

IT-Security in einer agilen Welt



Matthias Jambor

FiSi, System Administrator, DevOps Engineer

operating web application seit 2003

Team Lead IT-Security @ REWE digital

Kontakt: [@grambulf](#), [LinkedIn](#)

REWE

DER
Touristik

BILLA

PENNY.

BIPA

toom

1927 gegründet
61,2 Milliarden Euro
Umsatz
360.315 Mitarbeiter
15.686 Geschäfte
Lebensmittel, Touristik,
Baumarkt

2014 gegründet
~ 650 Kollegen
Online Shop,
Lieferservice,
Fulfillment,
Digitalisierung


REWE digital

Gin

Liefertermin wählen

Favoriten

Warenkorb 0,00 €

- Alle Produkte
- Meine Produkte
- Angebote
- Themenwelten

◀ Zurück

Deine Suche nach „Gin“ ergab 50 Treffer

Artikel pro Seite

40

Sortieren

Preis absteigend

Kategorien

Wein, Spirituosen & Tabak

Spirituosen & -
mischgetränke

Gin, Genever &
Wachholder

Mischgetränke &
Cocktails

Getränke

Drogerie & Kosmetik

Nahrungsmittel

Kaffee, Tee & Kakao

Eigenschaften

☐ *ANGEBOTE*

☐ Bio

☐ Alle Produkte

☒ REWE Lieferservice

☐ Versand per Paket



Windspiel Premium Dry Gin 0,5l

0,50l (1 l = 87,98 €)

43,99€



— 1 +



Hendrick's Gin 0,7l

0,70l (1 l = 49,86 €)

34,90€



— 1 +



Mombasa Club Premium Gin 0,7l

0,70l (1 l = 47,13 €)

