Infrastruktur und der Container-Plattform ist. Übergreifende Aspekte, die sich auf die komplette Organisation auswirken, sowie sicherheitstechnische Aspekte bzgl. der Infrastruktur und der Netze werden zentral gesteuert. Wir gehen davon aus, dass dafür bereits ein Sicherheitskonzept nach IT-Grundschutz vorliegt. In unserem Fokus liegt daher die Schicht 3 *IT-Systeme* des Grundschutzes, auf der das Docker-Ökosystem angesiedelt ist. Unsere vollständige Untersuchung kann unter [Ba17] abgerufen werden.

Aufbau der Arbeit: Abschnitt 2 beschreibt die Grundlagen dieser Arbeit. In Abschnitt 3 führen wir eine Risikoanalyse für Docker nach IT-Grundschutz durch und beschreiben spezifische Gefährdungen und Maßnahmen. Die Arbeit schließt mit einem Fazit in Abschnitt 4.

2 Grundlagen

In diesem Abschnitt stellen wir Docker Container [PR15] sowie die Vorgehensweise des IT-Grundschutzes nach BSI kurz vor.

2.1 Docker Container

Die Containervirtualisierung auf der Betriebssystemebene eines Linux-Systems kapselt Applikationen in Containern. Dies ermöglicht es, Systemressourcen wie Prozessor, Netzwerk oder Speicher zu verwalten, Applikationen über Systeme hinweg zu verschieben oder voneinander isolierte Container parallel auf dem selben Host-System zu betreiben. Dabei setzen die Container auf Funktionen des Linux-Kernels auf. Abbildung 1 zeigt einen typischen Docker-Aufbau.

Die Docker Architektur [Do17] besteht aus Docker Client, Docker Daemon, Docker Registry und den Docker Objekten (Images, Docker Files, Container). Der **Docker Client** nimmt Anweisungen des Anwenders entgegen. Der **Docker Daemon** stellt Systemfunktionen zum Erstellen, Betreiben und Verteilen von Containern zur Verfügung. Diese beiden Bestandteile bilden zusammen die Docker Engine. Die Docker-Engine nutzen drei voneinander isolierte Container. Ein Container besteht aus zwei Hauptverzeichnissen: `/bin` enthält die Binärdateien und `/lib` die dynamischen Bibliotheken und Kernel-Module, die für die Funktionalität eines Containers benötigt werden.

