Herausforderung DevOps statt DevOops

Betrachtungen aus dem Blickwinkel eines Sicherheitsverantwortlichen

Wolfgang Mayer, Head of IT Security
Corporate IT
HOERBIGER Deutschland Holding GmbH

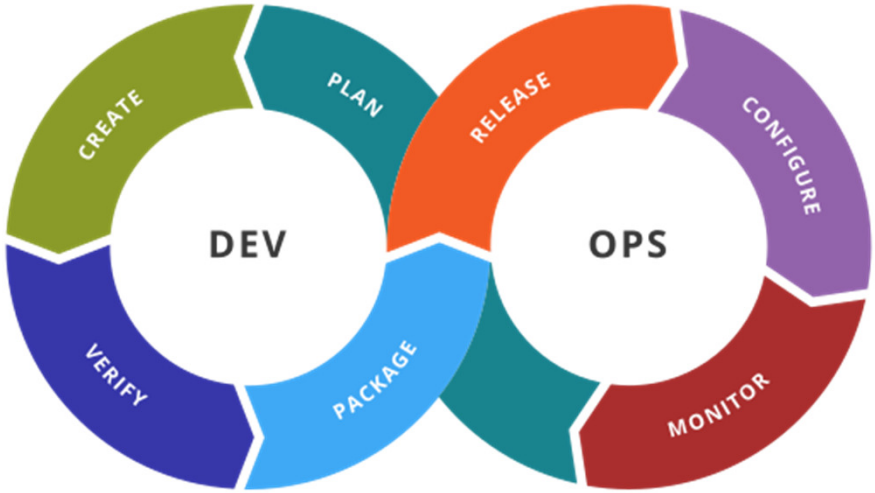
HOERBIGER

Prologue

Agile-Entwicklung und Service-, System-Betrieb in einer Organisationseinheit vereint

DevOps: Verschmelzung von Development & Operations

Organisationstruktur



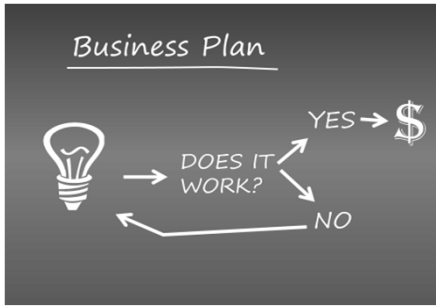
Vergleich agile Software Entwicklung: „Prozeduren um Denkweisen zu ändern“

ImgSrc: https://en.wikipedia.org/wiki/File:Devops-toolchain.svg;

DevOps Marketing Versprechungen & Erwartungen

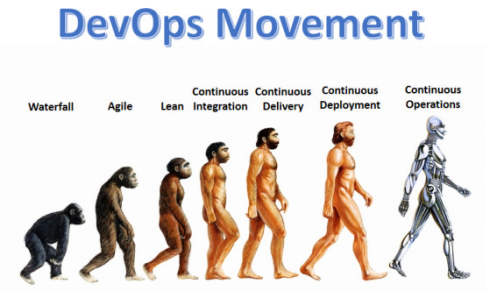
"… engage in this powerful steps in order to achieve outstanding results with DevOps …"

Business



- Opex Optimierung
  - Asseteffizienz
- Wettbewerbsvorteil
  - Marktpenetrierung & Diversifikation (fast,more)
- Kundenbindung
  - Continuous Delivery
- Hype Riding/Cool Culture
  - Apps, IoT, Industrie 4.0, Big Data

Development / Operations



- Automatisierung
  - Fehlervermeidung
- Qualität
  - Faktorisierung
- Wissens/Erfahrungsaustausch
  - Innovationstreiber
- Stability vs Quickfix
  - Dein Code/Dein System

Information Security & QA

- Security by design/default
  - DevSecOps
- Lifecycle
  - Planbare Produktzyklen
- Rollout/Deployment
  - Saubere Implementierung
- Messwerte
  - KeyPerformanceIndicator (KPI)

