scalable .CAPITAL

Regulated Workloads, Compliance and Security with AWS

a Fintech experience report

Dr. Andreas Schranzhofer
@Schranzhofer

Overview

- About Scalable Capital
- Regulation
- Requirements Analysis
- Options
- Conclusion
- Q&A

Scalable Capital - the Company

- Europe’s fastest growing **Digital Wealth Manager**
- Authorised financial institute in Germany and the UK
    - authorisations from BaFin and FCA
- Started in 2014, operating in Germany and the UK
    - offices in Munich and London
    - Go-Live DE: January 2016
    - Go-Live UK: August 2016
- > EUR 230m Assets under Management
- 100% cloud based, from Day 1

Scalable Capital - the Product

- Globally diversified ETF-Portfolio
- Risk managed
    - risk target is part of client mandate
- Data driven, quantitative approach
- Monitoring and rebalancing to meet risk target
- Minimum investment EUR 10,000 all-in fee 0.75%
- Paperless, no wet signature, video identification (KYC)
    - all digital experience

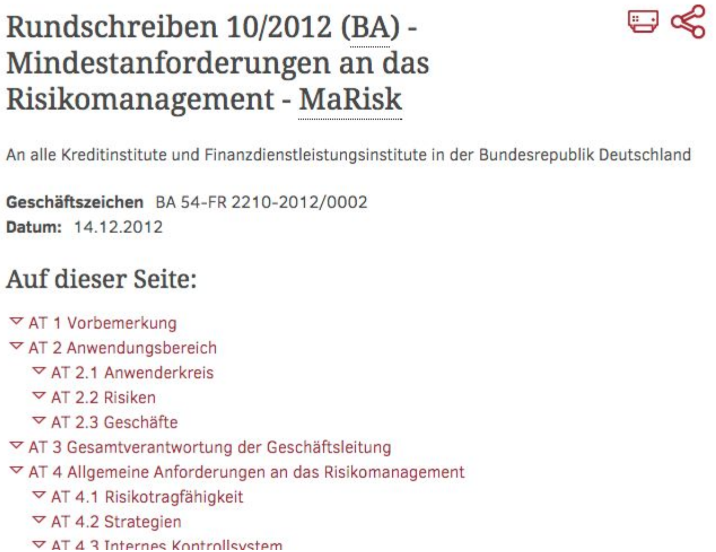
Regulation?

1. We strongly believe that it is essential for our Product
2. Regulation is a good thing

- Client Trust
- Business Model / Product
- Transparency

Regulation - DE

1. *Mindestanforderungen an das Risikomanagement* - **MaRisk**
2. *Bankaufsichtliche Anforderungen an die IT* - **BAIT**
3. As part of any application, the IT System will be scrutinized accordingly

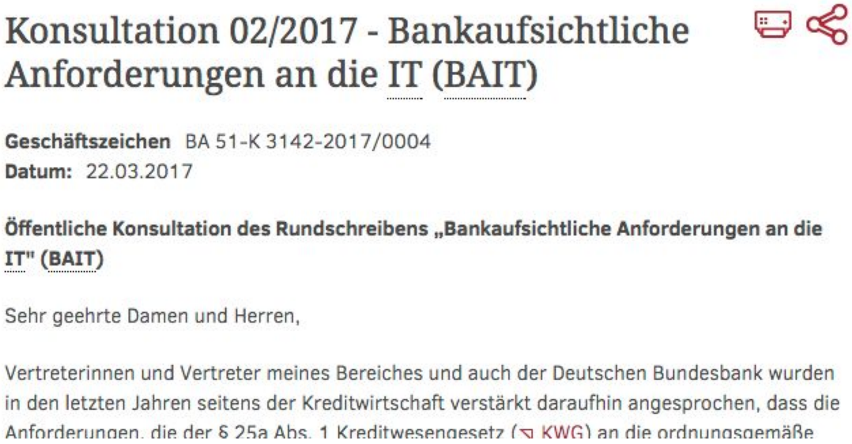


Rundschreiben 10/2012 (BA) - Mindestanforderungen an das Risikomanagement - MaRisk

An alle Kreditinstitute und Finanzdienstleistungsinstitute in der Bundesrepublik Deutschland

