Threat Modelling als Ausgangspunkt für sichere SW-Entwicklung

Roland Brethauer, SAP SE

Juni 2018

… über den Vortragenden

Roland Brethauer

- ein Berufsleben lang IT:
- als Entwickler, Berater, Projektleiter, Manager, …
- seit 8 Jahren Koordinator für Security-Aktivitäten
- ehrenamtlicher FIRST Lego®League-Coach/-Jury

FIRST
FOR INSPIRATION & RECOGNITION OF SCIENCE & TECHNOLOGY

Die Herausforderung:

Gefährliches Gießkannenprinzip

IT-Security-Budgets - am Bedarf vorbei investiert

Unternehmen wissen nicht, welche Daten besonders schützenswert sind. Sie investieren deshalb zu wenig zielgerichtet in IT-Sicherheit. Die Folge: Hohe Ausgaben, wenig Erfolg.

Quelle: www.computerwoche.de/a/it-security-budgets-am-bedarf-vorbei-investiert,3227385

Threat Modelling …

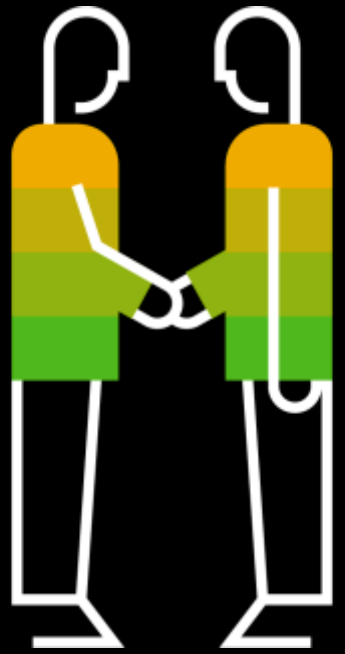
Praxis

Beispiel

Einführung

- **… eine Einführung**
- … ein konkretes, einfaches Beispiel
- … einige Erfahrungen aus der Praxis
- … Ihre Fragen, Erfahrungen & Meinungen

Threat Modelling bei SAP …



- ist eine strukturierte Methode zum Identifizieren von Bedrohungen und daraus abgeleiteten Sicherheitsanforderungen im Kontext bestimmter Angriffsszenarien.
- wird genutzt während der „Design Time“ der Architektur der Anwendung.
- ermöglicht eine Priorisierung der sicherheitsbezogenen Anforderungen und ein nachvollziehbares Risikomanagement.

Begrifflichkeiten…

- Assets →Schützenswerte Güter
- Threat →Bedrohung
- Vulnerability →Sicherheitslücke
- Attack →Angriff
- Countermeasure →Gegenmaßnahme

Schritt für Schritt …

Praxis

Beispiel

Einführung

Threat Modelling …

Praxis

Beispiel

Einführung

OWASP Secure Software Development Lifecycle Project(S-SDLC)

OWASP Secure Software Development Life Cycle Project(S-SDLC) is an overall security software methodology for Web and APP developers.

www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project

The OWASP Threat Model Project

This is a documentation project. We provide information on threat modeling techniques for web and cloud, with a focus on current and emerging techniques.