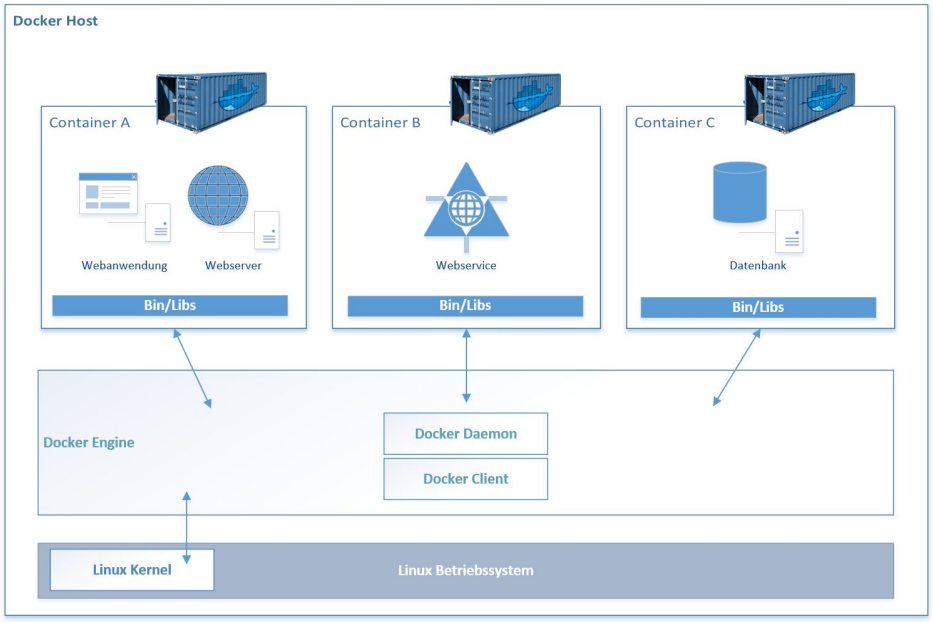

Abb. 1: Docker-Verbund

Client und Daemon können auf dem gleichen Host-System laufen oder der Client wird mit einem remote Daemon verbunden. Die Kommunikation findet über eine REST API, ein UNIX Socket oder eine andere Netzwerkschnittstelle statt. Wenn die Installation auf unterschiedlichen Systemen erfolgt, muss die Konfiguration bzgl. der jeweiligen Netzwerkinformationen manuell vorgenommen werden. Die **Docker Registry** verwaltet und speichert die Images. Docker Hub und Docker Cloud sind bspw. öffentlich zugängliche Registries. Docker ist in seinen Grundeinstellungen so konfiguriert, dass nach Images aus dem Docker Hub gesucht wird. Es besteht aber auch die Möglichkeit, eine private Registry für seine Images anzulegen, z.B. über die Docker Trusted Registry.

Docker **Images** sind schreibgeschützte Templates für die Erstellung eines Containers, d.h, ein **Container** ist die ausführbare Instanz eines Images. Ein Docker-Image besteht aus Layern: Einem Base Image mit einem Debian-Betriebssystem sowie mehreren Layern, die z.B. einem Apache Web-Server oder Anwendungen enthalten. Die Layer werden dabei mittels Union Mount über das Base Image „darübergelegt“. Das Advanced Unification Filesystem stellt dafür eine Copy-On-Write Funktion zur Verfügung. Diese Unterscheidung ist für das Sicherheitskonzept wichtig, da das Base Image oft aus öffentlichen Quellen stammt, während die übergeordneten Layer anwendungsspezifisch erstellt werden.

2.2 IT-Grundschutz nach BSI

Das BSI hat mit dem IT-Grundschutz ein erprobtes Verfahren zur Herstellung eines ausgewogenen Sicherheitsniveaus entwickelt, das aus vier Standards besteht und den Weg in eine ISO 27001-Zertifizierung ebnet:

- BSI-Standard 200-1: Management-Systeme für Informationssicherheit
- BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise
- BSI-Standard 200-3: Risikomanagement
- BSI Standard 100-4: Notfallmanagement

Vor der Modernisierung des IT-Grundschutzes im November 2017 verwiesen die BSI-Standards auf die IT-Grundschutz-Kataloge [Bu16], welche Standard-Sicherheitsmaßnahmen für typische Geschäftsprozesse, Anwendungen und IT-Systeme enthalten. In den aktuellen Standards wird stattdessen auf das IT-Grundschutz-Kompendium [Bu17b] verwiesen, das zwischen Basis-, Standard- und erhöhten Anforderungen an die IT-Sicherheit differenziert und ein flexibleres Risikomanagement inklusive nutzerdefinierter Schutzprofile und Bausteine unterstützt.

Unsere Arbeit basiert noch auf den BSI-Standards 100-1 bis 100-3 und der Ergänzung zum BSI-Standard 100-3 sowie den IT-Grundschutzkatalogen Stand 15. Ergänzungslieferung [Bu08a, Bu08b, Bu08c, Bu16]. Eine Übertragung unserer Erkenntnisse auf die Aktualisierung des IT-Grundschutzes ist jedoch gegeben: Zwar haben sich durch die neue Untergliederung des Bausteinkatalogs die Namen der von uns verwendeten Bausteine geändert. Sie sind jedoch hinreichend unverändert Bestandteil des IT-Grundschutz-Kompendiums (vgl. Baustein „B 3.304 Virtualisierung“ und „SYS.1.5 Virtualisierung“). Darüber hinaus haben wir keine Restrisiken als „akzeptabel“ bewertet – der neue Standard 200-3 legt sieht die Akzeptanz von Risiken eine andere Vorgehensweise vor als 100-3.

3 IT-Grundschutz für Docker-Container

Der IT-Grundschutz erfordert eine Definition des Informationsverbundes, damit der Geltungsbereich des Sicherheitskonzepts festgelegt werden kann. Wir beschränken uns hier auf das Docker-Ökosystem innerhalb der Schicht *IT-Systeme*. Wir legen dafür einen typischen Docker-Aufbau zugrunde, wie er in Abbildung 1 dargestellt ist. In Container A läuft eine Webanwendung auf einem Webserver. In Container B läuft ein Webservice, beispielsweise die Zahlungsmethode in einem E-Shop. In Container C wird eine Datenbank betrieben, die wiederum Logindaten beinhaltet. Diese drei Container werden isoliert voneinander betrieben, aber müssen miteinander kommunizieren. Wir haben den Informationsverbund in Anhang A zusammengefasst. Details finden sich in [Ba17].