Geschäftszeichen BA 54-FR 2210-2012/0002
Datum: 14.12.2012

Auf dieser Seite:



Konsultation 02/2017 - Bankaufsichtliche Anforderungen an die IT (BAIT)

Geschäftszeichen BA 51-K 3142-2017/0004
Datum: 22.03.2017

Öffentliche Konsultation des Rundschreibens „Bankaufsichtliche Anforderungen an die IT" (BAIT)

Sehr geehrte Damen und Herren,

Vertreterinnen und Vertreter meines Bereiches und auch der Deutschen Bundesbank wurden in den letzten Jahren seitens der Kreditwirtschaft verstärkt daraufhin angesprochen, dass die Anforderungen, die der § 25a Abs. 1 Kreditwesengesetz (↘ KWG) an die ordnungsgemäße

Requirements - regulatory

security

disaster recovery

data availability

data privacy / locality

business continuity

data integrity

compliance

audit

staff qualification

data confidentiality

permissions vetting

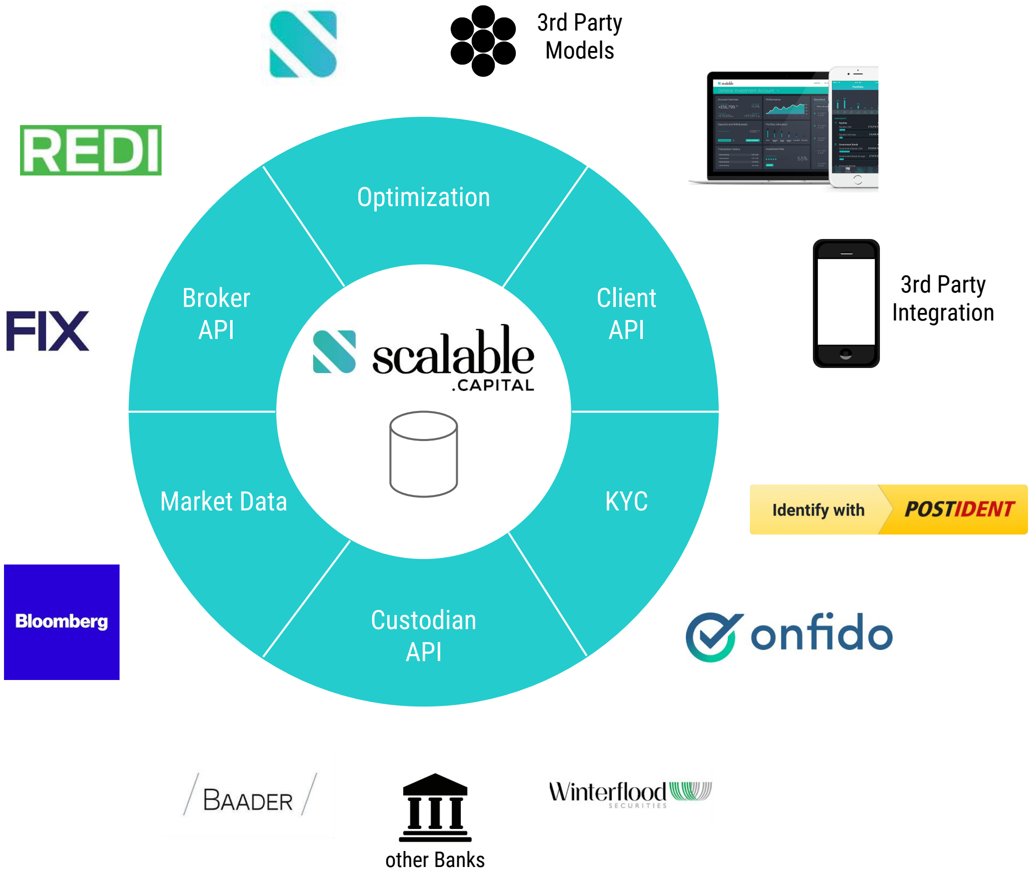
encryption

Requirements (non-regulatory)

