AMOS on ARO beim Goethe-Institut e.V.

Unsere gemeinsame Reise in die DevSecOps Welt

Sascha Beutler
Robin Walter

Immo Goltz
10/10/2022

DAS GOETHE-INSTITUT
EIN WELTUMSPANNENDES NETZWERK

GOETHE INSTITUT

Sprache. Kultur. Deutschland.

SPRACHE

KULTUR

DEUTSCHLAND

Das Goethe-Institut fördert die Kenntnis der deutschen Sprache im Ausland, pflegt die internationale kulturelle Zusammenarbeit und vermittelt ein umfassendes Deutschlandbild durch Information über das kulturelle, gesellschaftliche und politische Leben in Deutschland.

GOETHE INSTITUT | Atos

158 INSTITUTE IN 98 LÄNDERN, DAVON 12 INSTITUTE IN DEUTSCHLAND

4.060 MITARBEITER*INNEN WELTWEIT

GOETHE INSTITUT | Atos

SPRACHE

WELTWEIT 223.000 DEUTSCHKURSTEILNEHMENDE UND 470.000 PRÜFUNGEN

KULTUR

18.000 KULTUR-VERANSTALTUNGEN WELTWEIT UND 3.600 KOOPERATIONEN

GOETHE INSTITUT | Atos

We are the global leader in secure and decarbonized digital.

Supported by the talent and diversity of 112,000 employees in 71 countries, we generate an annual revenue of €11 billion.

We offer our clients a range of market-leading digital solutions and products alongside consultancy services, digital security and decarbonization offerings.

Wie alles begann

2019

Status Quo

Viele (kleine) Anwendungen
Diverse Stacks (PHP, Python, Node etc.)
Nicht immer professionelles Entwicklungsumfeld
Manchmal nur: "It Works On My Machine"

Anforderung

Enterprise gerechter Betrieb von Containern
Agile Entwicklung innovativer Produkte (LAB)

Ziele

Wirtschaftlichkeit & Time to Market
Ausfallsicherheit & Security
Verpflichtende Vorgaben für Projekte
Einfacher Zugriff für Entwickler
Standardisierung der Docker-Images

GOETHE INSTITUT | Atos

Der lange Weg

Was brauchen wir, was können wir?

12 2019

Anforderungsklärung

Anforderungen an die Plattform

Klärung der Stakeholder Strategisches "LAB"

Welche Lösungen gibt es?

Welches Know How haben wir?

01 2020

Auswahl Umgebung

Workshops mit Entwicklern, Microsoft und RZ Betrieb

Auswahl AKS Plattform zum Erfahrung sammeln

02 2020

POC AKS

Aufsetzen und Entwickeln eines realen Projekts des "LAB"

Volle Unterstützung durch Entwickler

Sehr komplex und aufwändig

Fazit: für Betrieb und Governance nicht geeignet

GOETHE INSTITUT | Atos

Der lange Weg
Evaluierung und Ausschreibung

03 2020

Pilotierung ARO

Begleitung durch Open Shift Experten

„Lernpartner App" des LAB als Prototyp

Aus Entwicklersicht vieles einfacher

Betrieb weiterhin nicht darstellbar

04 2020

Ausschreibung Betrieb

Leistungsbeschreibung für Betrieb und Plattformsupport

Anforderungen an Entwickler

Ausschreibungsunterlagen

08 2020

Vergabe Betrieb

Vergabe Betrieb und Entwicklerunterstützung an ATOS

Product Owner Plattform und Applikation: Goethe-Institut

Externe Entwicklerteams

GOETHE INSTITUT | Atos

AMOS auf Azure

Atos Managed OpenShift – Unsere gemeinsame Verantwortung

Goethe-Institut | Atos | AMOS (Atos) | Microsoft & Red Hat

Full Lifecycle Application Management

Erstellung, Betrieb und Verwaltung von Anwendungen

Clustermanagement

- Installation
- Konfiguration
- Betrieb
- Updates
- Weiterentwicklung
- Backup & Restore

Monitoring und Alerting

- Konfiguration
- Auswertung
- Reporting
- Trends

Additive Services

- OpenShift Services
- Azure Services
- Security Services
- etc.