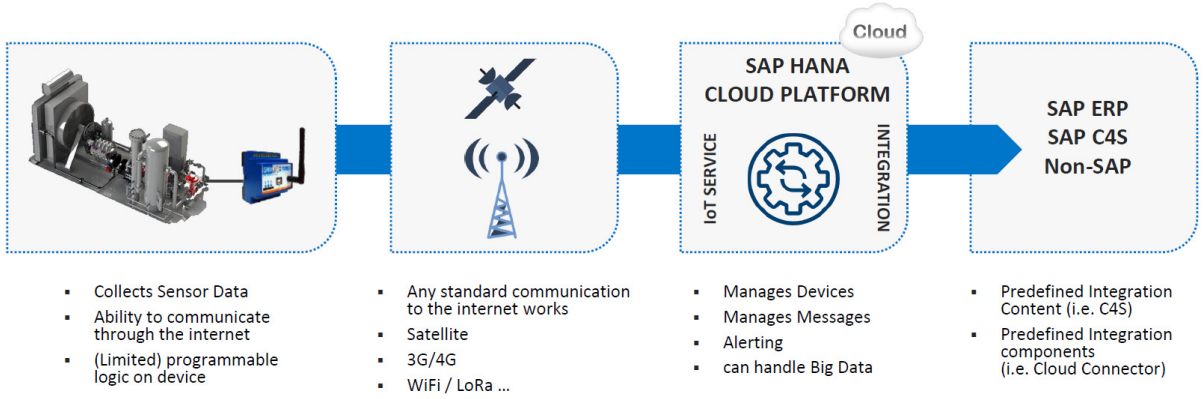
Source:Img_Businessplan, Img_DevOpsMovement, Img_OMG

Globale Prozesse für Entwicklung/Betrieb sind wesentlich

DevOps eine Herausforderung in seit 1895 gewachsener, globaler Matrix Organisation

Strategische Unternehmensbereiche 4 | Mitarbeiter ~7000 | Standorte +150 | Länder +50

Beispiel: Wellhead Compression | Lease Fleet



Development (inkl. R&D)

- 4 Länder (AT, DE, SE, US, IN)
- 12 Legal Entities ca. 220MA, (4 Entities Fokus Development)
- Von analog/digital Hardware zu Prozesslogic
- Assembler & VHDL über C/C++/C# & .NET zu Java&ABAP)
- External Contractors

Operations (inkl. Frontend)

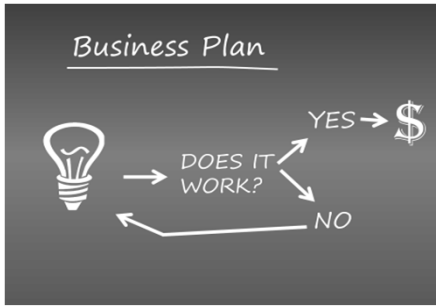
- 6 Länder (AT, DE, IN, SG, CN, US)
- 40 MA
- 1000 Server
- 11000 Endpoints
- External Contractors

Buzzer: IoT, Mobile, SupplyChain/Bigdata, Industrie4.0,Lean,

DevOps Realitätscheck & Ernüchterung

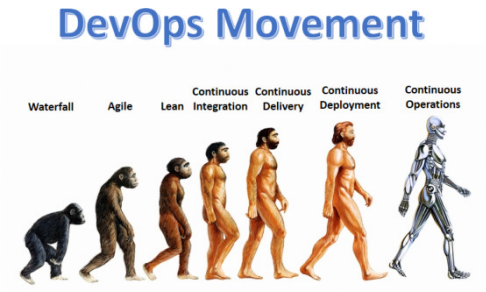
Buzzword Bingo

Business



- Opex Optimierung
  - weniger MA
- Wettbewerbsvorteil
  - Kurzlebige Produkte minderer Qualität
- Kundenbindung
  - Continous Escalation
- Hype Riding/Cool Culture
  - Done – we are cool

Development / Operations



- Automatisierung
  - Fehlerverlagerung
- Qualität
  - siehe Fehlerverlagerung
- Wissens/Erfahrungsaustausch
  - Kaffeepausen - siehe Opex Optimierung
- Stability vs Quickfix
  - Dein Code! Dein System!