32,99€



— 1 +

Mein Konto

Meine Daten

Meine Zahlungsdaten

Meine Bestellungen

Meine Lieferflat

Meine Coupons

Mein PAYBACK

Kontakteinstellungen

Datenverwaltung

Account löschen

Meine Daten

Zugangsdaten

E-Mail-Adresse

► Bearbeiten

Passwort

► Bearbeiten

Persönliche Daten

Anrede, Vor- und Nachname

Herr Klaus Klaus

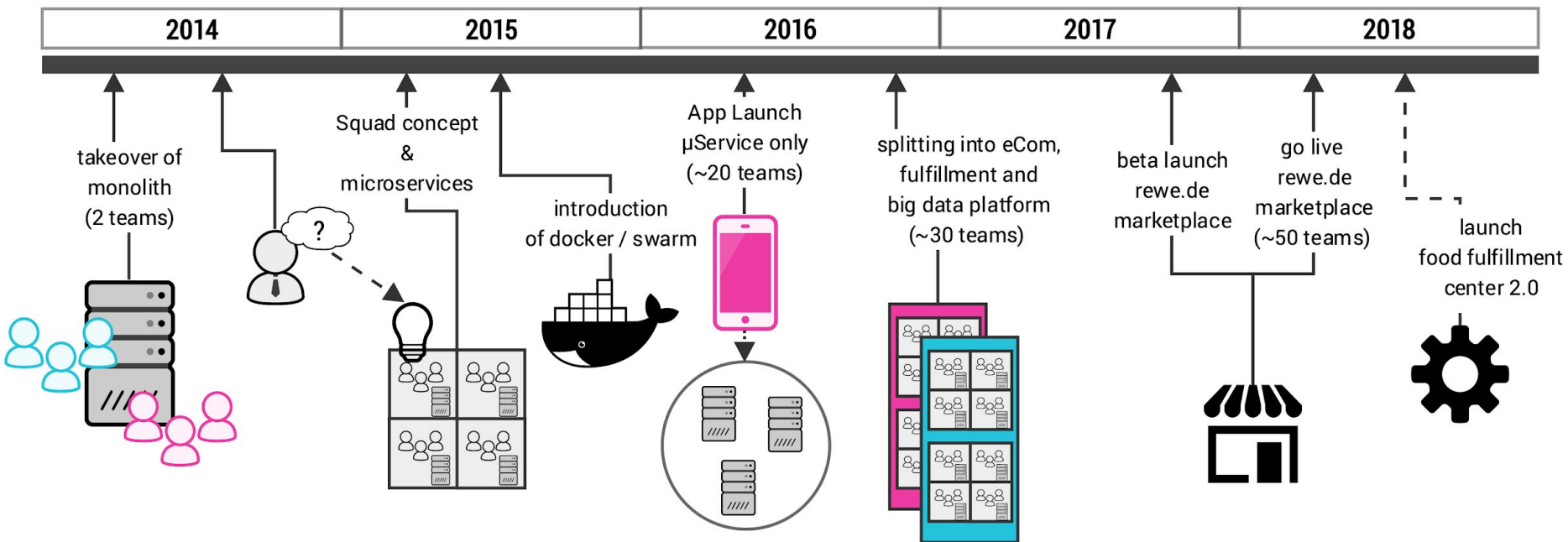
► Bearbeiten

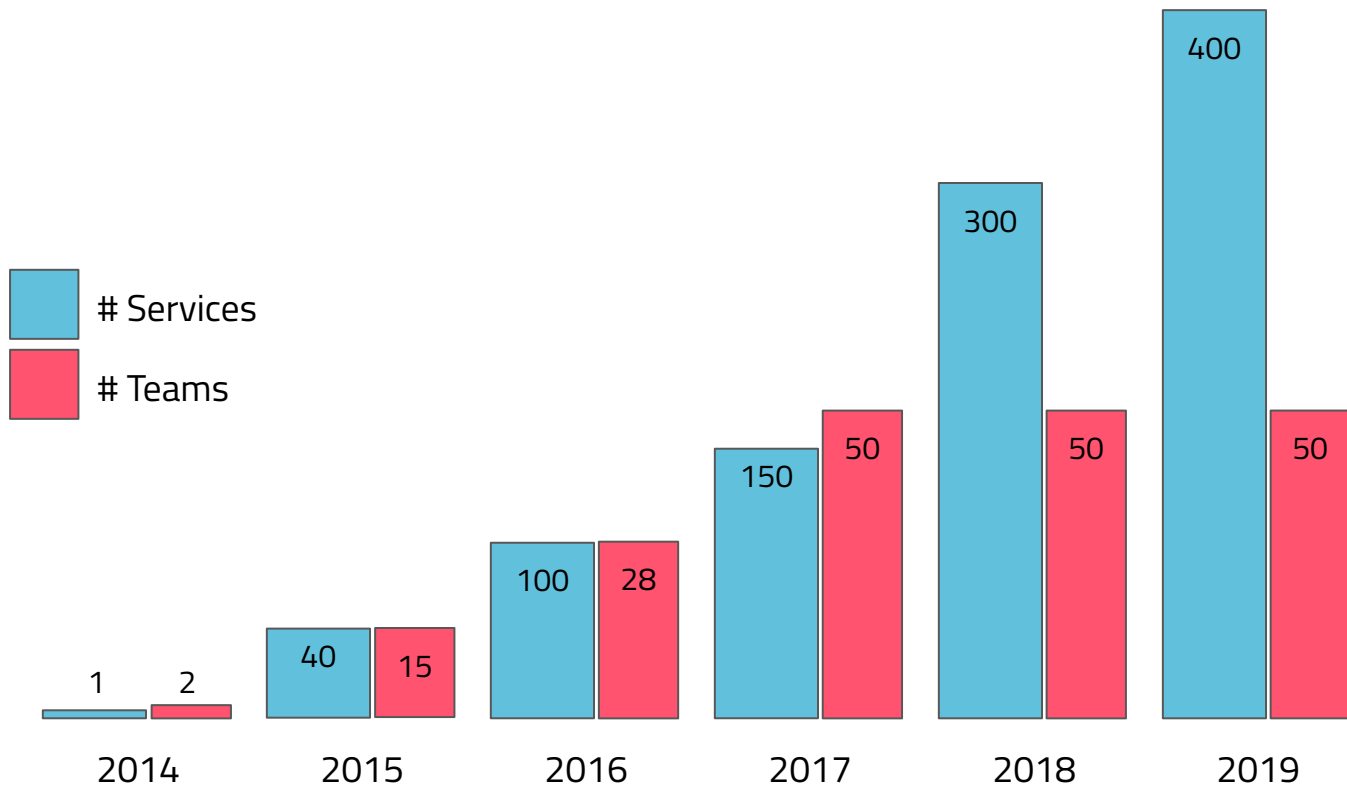
Adressen

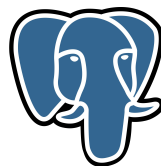
Rechnungsadresse (Privatkunde):

☐ Frau ☒ Herr

Vorname
Klaus







DevOps

- “Unser Ops Mensch hat gekündigt, wir machen jetzt DevOps”
- “Bei meiner neuen Firma ist es super. Wir haben keine Ops, die alles blockieren. Bei uns machen die Entwickler alles selbst. ”
- “Bei uns hat jeder root Zugriff. Wir machen jetzt DevOps”




DevOps Borat

@DEVOPS_BORAT

Folgen



To make error is human. To propagate error to all server in automatic way is **#devops**.

 Tweet übersetzen

20:55 - 26. Feb. 2011



Source: <https://twitter.com/petecheslock/status/595617204273618944>

“Devops is a way of thinking and a way of working. It is a framework for sharing stories and developing empathy, enabling people and teams to practice their crafts in effective and lasting ways. It is part of a cultural weave that shapes how we work and why.”

Effective DevOps - Jennifer Davis, Ryn Daniels

- **Astera Schneeweisz, “Building security teams” (AppSec EU 2017)**
- **Chris Wysopal, “Full Spectrum Engineer - The New Full-Stack” (Heise devsec Keynote 2017)**
