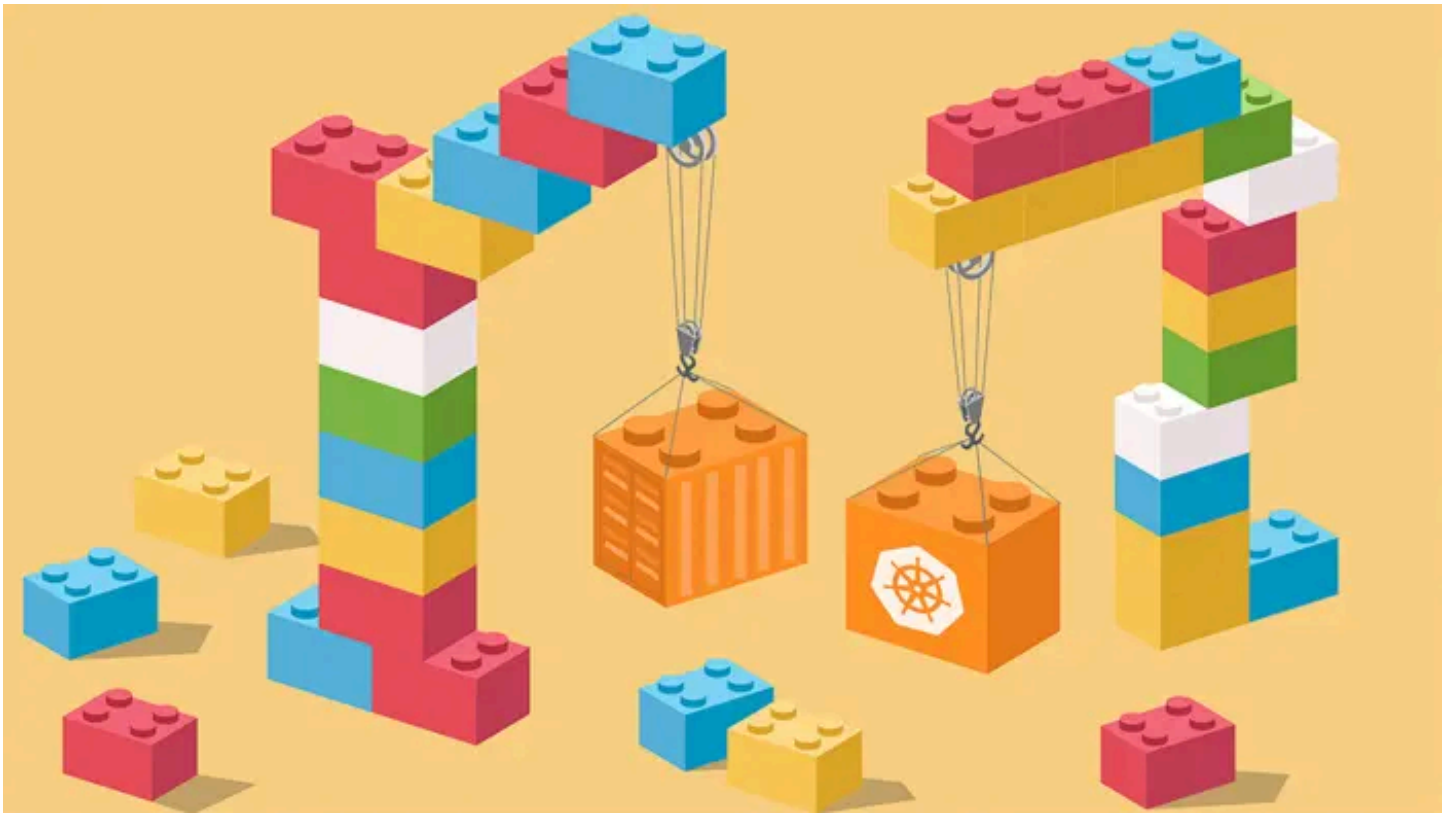
MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

# IT-Grundschutz: BSI-Anforderungen für Container und Kubernetes

28.09.2021 08:00 Uhr Christoph Puppe



**Die seit Langem erwarteten BSI-Grundschutz-Bausteine für den Betrieb von Containern werden endlich konkreter und stehen zur öffentlichen Kommentierung bereit.**