Cloud Native und DevSecOps Anwendungs-consulting

- Anwendungsberatung
- Anwendungsmigration
- Automatisierung
- Deployment- und Releasemanagement
- Workshops

Microsoft Azure

Azure Red Hat OpenShift

RED HAT® OPENSHIFT

GOETHE INSTITUT | Atos

AMOS für das Goethe Institut

Der Weg bisher

Übernahme

ARO-Umgebung
- Erstellung mit Microsoft
- Fünf initiale Projekte

Vertrag mit Atos

Transition

Konfiguration
- Angepasstes Monitoring
- Alerting
- Tägliche Reports
- Permanente externe Verfügbarkeitsprüfung

Handbücher
- Projekthandbuch
- Entwicklerhandbuch
- Betriebshandbuch

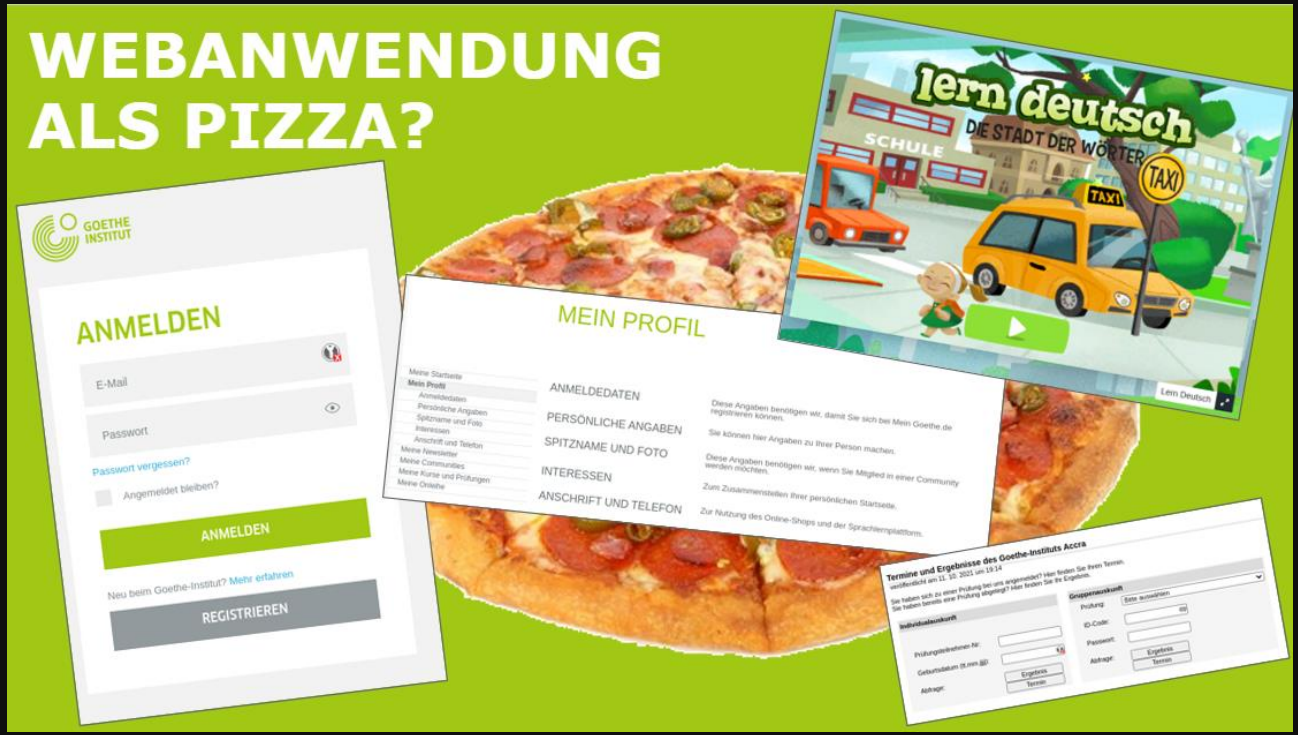
Entwicklung

Top-Themen:
- AAD Gruppen Synchronisation
- Backup & Restore
- Blueprint für Tekton Pipelines
- Projektbezogenes Alerting
- Zusätzliche StorageClass
- Applikationsmetriken
- …

GOETHE INSTITUT | Atos

Internes Marketing

Pizza und Live-Coding Webcast



Pizza as a Service Analogie

GOETHE INSTITUT | Atos

Unsere Erfahrungen

… meist Positiv

Der ARO Service war innerhalb von 2 Jahren immer verfügbar.

Securityupdates werden automatisch von Azure ausgerollt (Z-stream Update).

Alle weiteren geplanten Clusterupdates durch AMOS liefen immer problemlos.

Dies führt leider auch dazu, dass etcd Backups nicht vollumfänglich für ein Disaster Recovery nutzbar sind.