- **Dino Dai Zovi, “Every Security Team is a Software Team Now” (Blackhat Keynote 2019)**
- **Kelly Shortridge & Nicole Forsgren, “Controlled Chaos: The Inevitable Marriage of DevOps & Security” (Blackhat 2019)**
- **Everything from LocoMocoSec**

Bearbeitung eines Incidents

1. Cool und freundlichen bleiben
2. Incident Ticket erstellen und abarbeiten
3. Blameless Postmortem durchführen, z.B.
 - SRE bei Google
 - mit Kaffee die Kollegen besuchen
4. Verwendet die Erkenntnisse für positive Veränderungen

Bild von Ange Albertini



KEEP
CALM
AND

CA

```
*** glibc detected ***  
*** ./calm: double free or corrupti  
on (out): 0x0000f4e0fe9bf990 ***  
Aborted (core dumped)  
# █
```

Kultur

Veränderung der Security Kultur - Sinn eines Bootcamps

- Jeder neue Kollege bekommt alle nötigen und hilfreichen Informationen
- Alle sind auf dem gleichen Kenntnisstand
- Alle kennen die Werte und Kultur eures Unternehmens

Veränderung der Security Kultur - Mögliche, nicht technische Inhalte eines Bootcamps

- **Geschichte des Unternehmens**
- **Vision und Mission**
- **Erwartungshaltung zum zwischenmenschlichen Umgang**
- **Welche Ansprechpartner gibt es**
- **Wo gibt es Möglichkeiten zum Mittagessen**
- **Datenschutz und Informationssicherheit**

Veränderung der Security Kultur - Mögliche, technische Inhalte eines Bootcamps

- Deep Dive zur Architektur
- Tooling
- Datenbanken, Versionierungssystem
- Jira, Confluence (oder ähnliches)
- Vorstellung übergreifender Teams (Architekten, IT-Security, Incident Management, Office-IT, ...)