Das BSI reagiert auf die veränderten technischen Gegebenheiten und hat den Bereich zu Containern im IT-Grundschutz-Kompendium neu sortiert, da der bisherige Baustein hauptsächlich auf Linux-Container unter Kubernetes gemünzt war. Nach zwei Community Drafts mit Kommentierungsphasen erschien der bisherige Container-Baustein nun aufgeteilt erneut zur öffentlichen Kommentierung. Die beiden Entwürfe zu Containerisierung und Kubernetes sollen dann als neue IT-Grundschutz-Bausteine in die Edition 2022 des IT-Grundschutz-Kompendiums aufgenommen werden. Über die Entwicklung des Bausteins wurde in den Artikeln **"Container-Sicherheit: Entwurf des BSI-Bausteins für das Grundschutz-Kompendium" [1]** und **"IT-Sicherheit: Neuer Entwurf des BSI-Bausteins zu Containern" [2]** berichtet.

Wo früher der "SYS.1.6 Container" alle Anforderungen für die Container selbst, deren Betrieb und auch die Verwaltungssoftware enthielt, gibt es nun den "SYS.1.6 Containerisierung" für die Anforderungen an die Container und deren Runtimes und den "APP.4.4 Kubernetes" für das

Management des Containerbetriebs mit Kubernetes. Die Aufteilung war notwendig geworden, weil sich einerseits Kubernetes als dominierendes Betriebswerkzeug durchgesetzt hat und andererseits Container selbst nicht nur auf die Linux-Container unter Kubernetes beschränkt sind. Viele andere Betriebsarten, Containertechniken und Betriebssysteme sind für das Kompendium relevant und benötigten daher einen eigenständigen Baustein. Wer Kubernetes einsetzt, muss beide Bausteine beachten. Das BSI hat darauf geachtet, dass sie sich nicht überschneiden.

Inhaltlich blieben viele Bestandteile erhalten. In den 27 Anforderungen des neuen SYS.1.6 und den 21 Anforderungen des APP.4.4 finden sich nun aber auch Konkretisierungen, die Anwendern besser helfen, technische und organisatorische Maßnahmen zur Umsetzung zu definieren. Besonders das Thema Cluster unter Kubernetes hat durch die Aufteilung gewonnen. Fast alle erhöhten Anforderungen des APP.4.4 beziehen sich auf die Sicherheit der Nodes im Cluster. Auch das in vielen Organisationen heiß diskutierte Thema Separierung von Anwendungen ist nun klarer vorgegeben. Die Hoffnung ist, so die Umsetzung zu vereinfachen und die Sicherheit auf einem hohen Niveau zu halten, während gleichzeitig die Vorteile von Private- und Public-Cloud-Kubernetes-Clustern erhalten bleiben und deren Zahl überschaubar bleibt.

IX-TRACT

- Das BSI veröffentlicht für sein IT-Grundschutz-Kompendium zwei Bausteine zu Containern und Kubernetes zur öffentlichen Kommentierung.
- Die neuen Komponenten enthalten klare Anforderungen zu allen Themen des Containerbetriebs.
- Angesichts der derzeitigen Konsolidierung der Betriebstechnologien scheint der Veröffentlichungszeitpunkt günstig.

## Planung bleibt die Grundlage

Wie in jedem Baustein ist die Planung der Umgebungen von der Installation bis zur Außerbetriebnahme die Grundlage für den sicheren Betrieb. Hier enthalten beide Bausteine die üblichen Anforderungen an Dokumentation und Nachvollziehbarkeit der Planung. Allerdings wurde der durch die Aufteilung gewonnene Raum genutzt, auch Details der Planung in die Anforderungen aufzunehmen, die Anwendern mehr Planungssicherheit geben. So muss die Planung der Container die Verwaltung enthalten (SYS.1.6.A2) und auch die Bereitstellung und Verteilung von Images ist vorzubereiten (SYS.1.6.A4). Diese Planung wird für Kubernetes ergänzt um die Aspekte Planung der Separierung (APP.4.4.A1 und A4), der Automatisierung (APP.4.4.A2) und des Berechtigungsmanagements (APP.4.4.A3).