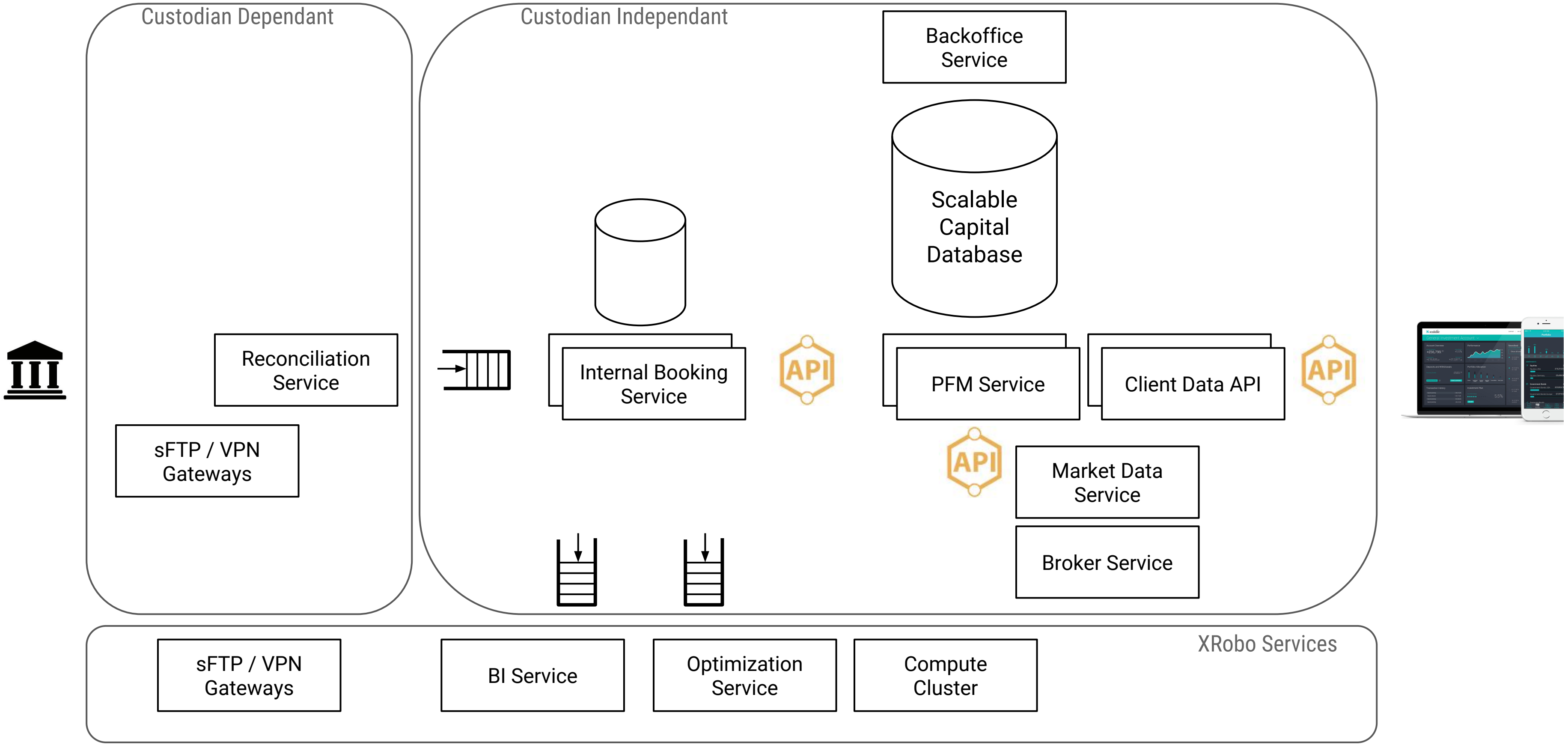
- System complexity
  - Multi-country, multi-currency, multi-bank setup
  - 3rd party data sources
- Computational load
  - Analyse 1000’s of portfolios daily
  - (Handle millions of API requests)
- Scalable to support strategic goals
  - Becoming Europe’s biggest Digital Wealth Manager
- Engineering organization
  - Flexibility on stack and process
  - Resource efficient

System Architecture

- Microservice architecture
- Independent actors
- Well-defined contracts
- Data abstraction layers
- 100% cloud based
- Fully automated delivery