Veränderung der Security Kultur - Präsenz zeigen

- Teamvorstellung im Bootcamp
- interne Tech Talks über Security
- "IT-Security News", was ist neu und betrifft die Kollegen
 - Veränderung von internen Regelungen
 - Kurzvorstellung von Pentestergebnissen
 - Aktuelle Ereignisse (LuminPDF, Firefox Mac OS X Backdoor)

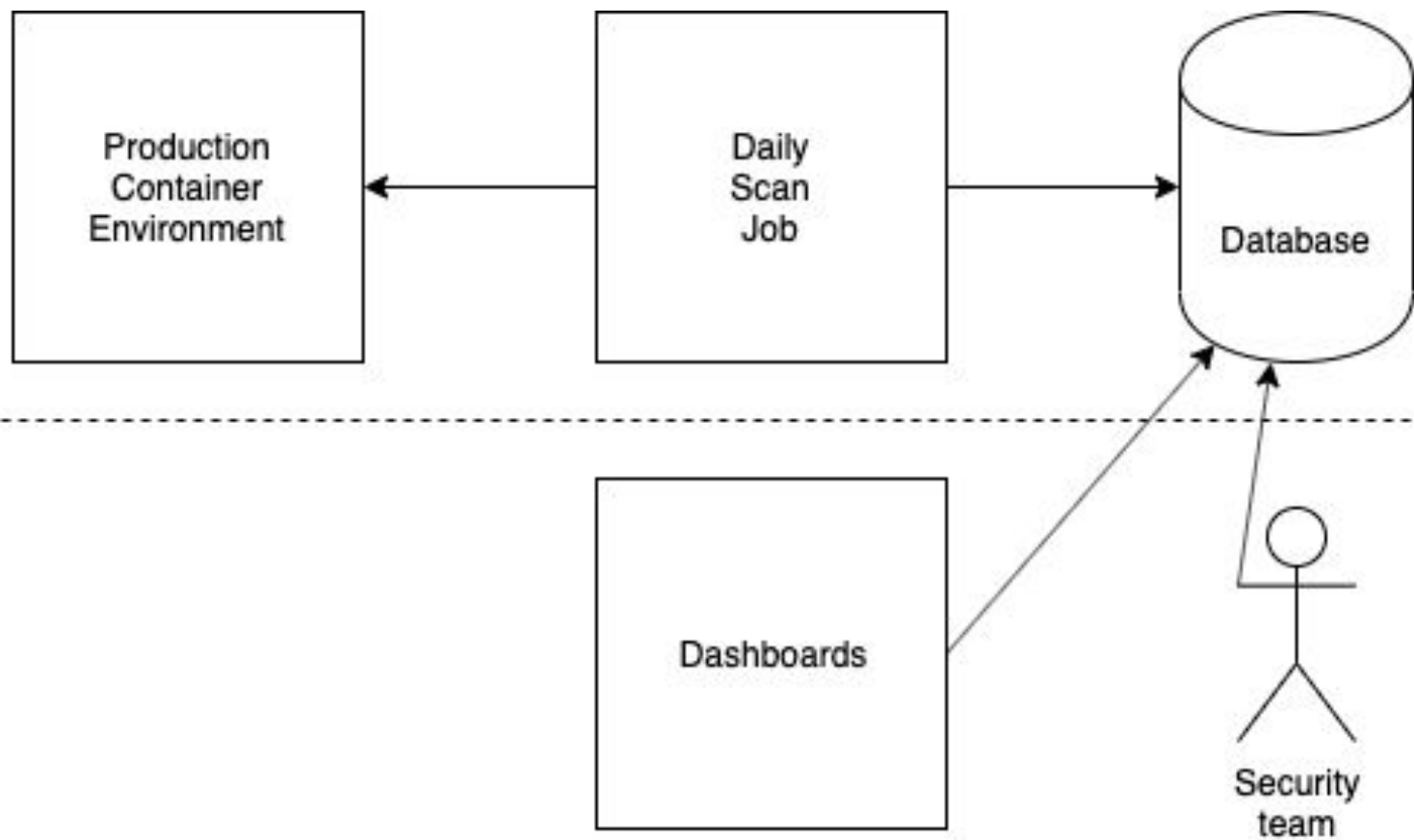
Veränderung der Security Kultur - Training und Ausbildung