## Container- und Kubernetes-Baustein

Insgesamt ist die Separierung bei den Basis-, Standard- und erhöhten Anforderungen jetzt stärker vertreten. Wie im BSI-IT-Grundschutz-Kompendium üblich, müssen Verwaltungs- und Wirknetze gut getrennt sein (SYS.1.6.A5 und APP.4.4.A7 sowie erhöht APP.4.4.A18). Die Trennung der einzelnen Prozesse mit Namespaces ist für den SYS.1.6 bereits in der Einleitung erklärt und wird für Kubernetes

auf Pods erweitert (APP.4.4.A5). Bei einem erhöhten Schutzbedarf gibt es auch eine – risikobasiert zu wählende – Anforderung für die Separierung von Containern durch Hypervisoren oder eine physische Trennung auf separaten Nodes (SYS.1.6.A27). Ergänzend dazu enthält der Kubernetes-Baustein Anforderungen für das Separieren von Anwendungen auf der Ebene von Namespaces, Clustern und Nodes (APP.4.4.A1 und erhöht die A14 und A15).

Für Images gibt es weiterhin Sicherheitsvorgaben, aber nur noch im Container-Baustein (SYS.1.6.A6, A12, A13, A14 und erhöht die A21 sowie A23). Dieser enthält auch alle Anforderungen für den Betrieb der Container. So sind hier die Anforderungen für Anwendungen in Containern (SYS.1.6.A9 und A11), für das Limitieren der Ressourcen (SYS.1.6.A15), die Art des Fernzugriffs (SYS.1.6.A16), die Privilegien (SYS.1.6.A17), die verwendeten Accounts (SYS.1.6.A18) und auch die Datenspeicher (SYS.1.6.A9) enthalten. Daneben widmet sich der Baustein noch Forensikvorbereitungen (SYS.1.6.A22), Hochverfügbarkeit (SYS.1.6.A26), Angriffserkennung (SYS.1.6.A25) und Härtung des Hosts für diesen Betriebszweck (SYS.1.6.A24).

MEHR ZU UNTERNEHMENS-IT UND SECURITY

**Layer 8 – Der Faktor Mensch in Bezug auf Unternehmenssicherheit [3]**

**Sicherheits- und Incident-Management mit Wazuh[4]**

**BSI: Warnungen zur IT-Sicherheit ernstnehmen [5]**

**Auswirkungen des Ukrainekriegs auf die IT-Sicherheit in Deutschland [6]**

**Überblick zu IT-Versicherungsschutz für kleine Unternehmen und Freelancer [7]**

**Ransomware-Angriffsmuster und die wichtigsten Schritte zum Schutz dagegen [8]**

**Wie Ransomware-Angriffe heute ablaufen [9]**

**Security: So arbeiten Incident-Response-Teams nach einem Ransomeware-Angriff [10]**

**IT-Recht: Sicherheitsanforderungen und Rechtsfragen zu Ransomware-Attacken [11]**

**Sicherheitsrisiken in der IT: OWASP Top 10 in neuer Version [12]**

**OKR-Einführung: häufige Fehler und wie sie dennoch gelingt [13]**

**Unternehmens-IT: Wie sich Managed Services wandeln [14]**

**Endgerätesicherheit und EDR-Tools: Gefahren schnell erkennen und reagieren [15]**

**Cybercrime: Ransomware-Entwicklung führt zu neuen Bekämpfungsstrategien [16]**

**Identity and Access Management der Zukunft: digitales Business, Zero Trust, SASE [17]**

**IT-Sicherheit: Ransomware-Attacken verhindern durch Security Learning Center [18]**

**IT-Grundschutz: BSI-Anforderungen für Container und Kubernetes [19]**

**IT-Security: Trainings als Vorbereitung für Sicherheitsvorfälle im Unternehmen [20]**

**IT-Security: PetitPotam und andere Wege, die Kontrolle über das AD zu übernehmen [21]**

**Incident Response und Forensik: Angreifer durch Logs enttarnen [22]**

**Cloud-Sicherheit: Cloud Security Operations Center im Vergleich [23]**

Auf diesen Anforderungen basiert der Kubernetes-Baustein und fokussiert sich auf Betrieb, Verwaltung, Cluster und Nodes. Neben den Konfigurationsdateien der Verwaltungssoftware (APP.4.4.A8) sind hier besonders die Prozesse der Automatisierung (APP.4.4.A10), der notwendigen Clusterinfrastruktur (APP.4.4.A12) und der Datensicherung (APP.4.4.A5) zu nennen. Die Pods als Kollektion mehrerer Container in einem OS-Namespace sind eine Kubernetes-Spezialität, für die es die schon genannten Anforderungen zur Separierung (APP.4.4.A4), aber auch für die Initialisierung (APP.4.4.A6) gibt. Für den hohen Schutzbedarf – oder nach Risiko ausgewählt – gibt es für Pods Anforderungen für Hochverfügbarkeit (APP.4.4.A19), verschlüsselte Datenhaltung (APP.4.4.A20) und regelmäßigen Neustart (APP.4.4.A21). Kubernetes verwendet Service Accounts und APP.4.4.A9 regelt deren Nutzung.