Aus dem Informationsverbund lässt sich ableiten, dass die existierenden BSI-Bausteine die IT-Anwendungen und die eingesetzte Server-Software bereits ausreichend absichern (s. Anhang B und C). Unsere zentrale Erkenntnis ist, dass für die Server-Systeme, auf denen Docker

abläuft, ein hoher Schutzbedarf besteht. Wir führen daher im Folgenden eine Risikoanalyse nach IT-Grundschutz für diese Systeme durch. Am Ende dieses Abschnitts diskutieren wir, inwiefern sich unsere Erkenntnisse von Docker auf die Containervirtualisierung im Allgemeinen und auf andere Anwendungsszenarien übertragen lassen.

3.1 Risikoanalyse für Server-Systeme mit Docker-Containern

Für die Docker Host-Komponente sind 9 Elementargefährdungen relevant:

- G 0.15 Abhören
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung von Informationen
- G 0.21 Manipulation von Hard-oder Software
- G 0.23 Unbefugtes Eindringen
- G 0.27 Ressourcenmangel
- G 0.32 Rechtemissbrauch
- G 0.40 Verhinderung von Diensten
- G 0.46 Integritätsverlust

Nachfolgend wird für jede Gefährdung eine Maßnahme aus dem Maßnahmen-Katalog festgelegt und bewertet. Wenn alle Bewertungskriterien mit „J“ gekennzeichnet werden, ist die Maßnahme ausreichend und eine Risikobehandlung kann entfallen. Anderenfalls wird die spezielle Gefährdungslage genauer untersucht und ergänzende Sicherheitsmaßnahmen vorgeschlagen. Ausführliche Begründungen für die Bewertungen können in [Ba17] eingesehen werden.

3.1.1 G 0.15 Abhören

Maßnahme	M 5.177 Serverseitige Verwendung von SSL/TLS	
Bewertung	Vollständigkeit vorhanden: J Mechanismenstärke ausreichend: J	Zuverlässigkeit gegeben: J Ausreichender Schutz: J
Begründung der Bewertung	Da die Datenobjekte D1 Personendaten, D2 Nutzdaten und D3 Accountdaten einen hohen Schutzbedarf bzgl. Vertraulichkeit aufweisen, muss sichergestellt werden, dass diese Datenobjekte über die Kommunikationsverbindung Kom2 nicht abgehört werden können. Dies wird durch serverseitiges SSL/TLS erreicht.	

3.1.2 G 0.18 Fehlplanung oder fehlende Anpassung

Maßnahme	M 2.38 Aufteilung der Administrationstätigkeiten M 2.446 Aufteilung der Administration bei Virtualisierungsserven

Bewertung	Vollständigkeit vorhanden: N Mechanismenstärke ausreichend: J	Zuverlässigkeit gegeben: J Ausreichender Schutz: N
Begründung der Bewertung	Die Administration virtueller IT-Systeme geht über die in M 2.38 und M 2.446 beschriebenen Rollen hinaus.	

Spezifische Gefährdungen / Maßnahmen: Ein Gefährdungsszenario ist der *Container Breakout*, der einem Angreifer Zugriff auf das Host-System oder auf weitere Container im gleichen System erlaubt, und zwar mit den Privilegien[4] des Containers, aus dem der Ausbruch erfolgte.

- **Definition der Systembenutzer** Docker-Container sind grundsätzlich nicht als privilegierte Container zu betreiben, damit Angreifer im Erfolgsfall nur unprivilegierten Zugriff auf andere Ressourcen erhalten.
- **Rechtemanagement** Es sind die Berechtigungen für die definierten Benutzergruppen auf Minimalität zu prüfen.
- **Rollenaufteilung** Wenn in der Maßnahme M 2.38 eine Rollenaufteilung der Administratoren festgelegt wird, ist zu prüfen, ob auch für virtuelle IT-Systeme eine Aufteilung notwendig ist.
- **Weitere Linux Funktionen** Schutzmaßnahmen wie apparmor, selinux, seccomp, filter und namespaces, die auf dem Host-System installiert werden, können das Risiko eines Ausbruchs aus einem Gastcontainer reduzieren.