www.owasp.org/index.php/OWASP_Threat_Model_Project

www.owasp.org/index.php/Threat_Modeling_Cheat_Sheet

https://twitter.com/owasp_cloudsec

https://speakerdeck.com/zeroxten/threat-modeling-the-ultimate-devsecops

Threat Modelling …

Praxis

Beispiel

Einführung

The Secure Software Development Lifecycle at SAP

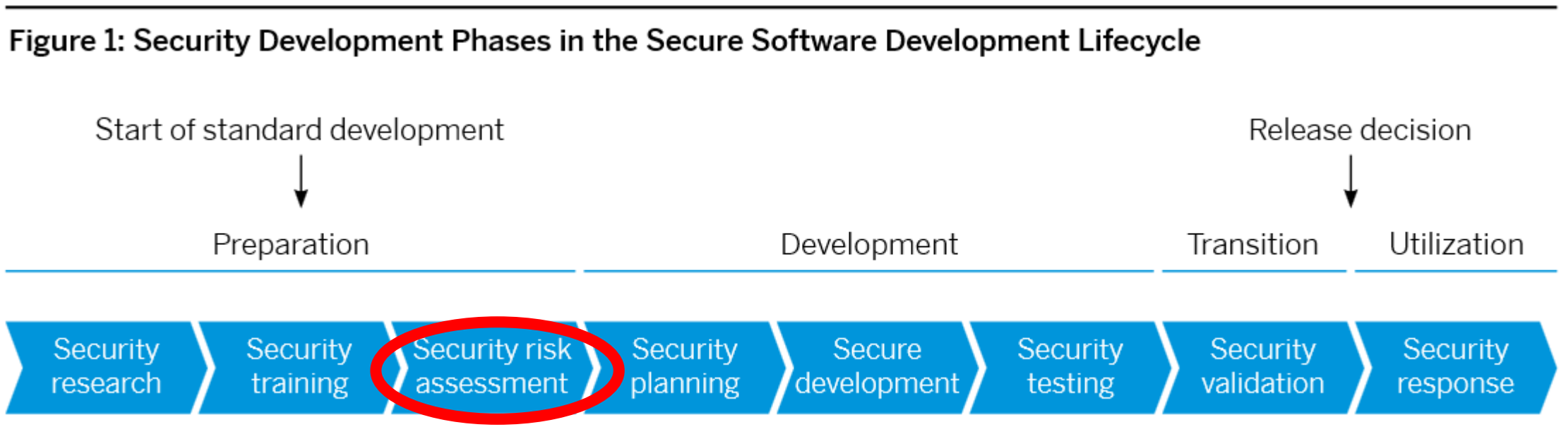


Figure 1: Security Development Phases in the Secure Software Development Lifecycle

Quelle: https://www.sap.com/documents/2016/03/a248a699-627c-0010-82c7-eda71af511fa.html

Threat Modelling …

Praxis

Beispiel

Einführung

Microsoft Store Products

Security Development Lifecycle

1. TRAINING	2. REQUIREMENTS	3. DESIGN	4. IMPLEMENTATION	5. VERIFICATION	6. RELEASE	7. RESPONSE
1. Core Security Training	2. Establish Security Requirements	5. Establish Design Requirements	8. Use Approved Tools	11. Perform Dynamic Analysis	14. Create an Incident Response Plan	Execute Incident Response Plan
	3. Create Quality Gates/Bug Bars	6. Perform Attack Surface Analysis/ Reduction	9. Deprecate Unsafe Functions	12. Perform Fuzz Testing	15. Conduct Final Security Review	
	4. Perform Security and Privacy Risk Assessments	7. Use Threat Modeling	10. Perform Static Analysis	13. Conduct Attack Surface Review	16. Certify Release and Archive	

Quelle: https://www.microsoft.com/en-us/sdl/process/training.aspx

Threat Modelling …

Praxis

Beispiel

Einführung

- … eine Einführung
- **… ein einfaches Beispiel**
- … einige Erfahrungen aus der Praxis
- … Ihre Fragen, Erfahrungen & Meinungen

Beispiel - mobiles Kundenstammblatt

Das Kundenstammblatt ermöglicht dem Außendienst den unmittelbaren Zugriff auf Informationen über einen Kunden mit dessen wichtigsten Eckdaten und aktuellen Aktivitäten. Das Kundestammblatt ist auch offline auf mobilen Endgeräten verfügbar.