GOETHE INSTITUT | Atos

Unsere Erfahrungen

… mit unerwarteten Problemen

Vertrag ≠ Vertrag

GI hatte aus Gründen der Kosteneffizienz VMs reserviert mit dem Ziel, den Cluster zu vergrößern. Leider war diese nicht direkt nutzbar, da Sie in einem anderen Azure Vertrag reserviert waren. Es war ein neuer Aufbau des Clusters im Zielvertrag nötig

Ausgesperrt

Azure AD Login war nicht mehr möglich. Ursache war ein abgelaufenes Service Account Token in Azure welches für die Integration im ARO Cluster hinterlegt ist. Ohne einen Notfalluser hätten wir den Zugriff verloren.

Backup?!

Azure empfiehlt Velero für Backup und Restore. Dies deckt aber nur Azure Disk über Snapshots ab. AMOS setzt hier Velero + Restic ein um auch Azure Files zu unterstützen.

VELERO

GOETHE INSTITUT | Atos

Unsere Erfahrungen

… und einer Veränderung des Mindsets

Cloud Native Softwareentwicklung mit Kubernetes benötigt neue Entwurfsmuster.

Entwicklerteams benötigen Schulung und Beratung.

In der VUCA* Welt bedarf eines iterativen Vorgehens und dazu passender Vertragsgestaltung.

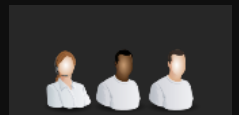
Continuous Improvement ist deshalb essentieller Teil von AMOS.

VUCA: Volatility, Uncertainty, Complexity & Ambiguity

GOETHE INSTITUT | Atos

DevSecOps

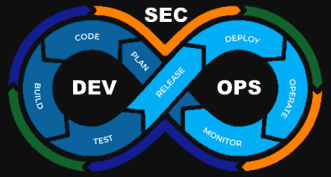
gemeinsame Verantwortung, shifting security left



Security Experts

AMOS Team

Dev Team



Manuelle Security Tests

IAST / RASP / DAST *

Network & Access Observability

Richtlinien Auditing & Enforcement

Image Scanning

Container Scanning

Statische Codeanalyse Unit Tests

Dependency Scanning

Security By Design

Kosten

* Interactive Security Tests / Runtime Application Self Protection / Dynamic Application Security Tests

GOETHE INSTITUT | Atos

Die Digitale Deutsch Prüfung des Goethe-Instituts

Auslöser einer Sicherheitsbedarfsanalyse des AMOS ARO Clusters

https://www.goethe.de/de/spr/kup/prf/prf/ddd.html

GOETHE INSTITUT | Atos

Anpassung der Cluster Security

Neue Anforderungen = neue Herausforderungen

Auftrag für eine Sicherheits-bedarfsanalyse des ARO Clusters durch Atos BDS

Basis: Die sechs relevaten Bausteine zum BSI Grundschutz

Unter anderem:

- Containerisierung
- Kubernetes

GOETHE INSTITUT | Atos

BSI Grundschutz

Kann, Soll und Muss Anforderungen

GOETHE INSTITUT | Atos

Anpassung der Cluster Security

Neue Anforderungen = neue Herausforderungen

We are here!