3.1.3 G 0.19 Offenlegung schützenswerter Informationen

Maßnahme	M 5.177 Serverseitige Verwendung von SSL/TLS	
Bewertung	Vollständigkeit vorhanden: J Mechanismenstärke ausreichend: J	Zuverlässigkeit gegeben: J Ausreichender Schutz: J
Begründung der Bewertung	Für hoch vertrauliche Daten (D1 Personendaten, D2 Nutzdaten, D3 Accountdaten), besteht die Gefahr einer Offenlegung durch technisches Versagen oder vorsätzliche Handlungen. Eine Absicherung durch SSL/TLS reduziert dieses Sicherheitsrisiko.	

Hinweis: Da unsere Risikoanalyse auf Docker-Container ausgerichtet ist, betrifft die Einschätzung der Maßnahme „Serverseitige Verwendung von SSL/TLS“ nur die Kommunikation der Docker-Container untereinander. Für eine Kommunikation nach außen ist unter Umständen eine separate Risikoanalsye erforderlich, ebenso für externe Aspekte wie beispielsweise ein ausgelagertes Speicher-Subsystem.

[4] Das Docker-Team arbeitet daran, den root-Benutzer in einem Container automatisch auf einen Nicht-Root-Benutzer im Host-System abzubilden (Reduzierung der Auswirkungen eines Ausbruchs).

3.1.4 G 0.21 Manipulation von Hard-oder Software

Maßnahme	M 2.448 Überwachung virtueller Infrastrukturen	
Bewertung	Vollständigkeit vorhanden: N Mechanismenstärke ausreichend: J	Zuverlässigkeit gegeben: J Ausreichender Schutz: N
Begründung der Bewertung	Durch zentrale Speicherung von Images im dem Docker Hub ergeben sich Angriffspunkte für die Manipulation von Software, die es bei bisheriger Virtualisierungstechnologie nicht gab.	

Spezifische Gefährdungen / Maßnahmen: Eine besondere Gefährdung durch Manipulation für Docker bei Container ist der Einsatz von *vergifteten Images*, d.h., Images aus öffentlicher Quelle, die einen Schadcode enthalten.

- **Docker Content Trust** Dies ist ein Feature von Docker, durch das Signieren mit dem öffentlichen Schlüssel des Entwicklers die Integrität der Images zu sichern und Image-Erzeuger zu schützen.
- **Docker Trusted Registry** Die Docker Trusted Registry bietet die Möglichkeit, die Images unter Verzicht einer öffentlich zugänglichen Registry on-premises oder in einer virtuellen private Cloud zu speichern und zu verwalten.

3.1.5 G 0.23 Unbefugtes Eindringen in IT-Systeme

Maßnahme	M 2.448 Überwachung virtueller Infrastrukturen M 4.346 Sichere Konfiguration virtueller IT-Systeme M 5.154 Sichere Konfiguration eines Netzes für virtuelle Infrastruktur	
Bewertung	Vollständigkeit vorhanden: N Mechanismenstärke ausreichend: J	Zuverlässigkeit gegeben: J Ausreichender Schutz: N
Begründung der Bewertung	Veränderungen an den Binärdateien wirken sich bei der Betriebssystemvirtualisierung auf alle Container aus und nicht nur auf den Virtualisierungsserver selbst.	

Spezifische Gefährdungen / Maßnahmen: Durch *unautorisierte Änderungen an Konfigurationsdateien* der virtuellen Infrastruktur können erhebliche und tiefgreifende Schäden entstehen, ebenso wie durch vorsätzliche oder versehentliche Fehlkonfigurationen der Netzzuordnung. Hier stellt insbesondere der *Docker Daemon* eine Angriffsoberfläche dar, da dieser root-Rechte besitzt und die Funktionsfähigkeit aller Container beeinflussen kann. Für Vertraulichkeit, Integrität oder Verfügbarkeit der Daten ist die *Integrität von Konfigurationsdaten* ausschlaggebend.

Für den Schutz des Docker Daemons sind mehrere aufeinander abgestimmte Maßnahmen erforderlich, die das Rollen- und Rechtemanagement betreffen, die Manipulation von Hard- oder Software sowie den Missbrauch von Berechtigungen berücksichtigen, sowie die Konfiguration des Host-Systems und des virtuellen Netzwerks absichern.