Praxis
Beispiel
Einführung

Mögliche schützenswerte Güter

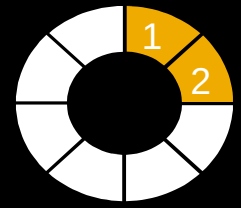
- Daten im Backend
- Mobile Daten, Kundenstammblatt
- Verfügbarkeit des Services
- CPU Last des Servers
- …

Praxis

Beispiel

Einführung

Geeignetes Architekturmodell

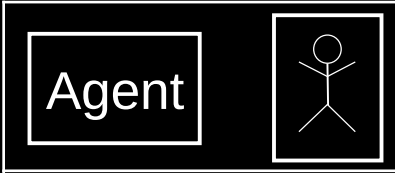
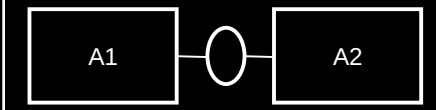


Praxis

Beispiel

Einführung

- Gezielt vereinfacht
- Modelliert mit „Fundamental Modelling Concepts“ (FMC)
- Kennzeichnung von „Trust Boundaries“

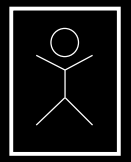
	**Agenten** verarbeiten Information, nutzen Speicher, kommunizieren über Kanäle
	**Speicher** enthalten Informationen, auf die Agenten zugreifen
	**Kanäle** werden von Agenten genutzt um Informationen zu transportieren