System Architecture



Custodian Dependant

Reconciliation Service

sFTP / VPN Gateways

Custodian Independant

Backoffice Service

Scalable Capital Database

Internal Booking Service

API

PFM Service

Client Data API

API

API

Market Data Service

Broker Service

XRobo Services

sFTP / VPN Gateways

BI Service

Optimization Service

Compute Cluster

Requirements - regulatory

security

disaster recovery

data availability

business continuity

data privacy / locality

data integrity

compliance

audit

staff qualification

data confidentiality

encryption

permissions vetting

Security

- In a secure system, you can provide
  - Data integrity, availability, authenticity and confidentiality (MaRisk AT 7.2)
- Usage of established standards
- Regularly tested and challenged
- Staff training
- Permission vetting process
- but also
  - Software / Change Management Process
  - Operations
  - …

Security is not a feature one can add, it is a process, executed relentlessly

Disaster Recovery / Business Continuity

- Contingency Plan, Business Continuity and recovery plans (MaRisk AT 7.3)
- How can time critical operations continue in case of an emergency
- How can the business recover and return to “normal” operations
- Whom and how to contact
- Regularly tested, refined and assessed

Data privacy / locality

- Personal / high sensitive data
- Required for business operations
- Data privacy laws in different jurisdictions
  - Safe Harbour / Privacy Shield
- Access rights for the authorities

Options

- We didn’t know everything back in 2014
- But we knew that, known unknowns can be managed

1. Outsource to an agency / provider
2. Build / host your own infrastructure
3. Somehow mix it

Options

1. Outsource to an agency / provider
    a. not compatible with company strategy

2. Build / host your own infrastructure
    a. 2 Countries
    b. Disaster Recovery, Business Continuity
    c. Scaling? keeping systems up to date
    d. …
    e. Cost and time to build is prohibitive

Somehow mix it

- This is where Cloud Services come into play

1. Rent Infrastructure and/or Services
2. Deploy your application on dedicated servers
3. If required, have full control of all your servers, databases etc.
4. Otherwise, use plug & play services
5. **Build your application, not (a) datacenter(s)**

Amazon Web Services (AWS) - is it a match?

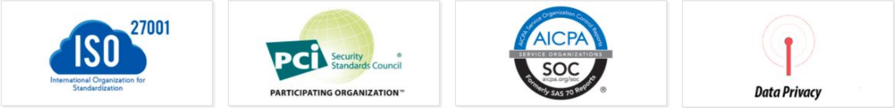
- System complexity
  - Adding instances, services, nodes, networks
- Computational load
  - Virtually infinite resources, from our perspective
- Scalable to support strategic goals
  - Availability zones (AZs) around the globe
  - Virtually infinite resources
- Engineering organization
  - Full control of servers where required
  - Services in line with our stack and process (CI/CD)
  - Engineers can focus on the application
  - Infrastructure as code

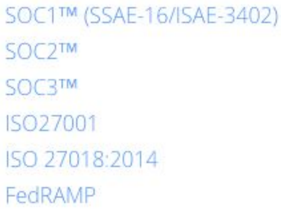
Amazon Web Services (AWS) - is it a match?

- Security
  - Up-to-date appliances
  - AWS WAF - Web Application Firewall
  - Amazon Virtual Private Cloud (VPC)
  - AWS CloudTrail
  - AWS CloudWatch
  - Managed NAT Gateways
- Disaster Recovery / Business Continuity
  - Multiple AZs
- Permission Vetting
  - AWS Identity and Access Management (IAM) - fine granular permissioning system
- Data privacy / locality
  - AZs around the globe
  - Most importantly, Frankfurt and Dublin with at least 2 AZs

Security

- AWS setup
  - ISO 27001
  - PCI ...
- Docker Images
- Regularly tested by external testers
  - App and Penetration Testing by Cognosec
    - QSA - Qualified Security Assessor by PCI
    - ASV - Approved Scanning Vendor by PCI
- Network Setup / Rules