- Bietet ein für euch zugeschnittenes Training zur sicheren Softwareentwicklung an
 - Externer Trainer behebt das Problem des Propheten im eigenen Land
 - Kleine Gruppen (<15 Menschen) involvieren jeden
 - Umgebung ist wichtig (Beispiel: Loge im Stadion o.ä.), vermeidet Räume in der Firma
 - Begleitet das Training sinnvoll, seid die Brücke zwischen Trainer und internen Anforderungen
 - Schafft eine gemeinsame Basis für alle
- Bei Budgetproblemen schmeisst ihr eine eurer "Next Generation Machine Learning"-Security-Appliances raus und verwendet die gesparten Lizenzkosten ;)
- Macht das Training spannend, einfach zugänglich, freiwillig, sinnvoll (insert no_shit_sherlock_meme.png here)

Technik

Software Bill of Material und Asset Management

- Das ist nicht einfach...
- Wisst was ihr betreibt, Beispiele:
 - Infrastructure as Code
 - OWASP Dependency Check
 - Google Cloud Asset Inventory
 - "VersionMonitor"
- Dann meldet zu patchende Lücken ausschließlich und explizit an betroffene Teams, bitte keine "jeder das das liest sollte mal sehen, ob sie vielleicht betroffen sein könnten" Mails



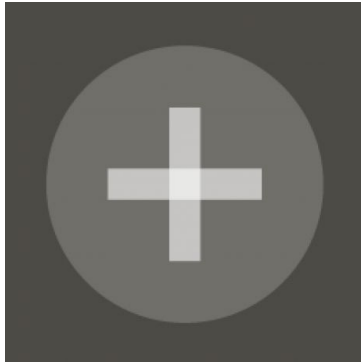
“OWASP TOP10 A9 Check” as a Service

- Bietet einen Service durch Tooling an
 - Zentraler Dependency Check
 - [Snyk.io](#)
 - [Container Scanner](#)
- Macht die Benutzung einfach und hilfreich
- Filtert False Positives raus
- Passt Regeln für euch an

Pentest oder Security Assessment

- Gute Pentest Teams sind eine hilfreiche Unterstützung
- Für ehrliches Feedback:
 - Whitebox Ansatz
 - Zugriff auf Code, Dokumentation, Entwickler
 - Planung und Vorbereitung gemeinsam mit Architekten, Entwicklern und Produkt-(Owner/Manager)
 - Präsentation der Findings mit allen betroffenen Teams
 - Gruppierung und Analyse der Findings, müsst ihr bei Training nachjustieren?
- Für die Governance-Checkbox im Excelsheet
 - Google Suche

Persönliche, gute Erfahrungen mit: Cure53, Recurity Labs, RedTeam Pentesting
Vortrag zur Auswahl eines Pentesting Anbieters



Zusammenfassung

- Seid nett zu euren Kollegen
- Kultur frisst Compliance zum Frühstück
- Sorgt dafür, dass jeder weiss, was von ihm erwartet wird
- Jeder muss die Ansprechpartner für unterschiedliche Fragen kennen
- Versorgt jeden einzelnen mit allem Basiswissen
- OWASP Top10 A9 ist einfach (und sehr schwer)
- Eine Verifizierung durch einen externe Partner ist sehr hilfreich
- be excellent to each other

- Unterstützt euch gegenseitig
- Schmeisst euren "Meinungsverstärker" weg
- Mit einer positiven Kultur und gemeinsamen Anstrengungen erreicht ihr mehr