Grob vereinfachte Architektur

Praxis

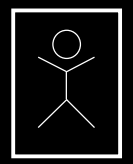
Beispiel

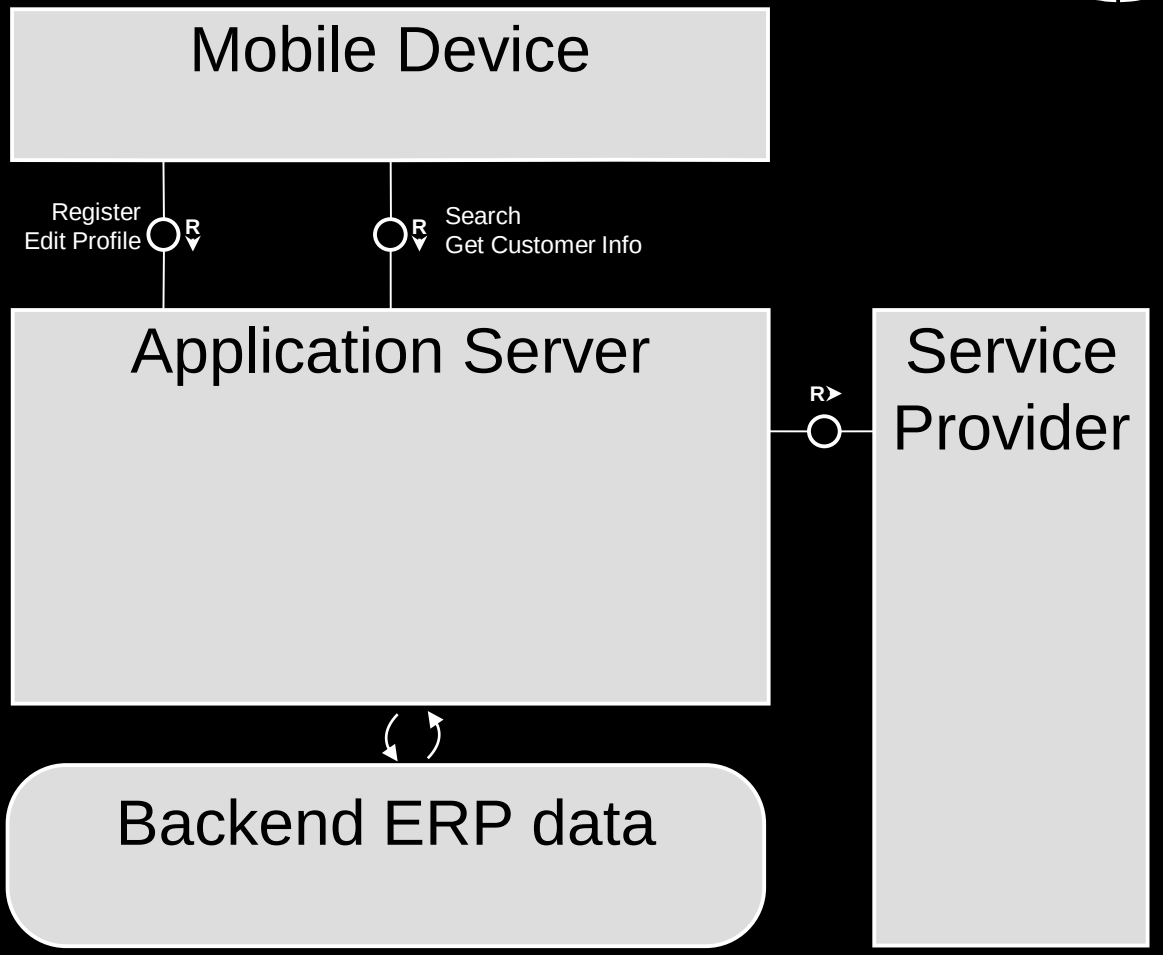
Einführung



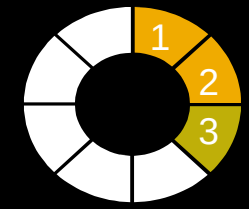
Sales

Admin





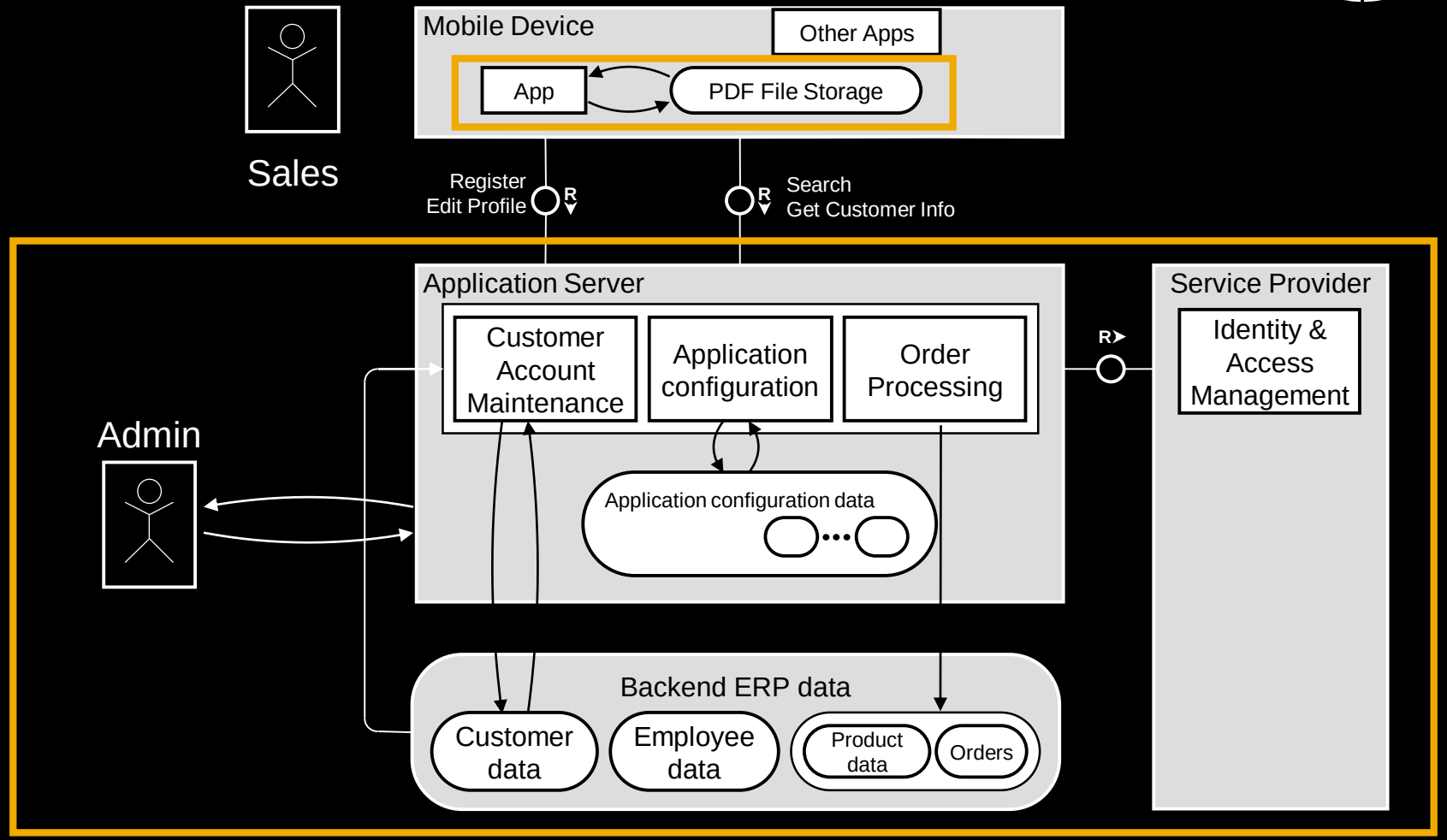
Wichtige Komponenten



Praxis

Beispiel

Einführung



Gefahrenpunkte identifizieren

Praxis

Beispiel

Einführung

Methodenvielfalt

- Offen
  - Brainstorming
  - Worst Case Szenario
- Geführt
  - OWASP Top 10, STRIDE, …
  - Firmenspezifische Checkliste: gesammelte Erfahrung

Was ist STRIDE?

Praxis

Beispiel

Einführung

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of Priviledges

Gefahrenpunkte dokumentieren

Praxis

Beispiel

Einführung

Beschreibung: Externer Zugriff (Vertrieb) sollen über Verfahren ***x***, interner Zugriff (Admin, DevOps) über Verfahren ***y*** erfolgen. Anhand des genutzten Verfahrens ***x*** oder ***y*** werden auch die Berechtigungen vorsortiert.

Konkrete Bedrohung: Eine fehlerhafte Zuordnung des Verfahrens gefährdet die Vertraulichkeit und Integrität der Daten.

Risiken bewerten

Praxis

Beispiel

Einführung

Bewertungskriterien:

