

IT-Grundschutzkompendium: BSI veröffentlicht Community Draft zu Containern

22.05.2018 10:16 Uhr Christoph Puppe, Dr. Jan Bundesmann



Auch vor der Bundesverwaltung macht die Containerisierung nicht halt. Deshalb erarbeitet das BSI einen Baustein für das IT-Grundschutzkompendium mit Vorgaben, die bei der Arbeit mit Containern einzuhalten sind.

Im Zuge der Modernisierung der Grundschutzkataloge, die seit August 2017 nun als Grundschutzkompendium erhältlich sind, hat das BSI am nun den Entwurf eines Bausteins für Container veröffentlicht. Die Umsetzungshinweise sind noch nicht einsehbar, aber die Rohfassung gibt einen Einblick, wie sich das BSI den Umgang mit Container in der Bundesverwaltung und in der Industrie vorstellt. Der Baustein ist als Community Draft zur Kommentierung freigegeben und in dieser Version keine verbindliche Vorgabe. Er ist für eine Zertifizierung nach ISO 27001 nach BSI Grundschutz noch nicht verbindlich, kann aber als Vorlage für einen eigenen Baustein dienen.

Container und / oder Sicherheit?

Container sind mittlerweile nicht nur in im Cloud-Stack Hosting zu finden, sondern sind dabei sich als eine Basis-Technik für das Hosting von Anwendungen im eigenen oder fremden Rechenzentrum

durchzusetzen. Eine Schwierigkeit ist dabei die Einschätzung, ob und wie Container die Sicherheit beeinflussen. Einerseits sind sie zur Separierung von Anwendungen geeignet, aber so wie auch *chroot* und *jails* früher, arbeiten alle Container auf dem gleichen Kernel. Besonders nach Rowhammer, Meltdown und Spectre, sowie allen Varianten dieser Angriffe ist die Unsicherheit hier hoch, wann und wie diese Separierung ausreichend ist.

Allerdings bieten Container Möglichkeiten zu Separierung, wie sie sonst nur SELinux oder AppArmor bieten. Syscalls, Ost-West-Datenverkehr und Ressourcenverbrauch lassen sich gut steuern und einschränken.

Diese Themen greift der Baustein auf und bietet Anhaltspunkte für Entscheidungen sowie konkrete Anforderungen für die Umsetzung von Sicherheitsmaßnahmen auf dem Container-Host und in den Images. Auch Pflege und Verwaltung der Images sind im Baustein enthalten. Spezifische Anforderungen an die Orchestrierung gehören nicht dazu.

Der **Entwurf [1]** wird sich sicherlich noch weiter entwickeln, auch werden die Umsetzungshinweise noch mehr Klarheit bringen, wie das BSI die Anforderungen auslegt und umgesetzt sehen möchte. iX wird über den Baustein in Ausgabe 7/18 ausführlicher berichten.

Hinweis in eigener Sache: Der Autor dieser Zeilen und des Artikels hat an diesem Entwurf mitgewirkt. (jab [2])

URL dieses Artikels:

<https://www.heise.de/-4053040>

Links in diesem Artikel:

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_Container.html

[2] <mailto:jab@ix.de>

Copyright © 2018 Heise Medien