- **Prüfsummen** Die Prüfung auf unautorisierte Änderungen der Konfigurationsdateien kann beispielsweise mittels Werkzeugen wie OS-SEC erfolgen.
- **Docker Bench for Security** Docker selbst bietet das Docker Bench for Security Script [Ce17] an, welches die eigene Docker Konfiguration prüft. Voraussetzung ist eine Dockerversion 1.10.0 oder aktueller.
- **Konfiguration der Netzfunktionen** Da Docker Container auf einem gängigen Linux-System betrieben werden, kann man auf bekannte Werkzeuge wie beispielsweise Puppet [Je17] zurückgreifen, um die Netzkomponenten zentral zu überwachen.
- **Benennung virtueller Netze** Wenn Netzverbindungen auf verschiedenen Host-Systemen gleich benannt sind, kann ein Container versehentlich mit dem falschen Netzwerk verbunden werden. Eine eindeutige und aussagekräftige Benennung der Netze sollte anhand der Funktion des Netzwerkes vorgenommen werden [Je17].
- **Storage Zentralisierung** Im Sicherheitskonzept muss festgelegt werden, ob Daten nach Beenden des Containers gelöscht werden oder ob ein Dateiverzeichnis des Containers auf ein Dateiverzeichnis des Host-Systems verknüpft wird. Das Host-System muss dann für eine Abgrenzung zwischen den Daten des Betriebssystemkerns, der Systembibliotheken und der gemeinsam genutzten Anwendungen sichergestellen.
- **Monitoring** Das Monitoring lässt sich durch den Einsatz eines Linux-Servers mit den systemeigenen Monitoring-Systemen wie Nagios bewerkstelligen [Je17].
- **Kommunikation zwischen Containern** Wird das Container Linking aktiviert, so müssen Container, die nicht miteinander kommunizieren dürfen, durch Firewalls oder physikalische Trennung voneinander isoliert werden. Maßnahme M 5.154 Sichere Konfiguration eines Netzes für virtuelle Infrastruktur bietet hierzu eine Grundlage.

3.1.6 G 0.27 Ressourcenmangel

Maßnahme	M 4.349 Sicherer Betrieb von virtuellen Infrastrukturen	
Bewertung	Vollständigkeit vorhanden: J Mechanismenstärke ausreichend: J	Zuverlässigkeit gegeben: J Ausreichender Schutz: J
Begründung der Bewertung	Bei dem Betrieb von einem Container Host-System sind die gleichen Dinge zu beachten wie bei einem Linux-Server. Dadurch greifen die üblichen Schutzmaßnahmen für den Zugriff auf einen Linux-Server.	

3.1.7 G 0.32 Missbrauch von Berechtigungen

Maßnahme	M 2.318 Sichere Installation eines IT-Systems M 2.444 Einsatzplanung für virtuelle IT-Systeme M 2.447 Sicherer Einsatz virtueller IT-Systeme M 3.72 Grundbegriffe der Virtualisierungstechnik	
Bewertung	Vollständigkeit vorhanden: J Mechanismenstärke ausreichend: N	Zuverlässigkeit gegeben: J Ausreichender Schutz: N
Begründung der Bewertung	Eine bedeutende Gefährdung für Container ist der Missbrauch von Rechten, insbesondere wenn Angreifer root-Rechte erlangen.	

Spezifische Gefährdungen / Maßnahmen: Da Container auf Kernel-Funktionen des Host-Systems zugreifen, können Angreifer mit *unrechtmäßig erworbenen* Berechtigungen großen Schaden anrichten. Gleiches gilt für den *Mißbrauch* von rechtmäßige Berechtigungen.

Neben den bereits unter G 0.18 Fehlplanung oder fehlende Anpassung aufgeführten Maßnahmen sollten folgende Hinweise beachtet werden:

- **Isolierung und Kapselung** Ein Schutz gegen den Missbrauch von Berechtigungen wird durch Isolierung und Kapselung von virtuellen IT-Systemen realisiert, beispielsweise mittels namespaces und cgroups.
- **Schulung der Administratoren** Da die Container-Technologie einer dynamischen Entwicklung unterliegt, kommt einer regelmäßigen Schulung große Bedeutung zu.

3.1.8 G 0.40 Verhinderung von Diensten (DoS)

Maßnahme	M 4.405 Verhinderung von DoS bei Webanwend. und -Services M 4.97 Ein Dienst pro Server	
Bewertung	Vollständigkeit vorhanden: N Mechanismenstärke ausreichend: J	Zuverlässigkeit gegeben: J Ausreichender Schutz: N
Begründung der Bewertung	Da sich mehrere Container die Ressourcen eines Systems teilen können, erhöht sich das Risiko durch einen Denial-of-Service-Angriff.	

