rt-solutions.de

experts you can trust.

Outsourcing der App-Entwicklung - Fluch oder Segen

Dr. Georg Lukas

17. Cyber-Sicherheits-Tag

IT-Security-Berater aus Köln

Unterstützung auf allen Ebenen:

- **Pen-Tests & App Security**
- **Outsourcing & Prozesse**
- **Risiko-Management & Compliance**

rt-solutions.de
experts you can trust.

Dr.-Ing. Georg Lukas

Schwerpunkte

- **Mobile Sicherheit**
- **Zahlungssysteme**
- **Awareness Trainings**

Agenda

rt-solutions.de

- **Die eigene App**
  - Ziele und Herausforderungen
  - Integration in die Corporate IT
- **Herausforderungen beim Outsourcing**
  - Technische Herausforderungen
  - Organisatorische Herausforderungen
  - Datenschutz
- **Fazit**

Ziele einer App

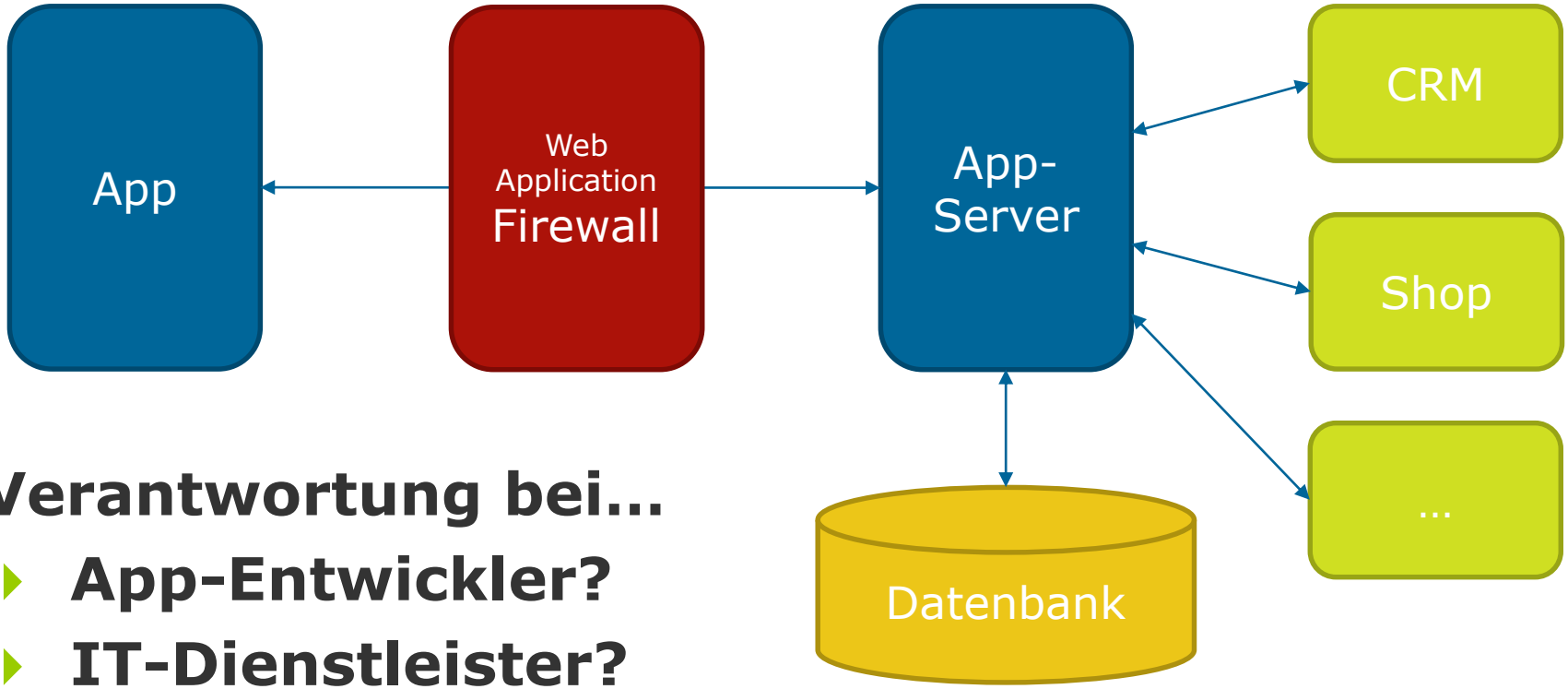
rt-solutions.de

- **Brand Awareness**
- **Bessere Kundenbindung**
- **Customer Self Service**
- **Zugriff auf eCommerce-Systeme**

- **Anforderungen:**
  - Günstig
  - Optisch ansprechend
  - Schnelle Umsetzung

Anbindung an die Corporate IT

rt-solutions.de



Verantwortung bei…

- **App-Entwickler?**
- **IT-Dienstleister?**
- **Auftraggeber!**

Fallstricke aus der Praxis

rt-solutions.de

Benutzer-Authentifizierung

- App sendet Nutzer-Passwort mit jeder Server-Anfrage
- App-Token, der außerdem zur Admin-UI berechtigt

Kommunikation (SSL/TLS)

- Fehlende Zertifikatsprüfung (Aussteller, Server-Name)
- Unverschlüsselte Übertragung im Datacenter (Passwörter!)

Sichere Schnittstellen

- Triviale URL-Änderung: `/getuser/23` zu `/getuser/24`
- Fehlende Validierung von Nutzereingaben