Information Security & QA

- C.I.A.
  - Availability
  - Integrity
  - Confidentiality
- Security Standards
  - Segregation of duty
  - Datensicherheit
- Gesetze/Verträge
  - Datenschutz
  - Supplier Requirements

Source:Img_Businessplan, Img_DevOpsMovement, Img_OMG

Struktur & Rahmenbedingungen zur Risikominimierung

Challenge Accepted in für mehr Dynamic

Areas	Herausforderung	Beispiel
GRC	▪ global unterschiedliche Gesetze ▪ Einhaltung von Standards ▪ Verträge & Supplierrequirements ▪ Zeitnahe Riskanalysis	▪ Datenschutz-,Cybersecuritygesetze ▪ ISO 27001, IEC 62443 (folge Folie) ▪ Versicherungen ▪ BIA/BCM
Culture	▪ Silodenken ▪ Kultur ▪ Intergration externer Ressourcen ▪ Bestehende, gelebte Prozesse	▪ Kingdoms, Wissenaustausch ▪ Assets (Sheldons), Zeit/Qualitätsaffinität ▪ „Die machen das schon, kostet ja genug!“ ▪ Übergangs Zeit, Widerstand
Business	▪ Opportunities vs Risks ▪ Keine Vision, Plan, Scope ▪ Controlling-, Managementschwächen ▪ IT als enabler für Business	▪ Marketing/Buzzword Gläubigkeit ▪ DevOps! Mach ma mal schnell ▪ Neue Tools - die machen das schon ▪ Vorbeugung von Shadow IT

Facts: only ISO27001 is normative binding

Guidelines are not mandatory

ISO27001 is the only normative binding document, Guidelines are not mandatory

Information Assets in Development and Testing

- Data access and protection mechanisms must be defined (A.8.2.1-3)
- Secure development environments development cycle (A.14.2.6)
- Suitable (protected) data in test environments (A.14.3.1)

Software development process controls

- Acceptance testing is mandatory (A.14.2.9)
- Security tests during the overall development process (A.14.2.8)
- Separation Development/Test/Production (A.12.1.4)

Controls for the software product

- Security system engineering principles (A.14.2.5).
- Information security requirements analysis/specification (A.14.1.1)
- Secure application-services/networks/transactions (A.14.1.2/A.14.1.3)

Agile Projects KeyChallenge

Development and testing overlap time-wise.

Roles overlap.

In the development methodology however, this is no excuse for missing documentation or non-implemented controls in an ISO 27001 audit.

All controls mentioned must exist for all projects

A clever strategy for dealing with ISO 27001 can help

ISO requires suppliers also to be managed with regard to information security

The work can be outsourced but the responsibility stays with the organization.

Controls for Release and Change Management

- Change management for changes in IT and business (A.12.1.2)
- Restriction on changes to software packages (A.14.2.4)
- System change control procedures (A.14.2.2)
- Technical review of applications after OP changes (A.14.2.3)
- Installation of software on operational systems (A.12.5.1)
- Separation of development/testing/production (A.12.1.4)
- Access control to program source code (A.9.4.5)