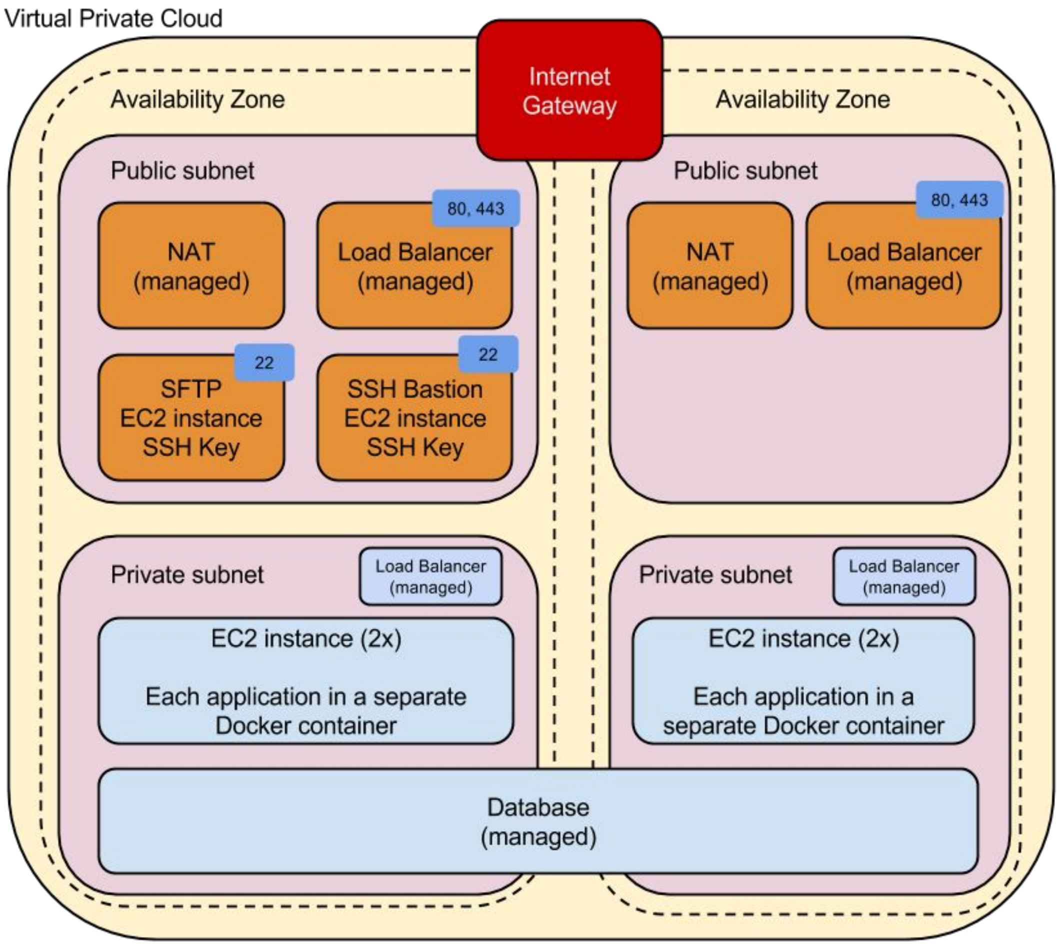

ISO 27001
International Organization for Standardization
PCI Security Standards Council
PARTICIPATING ORGANIZATION™
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports
Data Privacy