Spezifische Gefährdungen / Maßnahmen: Bei der Containervirtualisierung kann es neben klassischen *Denial-of-Service-Angriffen* auch zu einer *Überbuchung von Ressourcen* kommen, wenn die einzelnen Container durch Manipulation oder Fehlkonfiguration in Summe mehr Ressourcen zugewiesen bekommen, als physisch auf dem Host-System vorhanden sind.

- **Capabilities** Um eine Überbuchung zu verhindern, kann durch Linux-capabilities (limits, cgroups) der Zugriff der Containern auf CPU, Arbeitsspeicher, etc. limitiert werden.
- **Ein Dienst pro Server** Um die Auswirkungen eines Angriffs zu minimieren, sollte Maßnahme M 4.97 *Ein Dienst pro Server* in Betracht gezogen werden.

3.1.9 G 0.46 Integritätsverlust schützenswerter Information

Maßnahme	M 5.177 Serverseitige Verwendung von SSL/TLS	
Bewertung	Vollständigkeit vorhanden: J Mechanismenstärke ausreichend: J	Zuverlässigkeit gegeben: J Ausreichender Schutz: J
Begründung der Bewertung	Durch Manipulationen, Fehlverhalten, Fehlfunktionen etc. kann die Datenintegrität beeinträchtigt werden. SSL/TLS unterbindet dies.	

3.2 Diskussion

Erkenntnisse aus der Risikoanalyse: Der Aufbau des *IT-Verbunds* ergibt sich wesentlich aus dem Docker-Ökosystem, d.h., hier bestehen keine wesentlichen Änderungsmöglichkeiten. Beispielsweise ändern sich unsere Aussagen nicht, wenn der IT-Verbund statt in zwei in drei Rechenzentren parallel betrieben wird.

Mit den Datenobjekten D1 Personendaten, D2 Nutzdaten, D3 Accountdaten und D4 Konfigurationsdaten hat der IT-Verbund jeweils mindestens ein Datenobjekt, das einen hohen Schutzbedarf bzgl. Vertraulichkeit, Integrität und Verfügbarkeit aufweist. Da sich stets der höchste Schutzbedarf der Datenobjekte auf die Anwendungen und Systeme im IT-Verbund vererbt, hat die konkrete Wahl der Anwendung keinen Einfluss auf das Sicherheitskonzept, von Extremfällen (z.B. nicht-geschäftskritische Testplattformen ohne Außenverbindung oder das interne Logging von Prozessdaten ohne Personenbezug und Vertraulichkeitsanforderungen) abgesehen.

IT-Grundschutz für Containervirtualisierung: Neben den Maßnahmen, die sich aus dem Schutzbedarf der genannten Datenobjekte ableiten lassen, haben wir Maßnahmen identifiziert, die sich auf das Docker-Ökosystem beziehen. Diese Maßnahmen sind nicht Bestandteil der existierenden BSI-Bausteine. Sie sind jedoch für ein Sicherheitskonzept für die Containervirtualisierung unverzichtbar.

Zwar lassen sich aus dem Virtualisierungsbaustein B 3.304 einige Maßnahmen ableiten. Das BSI macht aber in der überarbeiteten Fassung SYS.1.5 dieses Bausteins im Grundschutz-Kompendium deutlich, dass dieser Baustein nicht für Docker-Container zu verwenden ist. Daher stellt sich die Frage, ob dafür ein benutzerdefinierter Baustein (s. [Bu17a]) durch die Nutzer der Containervirtualisierung erstellt werden sollte.

Die Containervirtualisierung ist eine junge Technologie, die noch stetig weiterentwickelt wird. Ein benutzerdefinierter Baustein hätte den Vorteil, dass dieser sehr rasch und unmittelbar durch die Domänenexperten erstellt werden könnte. Auf der anderen Seite wird die Containervirtualisierung in sehr heterogenen Umgebungen eingesetzt. Daher steht zu befürchten, dass Aufbau, Abstimmung und Pflege eines benutzerdefinierten Bausteins zu einem erheblichen und repetitivem Koordinationsaufwand unter den Anwendern führen würde, sodass Erweiterungen oder Korrekturen nur mit großem Zeitverzug umgesetzt werden könnten. Aus unserer Sicht ist daher die zentrale Aufnahme und Pflege eines generischen Bausteins „Containervirtualisierung“ durch das BSI die bessere Alternative.