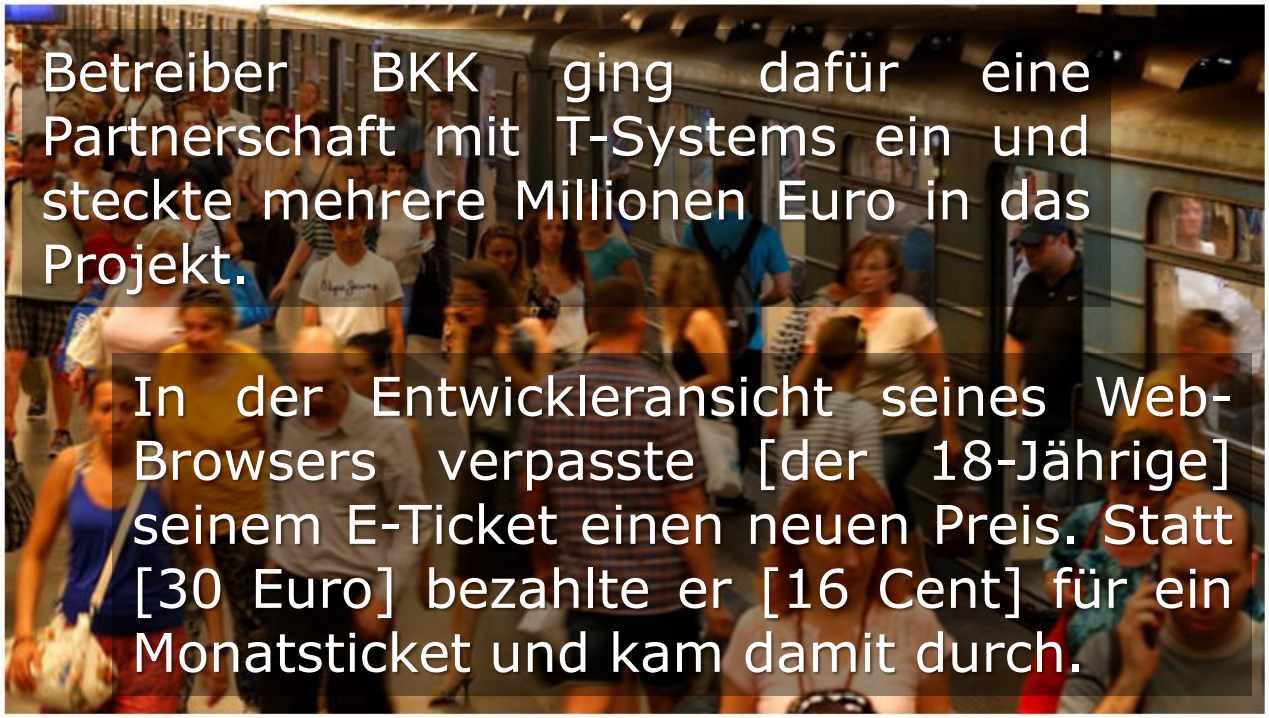
Validierung von Eingaben

rt-solutions.de

DIGITALISIERUNG

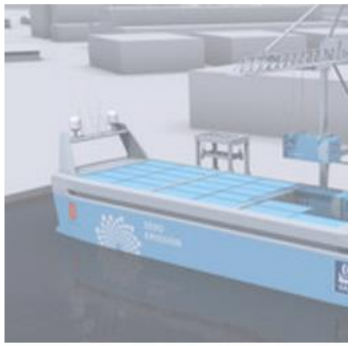
E-Ticket-Debakel: Budapester Öffis ernten Shitstorm

24.07.17, 10:49 Mail an die Redaktion



Über eine mobile Webseite soll man in Budapest erstmals elektronische Tickets für Öffis kaufen können. Durch einen Fehler ließ sich allerdings der Preis frei bestimmen - Foto: REUTERS/LASZLO BALOGH

FEATURED



SEEFAHRT

2018 soll erstes aut
Containerschiff star

Konsequenzen von Angriffen

rt-solutions.de

Abbildung als Kosten-Risiko

- **Negative Publicity**
- **Betrug durch Angriffe**
  - Abhängig von App-Funktionalität
- **Nach dem Launch / im Live-Betrieb**
  - Behebung deutlich schwieriger als vorher
  - Beeinträchtigung des laufenden Betriebs
  - Architektur-Änderungen kaum möglich
- **Missbrauch personenbezogener Daten**