SOC1™ (SSAE-16/ISAE-3402)
SOC2™
SOC3™
ISO27001
ISO 27018:2014
FedRAMP

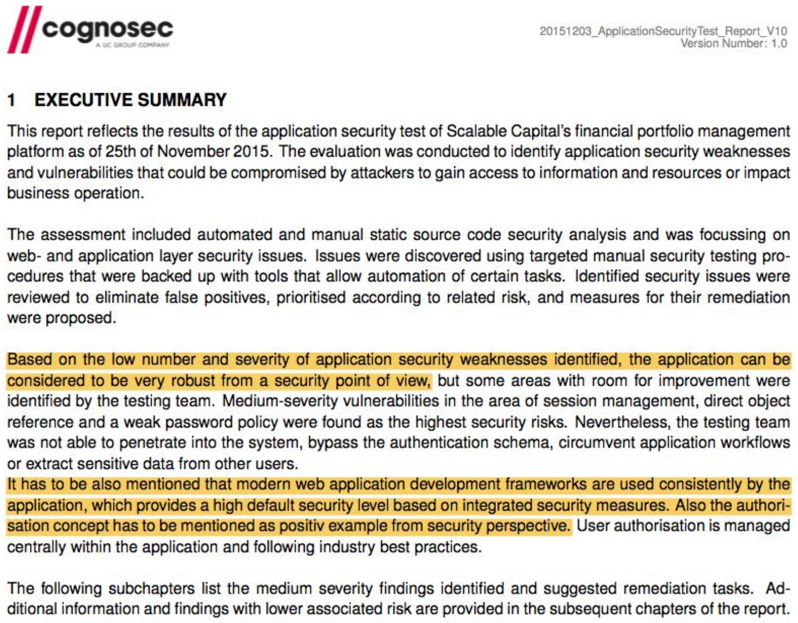
Network / Availability

- Intrusion
  - Access control
  - Minimal exposure
  - Specific gateways
- Availability
  - Redundant setup
  - Multi AZ setup
  - Frankfurt: 2 AZ
  - Dublin: 3 AZ
  - Load balancer setup
- Data Loss
  - Backup
  - Infrastructure as Code
    - for easy recovery



Assessment

- App and Penetration Testing by Cognosec
  - QSA - Qualified Security Assessor by PCI
  - ASV - Approved Scanning Vendor by PCI
- AWS Cloud Setup
  - ISO 27001, PCI Compliant, …
- Secure Software Development Process
  - Code Reviews
  - OWASP Top 10 checks
- Secure Organizational Setup
  - Employee education
  - Operations (2FA Authentication, Encryption)
- being active in the community
  - Talks, conferences, ...



//cognosec
A UC GROUP COMPANY

20151203_ApplicationSecurityTest_Report_V10
Version Number: 1.0

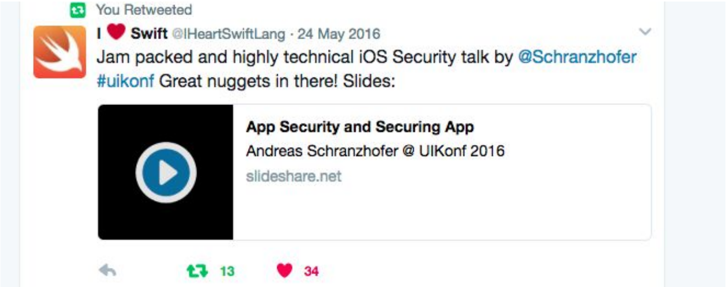
1 EXECUTIVE SUMMARY

This report reflects the results of the application security test of Scalable Capital's financial portfolio management platform as of 25th of November 2015. The evaluation was conducted to identify application security weaknesses and vulnerabilities that could be compromised by attackers to gain access to information and resources or impact business operation.

The assessment included automated and manual static source code security analysis and was focussing on web- and application layer security issues. Issues were discovered using targeted manual security testing procedures that were backed up with tools that allow automation of certain tasks. Identified security issues were reviewed to eliminate false positives, prioritised according to related risk, and measures for their remediation were proposed.

Based on the low number and severity of application security weaknesses identified, the application can be considered to be very robust from a security point of view, but some areas with room for improvement were identified by the testing team. Medium-severity vulnerabilities in the area of session management, direct object reference and a weak password policy were found as the highest security risks. Nevertheless, the testing team was not able to penetrate into the system, bypass the authentication schema, circumvent application workflows or extract sensitive data from other users.
It has to be also mentioned that modern web application development frameworks are used consistently by the application, which provides a high default security level based on integrated security measures. Also the authorisation concept has to be mentioned as positiv example from security perspective. User authorisation is managed centrally within the application and following industry best practices.

The following subchapters list the medium severity findings identified and suggested remediation tasks. Additional information and findings with lower associated risk are provided in the subsequent chapters of the report.