Beauftragung → Analyse → Strukturierung → Entscheidung → Umsetzung

Auftrag für eine Sicherheits-bedarfsanalyse des ARO Clusters durch Atos BDS

Basis: Die sechs relevanten Bausteine zum BSI Grundschutz

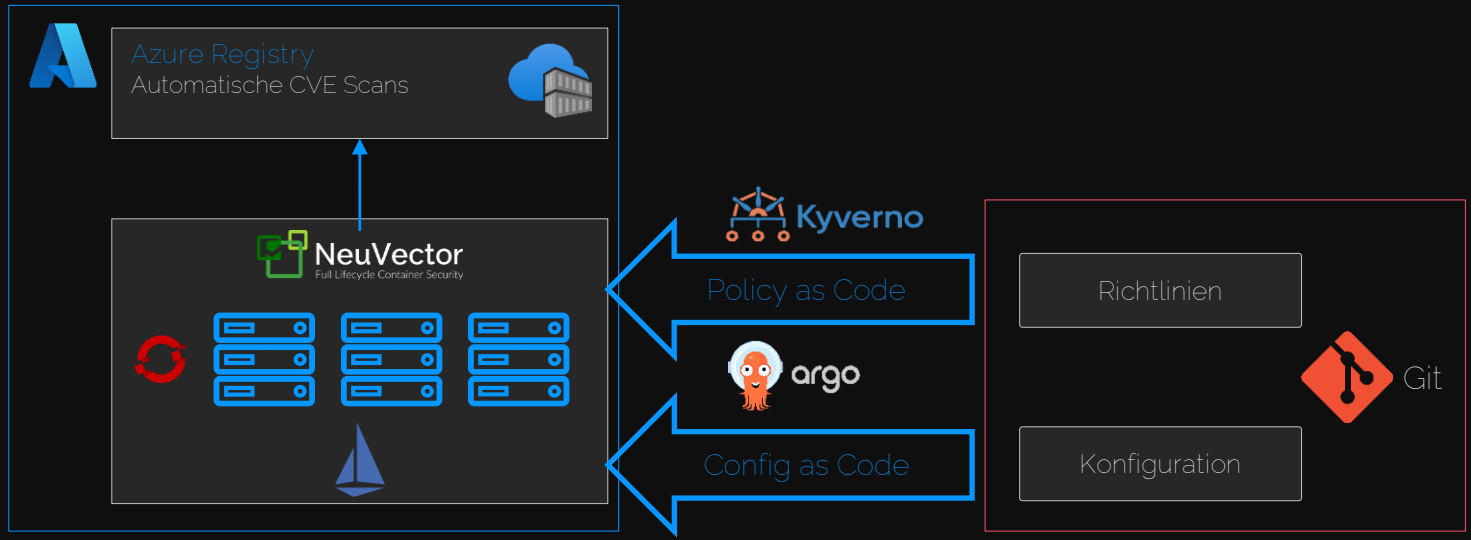
Unter anderem:
- Containerisierung
- Kubernetes

Entscheidungen im Goethe Institut:
- Umsetzung
- Priorisierung

Umsetzung in mehreren Scrum Projekten.

GOETHE INSTITUT | Atos

Ausblick: „Defense In Depth"



Service Mesh (Istio)

E2E Verschlüsselung
Zugriffs und Flusssteuerung
Sichtbarkeit

Policy Management (Kyverno)

Richtlinienverwaltung
Verstoßauditing und Erzwingung
Setzen von Defaults

GitOps (Argo)

Azure Repos (Git) = "Single Source of Truth"
Disaster Recovery enabler

Vulnerability Management (NeuVector)

Compliance
Runtime Security
Supply Chain Security
Network Visibility
Container Segmentation

GOETHE INSTITUT | Atos

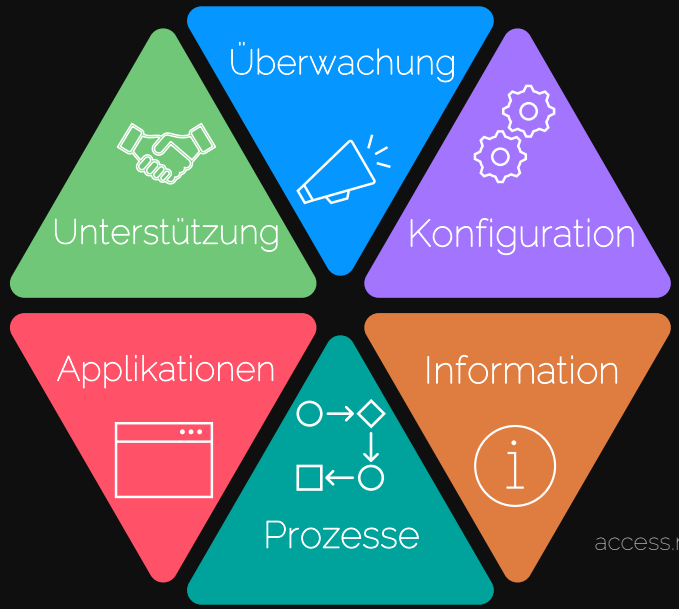
DevSecOps beim Goethe-Institut

Security begleitet uns dauerhaft

Unterstützung
Unterstützung der Entwickler (Entwicklerhandbuch, How-to-Artikel, …)

Applikationen
Schutzbedarfsprüfungen relevanter Anwendungen

Prozesse
Prozessänderungen. Z.B. bei Changes Security einbinden und Möglichkeit des Widerspruchs beachten.



Überwachung
Zusätzliches Logging, Monitoring und Alerting

Konfiguration
Kontinuierliche Anpassung aufgrund sich ändernder Anforderungen und Updates

Information
Stetiges Informieren über generelle und produktbezogene Schwachstellen. Für Red Hat: access.redhat.com/security/vulnerabilities

GOETHE INSTITUT | Atos

Thank you!

sascha.beutler@atos.net
robin.walter@atos.net

immo.goltz@goethe.de
10/10/2022