## Kreuzreferenztabelle

**Kreuzreferenztabelle zum Baustein APP.4.4 Kubernetes**

| APP.4.4 | Name | CIA | G 0.14 | G 0.19 | G 0.20 | G 0.21 | G 0.23 | G 0.25 |
|---|---|---|---|---|---|---|---|---|
| **APP.4.4.A1** | Planung der Separierung der Anwendungen | | ✓ | ✓ | | | ✓ | |
| **APP.4.4.A2** | Planung der Automatisierung mit CI/CD | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **APP.4.4.A3** | Identitäts- und Berechtigungsmanagement bei Kubernetes | | ✓ | ✓ | | | ✓ | |
| **APP.4.4.A4** | Separierung von Pods | | ✓ | ✓ | | ✓ | ✓ | |
| **APP.4.4.A5** | Datensicherung im Cluster | | | | | | | |
| **APP.4.4.A6** | Initialisierung von Pods | | | | | | | ✓ |
| **APP.4.4.A7** | Separierung der Netze bei Kubernetes | | ✓ | ✓ | | ✓ | ✓ | |
| **APP.4.4.A8** | Absicherung von Konfigurationsdateien bei Kubernetes | | ✓ | ✓ | | ✓ | ✓ | |
| **APP.4.4.A09** | Nutzung von Kubernetes Service-Accounts | | ✓ | | | ✓ | | |
| **APP.4.4.A10** | Absicherung von Prozessen der Automatisierung | | ✓ | ✓ | | ✓ | ✓ | ✓ |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **APP.4.4.A11** | Überwachung der Container | | | | | | | ✓ |
| **APP.4.4.A12** | Absicherung der Infrastruktur-Anwendungen | | ✓ | ✓ | | ✓ | ✓ | |
| **APP.4.4.A13** | Automatisierte Auditierung der Konfiguration | CIA | ✓ | ✓ | | ✓ | ✓ | |
| **APP.4.4.A14** | Verwendung dedizierter Nodes | CIA | ✓ | ✓ | | | ✓ | |
| **APP.4.4.A15** | Trennung von Anwendungen auf Node- und Cluster-Ebene | CIA | ✓ | ✓ | | | ✓ | |
| **APP.4.4.A16** | Verwendung von Operatoren | CIA | | | | | | ✓ |
| **APP.4.4.A17** | Attestierung von Nodes | CIA | ✓ | ✓ | | | ✓ | |
| **APP.4.4.A18** | Verwendung von Mikro-Segmentierung | CI | ✓ | ✓ | | | ✓ | |
| **APP.4.4.A19** | Hochverfügbarkeit von Pods | A | | | | | | ✓ |
| **APP.4.4.A20** | Verschlüsselte Datenhaltung bei Pods | C | ✓ | ✓ | | | ✓ | |
| **APP.4.4.A21** | Regelmäßiger Neustart von Pods | CIA | ✓ | ✓ | | | ✓ | |

**Alle BSI-Bausteine sind risikoorientiert aufgebaut. Die Kreuztabelle zeigt, welche Anforderungen welche Gefährdungen abdecken.**

**Quelle: BSI**

**[24]**

## Fazit

Die Welt der Container hat sich in den letzten Jahren sehr schnell entwickelt. Wo früher mit Docker, Inc. noch ein Hersteller und seine Technik dominierte, gibt es im Jahr 2021 weitere sehr erfolgreiche Open-Source-Container-Runtimes. Und für die Orchestrierung hat sich mit Kubernetes ein Sieger herauskristallisiert. Diesen Trend hat das BSI intensiv verfolgt und die Entwicklung der Bausteine jeweils daran angepasst. Container als Betriebsoption unter Linux, Windows, AIX, Z/OS und anderen sind nun klar und verbindlich geregelt.

Und auch für Kubernetes als Technologie gibt es nun einen Baustein zur **Kommentierung [25]** als Public Draft, der für alle darauf aufsetzenden Produkte wie OpenShift, Rancher und die diversen Distributionen anwendbar ist. Der Zeitpunkt der Veröffentlichung scheint gut gewählt, da derzeit eine Konsolidierung der Basistechnologien stattfindet und die Bausteine hoffentlich für einen längeren Zeitraum ihre Relevanz behalten.