4 Zusammenfassung

Das Ziel dieser Arbeit bestand in der Entwicklung eines IT-Sicherheitskonzepts nach BSI IT-Grundschutz für Docker Container auf einem physikalischen Host-System in einer On-Premise Umgebung, sowie in der Verallgemeinerung dieser Erkenntnisse. Wir können feststellen, dass die BSI Grundschutz-Kataloge eine wertvolle Hilfestellung bei der Erstellung eines Sicherheitskonzepts für Docker bieten, insbesondere wenn es sich um Maßnahmen handelt, die auf Grund des Schutzbedarfs der Datenobjekte umzusetzen sind.

Maßnahmen, die sich auf das Docker Ökosystem beziehen, sind jedoch entweder selbst zu erarbeiten oder aus Virtualisierungsbaustein B 3.304 abzuleiten, der dafür jedoch nicht gedacht ist. Daher würde sich die Erstellung eines generischen Virtualisierungsbausteins durch das BSI anbieten. In der Zwischenzeit ließe sich ein Sicherheitskonzept für die Containervirtualisierung auch mittels eines benutzerdefinierten Bausteins umsetzen.

Literaturverzeichnis

[Ba17] Bauer, Stephanie: Erarbeitung eines Informationssicherheitskonzepts nach IT-Grundschutz für Docker Container. Bachelor-Arbeit, Hochschule für Telekommunikation Leipzig, Kopie s. http://www.webcitation.org/6xAkE4g1l, 2017.

[Bu08a] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-1, Managementsysteme für Informationssicherheit (ISMS). https://www.bsi.bund.de, 2008.

[Bu08b] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-2, IT-Grundschutz-Vorgehnsweise. https://www.bsi.bund.de, 2008.

[Bu08c] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz. https://www.bsi.bund.de, 2008.

[Bu11] Bundesamt für Sicherheit in der Informationstechnik: Webkurs IT-Grundschutz, IT -Grundschutz im Selbststudium. https://www.bsi.bund.de, 2011.

[Bu14] Bundesamt für Sicherheit in der Informationstechnik: Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz. https://www.bsi.bund.de, 2014.

[Bu16] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, 15.Ergänzungslieferung - 2016. https://www.bsi.bund.de, 2016.

[Bu17a] Bundesamt für Sicherheit in der Informationstechnik: Autorenrichtlinie zur Erstellung eines benutzerdefinierten Bausteins. https://www.bsi.bund.de, 2017.

[Bu17b] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium 2018, 1. Edition. https://www.bsi.bund.de, 2017.

[Ce17] Center for Internet Security: Docker Community Edition Benchmark. https://www.cisecurity.org, 2017.

[Do17] Docker Inc.: Docker Overview. https://docs.docker.com/engine/docker-overview/, Kopie s. http://www.webcitation.org/6xE2rYUYa, 2017.

[Gö17] Göbel, Lars: Container-as-a-Service - Die Zukunft der Virtualisierung. Cloud Computing Insider, Kopie s. http://www.webcitation.org/6xE2RH90v, 2017.

[Je17] Jedecke, Daniel: IT-Grundschutz in LXC-Container verpackt - Gut separiert. ix - Magazin für professionelle Informationstechnik, 5:116–, 2017.

[PR15] Pethuru Raj, Jeeva S. Chelladhurai, Vinod Singh: Learning Docker. Packt Publishing, 2015.

A Informationsverbund und Strukturanalyse

Für die Schutzbedarfsfeststellung ist eine Erfassung der IT-Systeme, IT-Anwendungen und die Kommunikationsverbindungen erforderlich. Als kleinste Einheit werden die Daten im IT-Verbund erfasst (s. Tabelle 1).

Nr.	Datenobjekt	Anmerkung
D1	Personendaten	personenbezogene Daten gemäß § 3 Abs. 1 BDSG
D2	Nutzdaten	generische Fachdaten
D3	Accountdaten	Authentifizierung und Autorisierung
D4	Konfigurationsdaten	Konfigurationsdaten und Parameter inkl. DNS und NTP
D5	Protokolldaten	Technische Protokolldaten (Monitoring)

Tab. 1: Datenerfassung

In Tabelle 2 werden diese Daten den IT-Anwendungen im Informationsverbund zugeordnet. Mit Fokus auf Docker verzichten wir auf die eigenständige Erfassung des Betriebssystems.