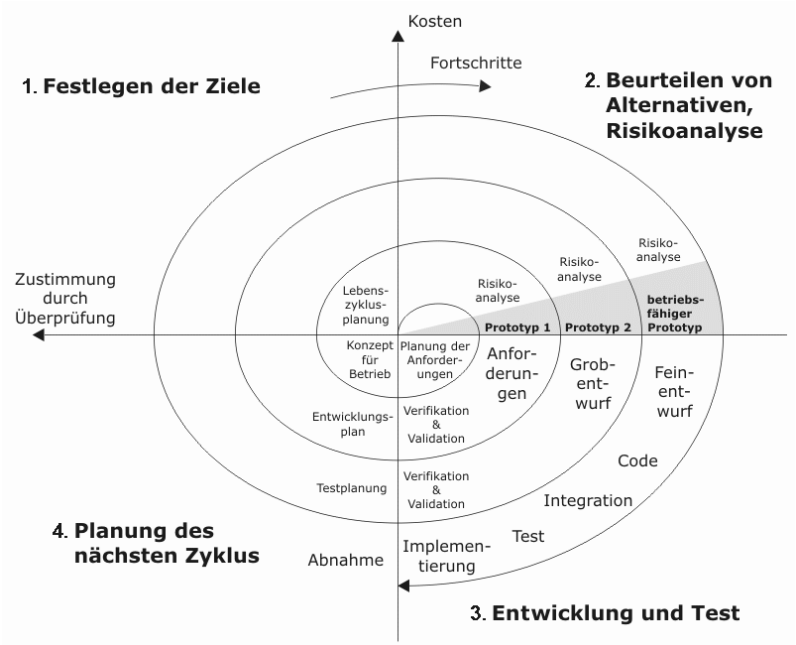
Controls for Outsourcing

- The sourcing partners obtain sensitive data they should not have.
- Their software development and testing processes might not address the information security needs properly. (A.14.2.7)
- Requires suppliers also to be managed with regard to information security (A.15).

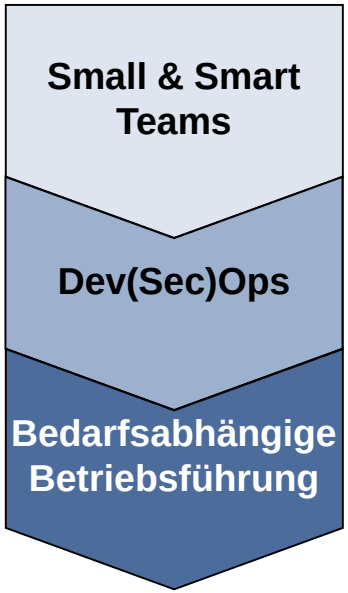
Mögliche Lösungsstrategie und Umsetzung

Identify Opportunities & Risks | Vision, Scope & Resources | Proper Controlling & Procedures

Iteratives Spiralmodell (B.W. Boehm)



Erweiterung zu Spiralmodell



- Supervised von zb. Scrum Master
- InfoSec als weiterer Stakeholder

- Iteration 3 Integration: Migration in PoC/agilen Betrieb wenn geeignet

- Fortführung/Stop des agilen Betriebs
- Ersatz durch neuen PoC
- Spinn Off
- Migration in klassischen Standard Betrieb (Sicherstellung SDLC)

Source: https://de.wikipedia.org/wiki/Datei:Spiralmodel_nach_Boehm.png;

Summary - Challenge Accepted

Conclusion – DevOps ist eine von mehreren Möglichkeiten

A) DevOps ist leichter umsetzbar als Startup/Greenfieldansatz und/oder in kleinen Entitäten

B) Mindset change, GRC und Übergabe/Übergangs Zeit sind die grössten Herausforderungen

C) … engaged and powerful IT together with Business achieves outstanding results …

DevOps ist eine Chance! Nicht überall und um jeden Preis

About me

Wolfgang Mayer

LinkedIn

Head of IT Security
Executive
Corporate IT

HOERBIGER Deutschland Holding GmbH - Zweigniederlassung Wien
Seestadtstraße 25,
1220 Vienna, Austria
http://www.hoerbiger.com

+25 Jahre IT Erfahrung mit Schwerpunkt Informations-Sicherheit

- Seit 2014 global verantwortlich für Information Security bei HOERBIGER
- IT-Security Koordinator bei Raiffeisen Informatik,
- CISO bei Valartis Bank (Austria) AG.
- Anglo Irish Bank (Austria) AG, Information Security Officer Austria
- Davor als System- und Netzwerkadministrator in diversen privatwirtschaftlichen KMUs

DANKE FÜR DIE AUFMERKSAMKEIT