You Retweeted

I ♥ Swift @IHeartSwiftLang · 24 May 2016

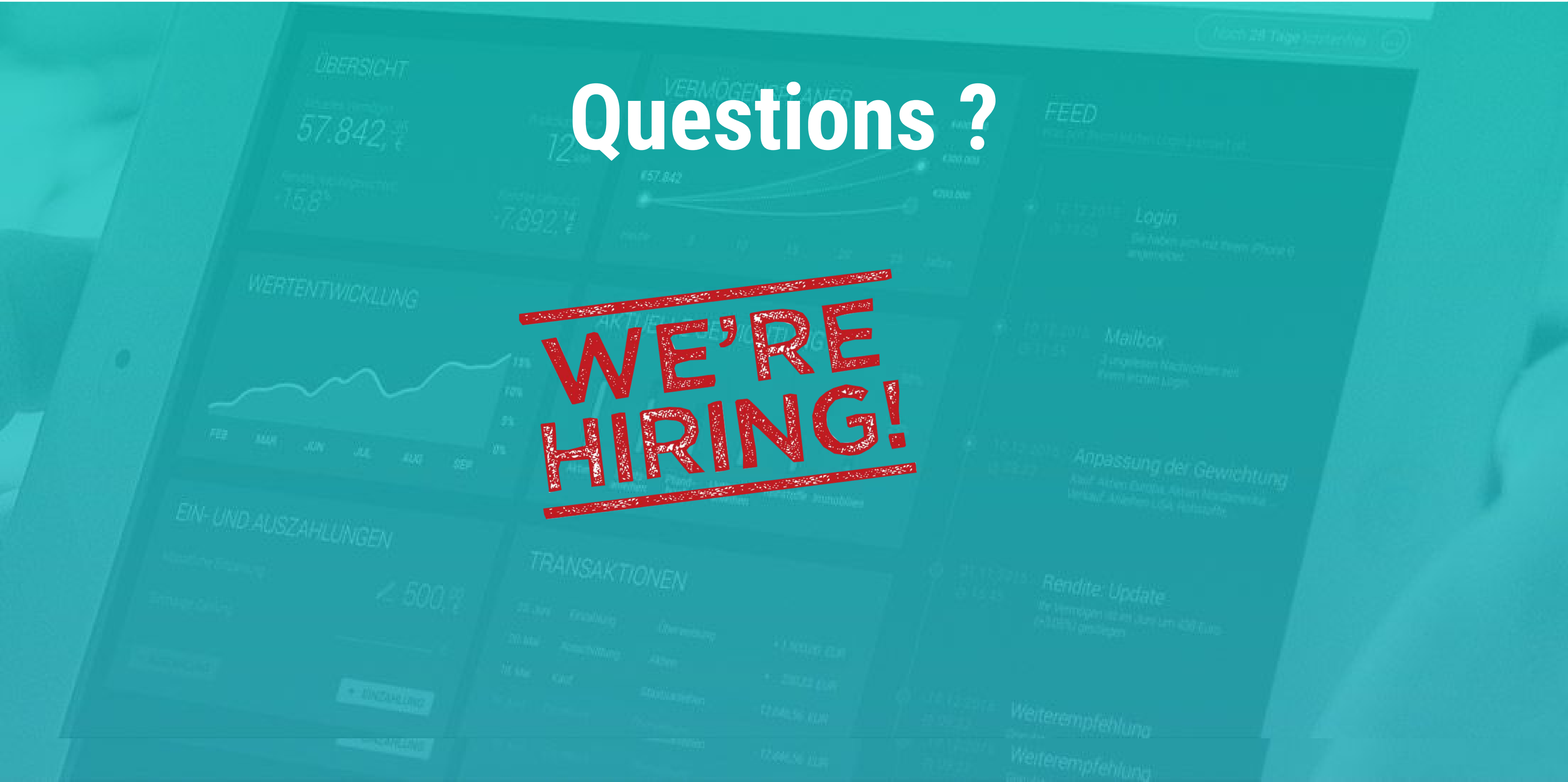
Jam packed and highly technical iOS Security talk by @Schranzhofer #uikonf Great nuggets in there! Slides:

App Security and Securing App
Andreas Schranzhofer @ UIKonf 2016
slideshare.net

Conclusion

- Amazon Web Services is a good fit to execute regulated workloads
  - Regions worldwide
  - Availability Zones
  - Standardized services
- Allowed us to focus on our business applications
- small Start-Up, back in 2014 and today
  - Building this ourselves would have been prohibitive
- New services all the time - play time.

Questions ?



WE'RE HIRING!