*Der Autor war an der Initiierung und Entwicklung der Bausteine beteiligt.*

*Christoph Puppe ist Managing IT Security Architect und Auditteamleiter für ISO 27001 nach Grundschutz bei SVA System Vertrieb Alexander GmbH, Mitautor des Grundschutz-Kompendiums und ehemaliger Penetrationstester.*

(**avr [26]**)

---

**URL dieses Artikels:**

`https://www.heise.de/-6200393`

## Links in diesem Artikel:

**[1]** https://www.heise.de/hintergrund/Container-Sicherheit-Entwurf-des-BSI-Bausteins-fuer-das-Grundschutz-Kompendium-4220176.html

**[2]** https://www.heise.de/hintergrund/IT-Sicherheit-Neuer-Entwurf-des-BSI-Bausteins-zu-Containern-4703039.html

**[3]** https://www.heise.de/hintergrund/Wie-Angreifer-dank-psychologischer-Tricks-in-Unternehmen-eindringen-7317970.html

**[4]** https://www.heise.de/tests/Sicherheits-und-Incident-Management-mit-Wazuh-7218423.html

**[5]** https://www.heise.de/hintergrund/BSI-Warnungen-zur-IT-Sicherheit-ernst-nehmen-7143015.html

**[6]** https://www.heise.de/hintergrund/Ukrainekrieg-Auswirkungen-auf-die-IT-Sicherheit-in-Deutschland-6668405.html

**[7]** https://www.heise.de/hintergrund/IT-Versicherungsschutz-fuer-kleine-Unternehmen-und-Freelancer-6489094.html

**[8]** https://www.heise.de/ratgeber/Security-Ransomware-Angriffsmuster-und-wie-man-sich-vor-ihnen-schuetzt-6457415.html

**[9]** https://www.heise.de/ratgeber/Security-So-laufen-Ransomware-Angriffe-heute-ab-6457906.html

**[10]** https://www.heise.de/ratgeber/Security-So-arbeiten-Incident-Response-Teams-nach-einem-Ransomeware-Angriff-6473782.html

**[11]** https://www.heise.de/hintergrund/IT-Recht-Sicherheitsanforderungen-und-Rechtsfragen-zu-Ransomware-Attacken-6474409.html

**[12]** https://www.heise.de/hintergrund/OWASP-Top-10-Sicherheitsrisiken-in-Web-Anwendungen-6332056.html

**[13]** https://www.heise.de/hintergrund/OKR-Einfuehrung-in-Firmen-Haeufige-Fehler-und-wie-es-dennoch-klappt-6291471.html

**[14]** https://www.heise.de/ratgeber/Unternehmens-IT-Wie-sich-Managed-Services-wandeln-6233929.html

**[15]** https://www.heise.de/ratgeber/Endgeraetesicherheit-und-EDR-Tools-Gefahren-schnell-erkennen-und-reagieren-6222034.html

**[16]** https://www.heise.de/hintergrund/Cybercrime-Ransomware-Entwicklung-fuehrt-zu-neuen-Bekaempfungsstrategien-6220960.html

**[17]** https://www.heise.de/hintergrund/Identity-and-Access-Management-der-Zukunft-Digitales-Business-Zero-Trust-SASE-6203741.html

**[18]** https://www.heise.de/hintergrund/IT-Sicherheit-Ransomware-Attacken-verhindern-durch-Security-Learning-Center-6204081.html

**[19]** https://www.heise.de/hintergrund/IT-Grundschutz-BSI-Anforderungen-fuer-Container-und-Kubernetes-6200393.html

**[20]** https://www.heise.de/hintergrund/IT-Security-Trainings-als-Vorbereitung-fuer-Sicherheitsvorfaelle-im-Unternehmen-6196247.html

**[21]** https://www.heise.de/ratgeber/IT-Security-PetitPotam-und-andere-Wege-die-Kontrolle-ueber-das-AD-zu-uebernehmen-6170976.html

**[22]** https://www.heise.de/hintergrund/Netzwerksicherheit-im-Active-Directory-So-enttarnen-Sie-Angreifer-durch-Logs-6141370.html

**[23]** https://www.heise.de/hintergrund/Cloud-Sicherheit-Cloud-Security-Operations-Center-im-Vergleich-6110834.html

**[24]** https://www.heise.de/ix/

**[25]** https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Drafts/it-grundschutz-drafts_node.html

**[26]** mailto:avr@ix.de