# Sicherung und Standardisierung: Ein Schlüssel zur nationalen Sicherheit

**Branche**

Regierung

**Standort**

Deutschland

**Zentrale Herausforderungen**

- Segregation der Umgebung
- Hohe Sicherheitsanforderungen
- Container Hosting

**VMware Produkte**

- VMware Cloud Foundation mit Tanzu
- VMware Aria Automation
- VMware Aria Operations
- VMware Tanzu Kubernetes Grid
- VMware Log Insight

„Das wollte ich immer schon mal sagen", begann Marcus Schoen, Cloud Solution Architect bei comdivision, „aus Gründen der nationalen Sicherheit können wir den Namen unseres Auftraggebers nicht preisgeben." Es klingt vielleicht dramatischer, als es ist, doch selten würde eine Behörde Einblicke in ihre Strukturen oder den Aufbau ihrer Infrastruktur gewähren. Lassen wir es dabei, dass es sich um Finanzmanagement handelt. Auch ohne Kenntnis der Identität des Kunden hat Marcus eine fesselnde Geschichte über die Maximierung von Standardisierungsmaßnahmen zu erzählen.


Neue Sicherheitsrichtlinien und überholte Technik zwangen unsere Auftraggeber dazu, ihre Ansätze bezüglich der Rechenzentrumsinfrastruktur zu überdenken. Früher verließen sie sich hauptsächlich auf Legacy Infrastruktur, die aus Sicherheitsgründen stark normiert waren. Doch nun war die Virtualisierungsumgebung am Ende ihrer Lebenszeit angelangt (Support end-of-life).

Ein hochmodernes – softwaredefiniertes – Rechenzentrum zu haben, war ihre oberste Priorität. Allerdings betonte der Projektleiter, dass „es standardisiert und gesichert sein musste, um zukünftige Anforderungen vorherzusehen. Wir hatten eine Referenzarchitektur im Sinn, die zukünftige Plattform- und Anwendungsanforderungen ohne bedeutende Anpassungen unterstützen würde."

Weiter führte der Leiter aus, dass „die zentrale Voraussetzung für das neue System das Design des Infrastrukturstacks war, einschließlich Hardware und der Flexibilität für diverse Nutzungsszenarien. Obwohl wir internes Fachwissen für den Routinebetrieb haben, war hier spezialisiertes Wissen gefragt." Hier kamen Marcus und sein Team ins Spiel.

## Die Herausforderung

Neben dem Design der Infrastruktur war es notwendig, dass alle Dienste, wie Automatisierung und Überwachung der Systemdienste, direkt von der Plattform bereitgestellt wurden. Für die Notfallwiederherstellung durch ein zusätzliches Cold-Standby-Datenzentrum mussten Komponenten wie Sicherheitsrichtlinien, Cloud-Management sowie Überwachung und Dokumentation integriert werden.

Der finale Blueprint erforderte Autonomie ohne externe Abhängigkeiten. Das System musste eine gewisse Mobilität aufweisen, denn, obwohl es unwahrscheinlich erscheint, sollte es im Falle einer nationalen Krise möglich sein, die Technologie zu verlagern, ohne auf Inkompatibilitäten mit wesentlichen Komponenten wie Netzwerkkarten (virtuell oder physisch) zu stoßen.

## Die Lösung

„Mit VMware Cloud Foundation, ergänzt durch Tanzu, hatten wir bereits eine hochgradig standardisierte Grundlage“, betonte Schoen. Es war jedoch notwendig, jede Komponente – von der Hardware bis zum Workflow – gemäß unserem Anforderungsprofil zu dokumentieren und zu überprüfen. Bei identifizierten Defiziten arbeiteten wir eng mit unseren VMware-Kontakten in Palo Alto zusammen, um sie zu adressieren. Beispielsweise mussten wir neue Technologien für die Netzwerksegmentierung anpassen, externe Sicherheitslösungen integrieren und die Flexibilität und Erweiterbarkeit der Workload-Domain-Bereitstellungen verbessern – um nur einige Herausforderungen zu nennen.

Schoen bemerkte, dass „alles in einer Referenzarchitektur aufgezeichnet wurde, die optionale Komponenten je nach Anwendungsbereich umfasst. Besonders bemerkenswert sind die Sicherheitsaspekte, Autonomie und die Anpassung des Bereitstellungsprozesses, um spezifische Schritte einzubeziehen.“

## Das Ergebnis

Zusammenfassend erhielt der Kunde eine erneuerte Infrastruktur, in der:

- VMware Cloud Foundation den Charakter von Blaupausen und deren Wiederholbarkeit sicherstellt,

- VMware Tanzu Kubernetes Grid als „Modul" für spezielle Anwendungsszenarien integriert ist,
- VMware NSX-T in einem hochausgelasteten Umfeld mit vielen Gruppen und Regeln verwendet wird,
- sämtliche Endbenutzerdienste durch VMware Aria Automation abgedeckt werden,
- VMware Aria Operations als Schlüsselwerkzeug dient, das Betriebsteams mit maßgeschneiderten Gesundheits-Dashboards versorgt,
- und schließlich und schließlich VMware Aria Log Insight als zentraler Log-Empfänger fungiert, der Daten an das zentrale Security Information and Event Management (SIEM) der Agentur übermittelt.

Mit der Zeit wird das System hundertfach implementiert werden und kann viel flexibler auf neue Technologien wie Container reagieren als das veraltete System.

## Weitere Details?

Würden Sie gerne mehr Details zu diesem oder anderen Projekten der comdivision erfahren? Kontaktieren Sie uns via E-Mail: info@comdivision.com, telefonisch unter: +49 251 703839 0 oder schauen Sie sich weitere Case Studys unter https://www.comdivision.com/cd-solutions/modern-apps#Case-Study-Section an.