Containerbetrieb in Rechenzentren der öffentlichen Hand

Die Einführung eines Containerbetriebes ist vordringlich eine organisatorische Aufgabe.

Zum Hintergrund: Mehr und mehr Applikationen werden auf eine Micro-Service Architektur umgestellt und Container-basiert entwickelt oder ausgeliefert. In der Industrie hat sich Kubernetes als Orchestration für den Containerbetrieb durchgesetzt und wird schrittweise auch in der IT der öffentlichen Hand eingeführt. Dies bringt große Chancen, aber auch große Risiken für die IT – „best practice" ist daher, daß man sich in einem strukturierten Prozeß der Risiken bewußt wird und von Anfang an Maßnahmen zur Risikovermeidung/-begrenzung plant und umsetzt (nach Dirk Broens, Deutsche Post DHL P&P).

Ein wesentlicher Unterschied von Micro-Service Applikationen zu traditionellen IT-Systemen ist eine deutlich höhere Release-Frequenz (z.T. täglich) und ein wesentlich flexiblerer Umgang mit sich verändernden Anforderungen; sehr oft kommen in der Software-Entwicklung agile Methoden zum Einsatz. Auch in der Orchestrations-Software für den Container-Betrieb sind regelmäßige Release-Wechsel eher die Norm als die Ausnahme.

Traditionelle IT-Abteilungen arbeiten meist entlang festgelegter (ITIL-)Prozesse und sind nicht darauf ausgerichtet, schnell auf Veränderungen zu reagieren. Hierin liegt das größte Risiko für die Daten- und Betriebssicherheit – um auf die sich schnell verändernden Anforderungen rechtzeitig und angemessen reagieren zu können, muß sich die IT-Abteilung an die agile Arbeitsweise der Software-Entwicklung anpassen.

In der Software-Entwicklung haben sich kombinierte, selbst-verantwortliche und selbst-organisierte Teams durchgesetzt („DevOps" bzw. „DevSecOps"); es ist die Herausforderung für die IT der öffentlichen Hand, ihre Organisationsstrukturen entsprechend fortzuentwickeln und anzupassen.

Es gilt für die Security in der agilen Software-Entwicklung und im Containerbetrieb der Grundsatz, daß Sicherheits-Probleme aus dem Build nicht mehr im Run aufgefangen werden können („shift-left"), dies ist ein grundlegender Unterschied zum Betrieb z.B. einer Virtualisierungsplattform. Für die durchgängige Sicherheit einer Anwendung ist daher eine enge Zusammenarbeit zwischen Entwicklung und Betrieb unbedingt notwendig. Außerdem sollten Sicherheits-Techniken im Containerbetrieb, wie z.B. Source-Code Scanning, Image Vulnerability Scanning und eine Container-Firewall Lösung zum Einsatz kommen.

In der engen Zusammenarbeit zwischen Entwicklung und Betrieb ist es sinnvoll, auch die Infrastruktur als veränderlich bzw. vergänglich zu betrachten und wie Quelltext zu behandeln („Infrastructure-as-Code"); der Aufbau und die Konfiguration von Infrastrukturelementen wird so in die Hand der Entwickler:innen gelegt werden und paßt sich flexibel an die Bedürfnisse der Anwendungen an („Software-Defined Everything").

Die notwendigen Änderungen in der Organisationsstruktur werden am Anfang die Kosten steigen lassen und wahrscheinlich auch alle Zeitrahmen sprengen; auf lange Sicht lassen sich in einer agilen Struktur jedoch deutliche Kostensenkungen realisieren und gleichzeitig die Zufriedenheit der Mitarbeiter:innen signifikant erhöhen.

Köln, im Juni 2021