Personenbezogene Daten

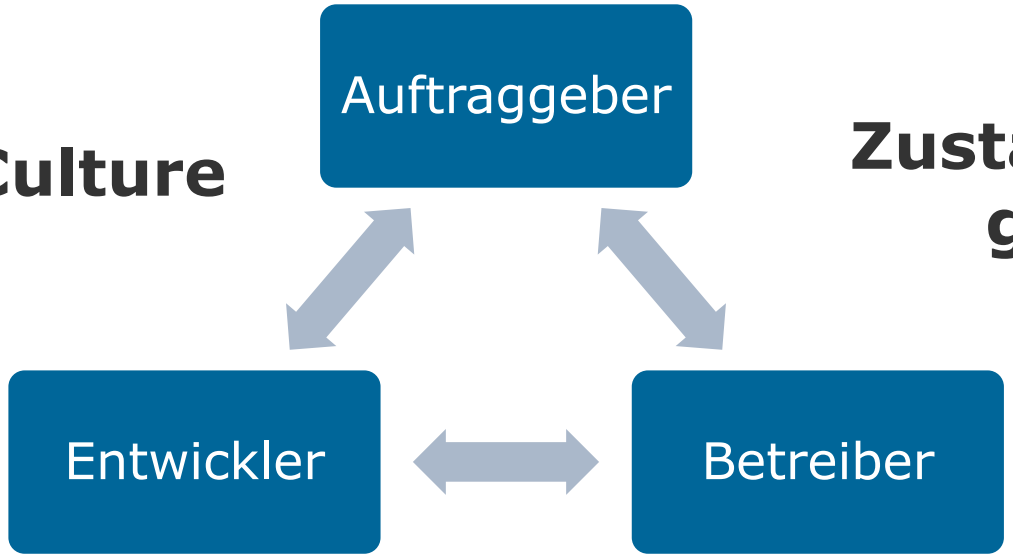
rt-solutions.de

- **Verantwortung immer beim Auftraggeber**
  - Pflicht zur Datenschutzeinhaltung
  - Haftbarkeit!
- **BDSG: §9 mit Anlage**
  - Mindestvorgaben für Datenschutz
  - Bußgelder bis 300.000 EUR
- **EU-Datenschutzverordnung (EU-DSGVO)**
  - Gültig ab Mai 2018
  - Bußgeld: 20 Mio EUR bzw. 4% Jahresumsatz
- **Erhebliches Geschäftsrisiko!**

Planung als Gesamtprojekt

rt-solutions.de

Corporate Culture



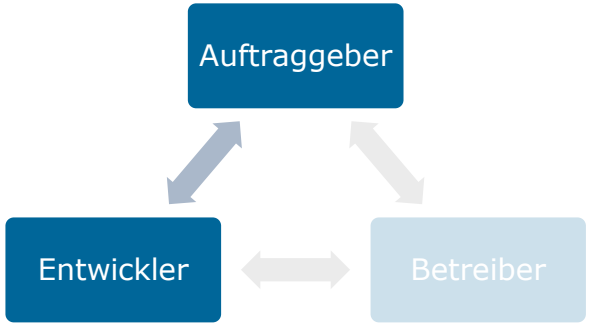
Zuständigkeits-grenzen

- **Aufteilung von Verantwortlichkeiten**
- **Vertragliche Regelungen zum Datenschutz**
- **Langfristige Wartung von App und Diensten**

Empfehlungen zur Umsetzung - App

rt-solutions.de

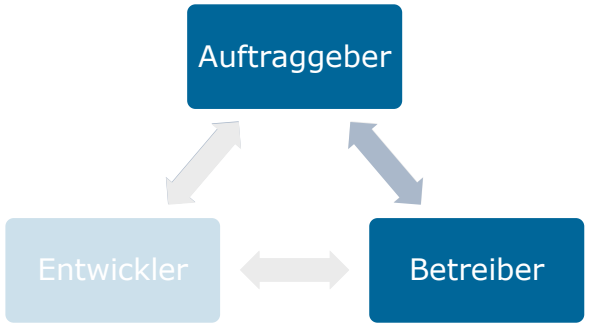
- **Prinzipielle Annahmen**
  - Endnutzer-Geräte nicht vertrauenswürdig!
  - Schnittstellen dauerhaft im Internet exponiert!



- **App- und Schnittstellen-Qualität**
  - Best Practices zur Software-Entwicklung
  - OWASP Top-10-Liste
  - App-Wartung durch Entwickler bzw. Übergabe
    - Betriebssystem-Änderungen, Bug-Fixes

Empfehlungen zur Umsetzung - Server

rt-solutions.de



- **Server-Betrieb und Wartung**
  - Monitoring
    - (Audit) Logging
    - Erkennung von Angriffen
  - Skalierung im Betrieb (Pokemon GO)
  - Administrativer Zugriff (Yahoo!)
    - 2-Faktor-Authentifizierung, Firewall-Zonen
  - Patch Management (WannaCry!)

Fazit

rt-solutions.de

- **App-Outsourcing kann funktionieren**
  - Konzept und Verantwortlichkeiten definieren
  - Standards für Code-Qualität und Sicherheit festschreiben
  - Nachhaltigen Betrieb von App und Server sicherstellen
  - Datenschutz beachten (lassen)

- **Unabhängigen Security-Audit des Gesamtsystems App+Service durchführen!**

Vielen Dank für Ihre Aufmerksamkeit!

rt-solutions.de
experts you can trust.

Dr. Georg Lukas
+49 (0)221 /93724-16
lukas@rt-solutions.de