Nr.	Beschreibung	verarbeitete Daten	Software
A1	Webanwendung	D1, D2, D3, D4, D5	Allgemeine Webanwendung z.B. PHP
A2	Webserver	D1, D2, D4, D5	Apache Webserver
A3	Webservice	D2, D3, D4, D5	REST-basierter Dienst
A4	Datenbank	D1, D2, D3, D4, D5	Allgemeine Datenbank z.B. MySQL

Tab. 2: Strukturanalyse IT-Anwendungen, Server-Software und Kommunikationsverbindung

Weiterhin bezeichnet „Server-Software“ die Software, die auf dem Host-System aufsetzt, und „Docker Software“ die Bestandteile der Docker Engine. S1 und S2 stehen für je einen RZ-Standort basierend auf einem x86 Linux-Server (aktiv) - hier ordnen wir D1, D2, D3, D4 und D5 zu. Die Docker-Software SSW1 verarbeitet Daten entsprechend D4 und D5 mit Bezug zu S1 und S2. Die Kritikalität der Kommunikationsverbindungen KOM1 (extern, D1, D2, D3, Internet:https) und KOM2 (intern, D1, D2, D3, D4, D5, S1-S2 bidirektional SSH) richtet sich nach (1) der Existenz einer Außenverbindung und (2) dem Schutzbedarf der zu übertragenden Datenobjekte. Die Schutzbedarfsfeststellung erfolgt gemäß BSI-Standard 100-2 anhand der verwendeten Datenobjekte, indem typische Schadensszenarien (Verstoß gegen Gesetze, Gesundheitsschäden, Beeinträchtigung der Aufgabenerfüllung, finanzielle Auswirkungen, etc.) zugrundegelegt werden.

B Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung erfolgt gemäß BSI-Standard 100-2 anhand der Datenobjekte (Tabelle 3), indem typische Schadensszenarien (Verstoß gegen Gesetze, Gesundheitsschäden, Beeinträchtigung der Aufgabenerfüllung, etc.) zugrundegelegt werden.

Komponente	Vertraulichkeit	Integrität	Verfügbarkeit
D1: Personendaten	hoch	normal	normal
D2: Nutzdaten	hoch	normal	hoch
D3: Accountdaten	hoch	normal	normal
D4: Konfigurationsdaten	normal	hoch	normal
D5: Protokolldaten	normal	normal	normal

Tab. 3: Ergebnisse der Schutzbedarfsfeststellung für Datenobjekte

Der Schutzbedarf für eine IT-Anwendung entspricht dem höchsten Schutzbedarf der von der Anwendung verarbeiteten Datenobjekte. Äquivalent werden die Schutzbedarfe für die Server-Software und Server-Systeme festgelegt.

C Ergänzende Sicherheitsanalyse

In der ergänzenden Sicherheitsanalyse wird zunächst ermittelt, ob die Schutzbedarfe der IT-Anwendungen mit den BSI-Standardbausteinen abgedeckt werden können (Tabelle 4).

Komponente	**Begründung für Gefährdungsübersicht und Risikoanalyse**
A1: Webanwendung	Durch den Baustein B 5.21 und die dazugehörigen Maßnahmen können alle bekannten Gefährdungen abgedeckt werden.
A2: Webserver	Durch den Baustein B 5.4 und die dazugehörigen Maßnahmen können alle bekannten Gefährdungen abgedeckt werden.
A3: Webservice	Durch den Baustein B 5.24 und die dazugehörigen Maßnahmen können alle bekannten Gefährdungen abgedeckt werden.
A4: Datenbank	Durch den Baustein B 5.7 und die dazugehörigen Maßnahmen können alle bekannten Gefährdungen abgedeckt werden.

Tab. 4: Ergänzende Sicherheitsanalyse für IT-Anwendungen

Für jede IT-Anwendung gibt es einen passenden Baustein, und keine der Anwendungen weist einen sehr hohen Schutzbedarf auf. Hier muss keine Risikoanalyse durchgeführt werden. Dasselbe gilt für die Server-Software SSW1:Docker Software (Baustein B 1.10 und die dazugehörigen Maßnahmen). Für die Server-Systeme S1 und S2 ist dagegen eine Risikoanalyse durchzuführen, da die Technologie der Container nicht vollständig durch bestehende BSI-Bausteine abgedeckt werden.