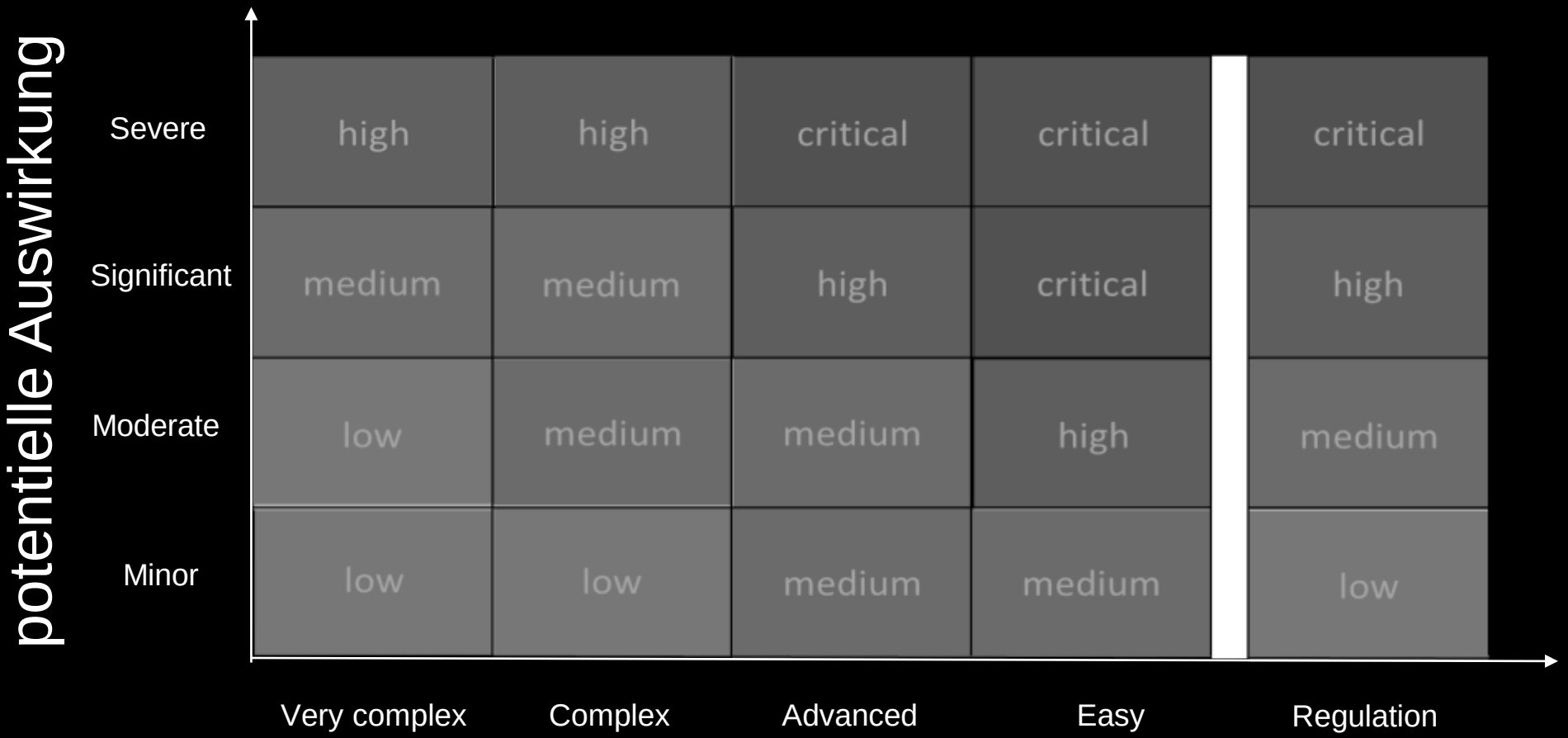
- Komplexität des Angriffs
- Potentielle Auswirkungen

Risiken bewerten

Praxis

Beispiel

Einführung



Risiken bewerten

Praxis

Beispiel

Einführung

Gefahrenpunkt „Zugriff“:

- Komplexität des Angriffs: Komplex
  - Voraussetzung: Legitimierter Zugriff als Nutzer
  - Angriffspfad: Fehlerhafte Konfiguration für Administratoren (zufällig oder absichtlich)
- Potentielle Auswirkung: Signifikant
  - Vertraulichkeit der Daten
  - Integrität der Daten

Risiken bewerten

Praxis

Beispiel

Einführung

potentielle Auswirkung

	Very complex	Complex	Advanced	Easy	Regulation
Severe	high	high	critical	critical	critical
Significant	medium	medium	high	critical	high
Moderate	low	medium	medium	high	medium
Minor	low	low	medium	medium	low

Komplexität des Angriffs

Gegenmaßnahmen erarbeiten

Praxis

Beispiel

Einführung

Gefahrenpunkt „Zugriff“:

- Mögliche Gegenmaßnahmen

$$
- Separate Programme zur Prüfung der Konfiguration: Health Checks & Controls

$
- Automatisierte Überwachung dieser „Health Checks & Controls“ im Betrieb

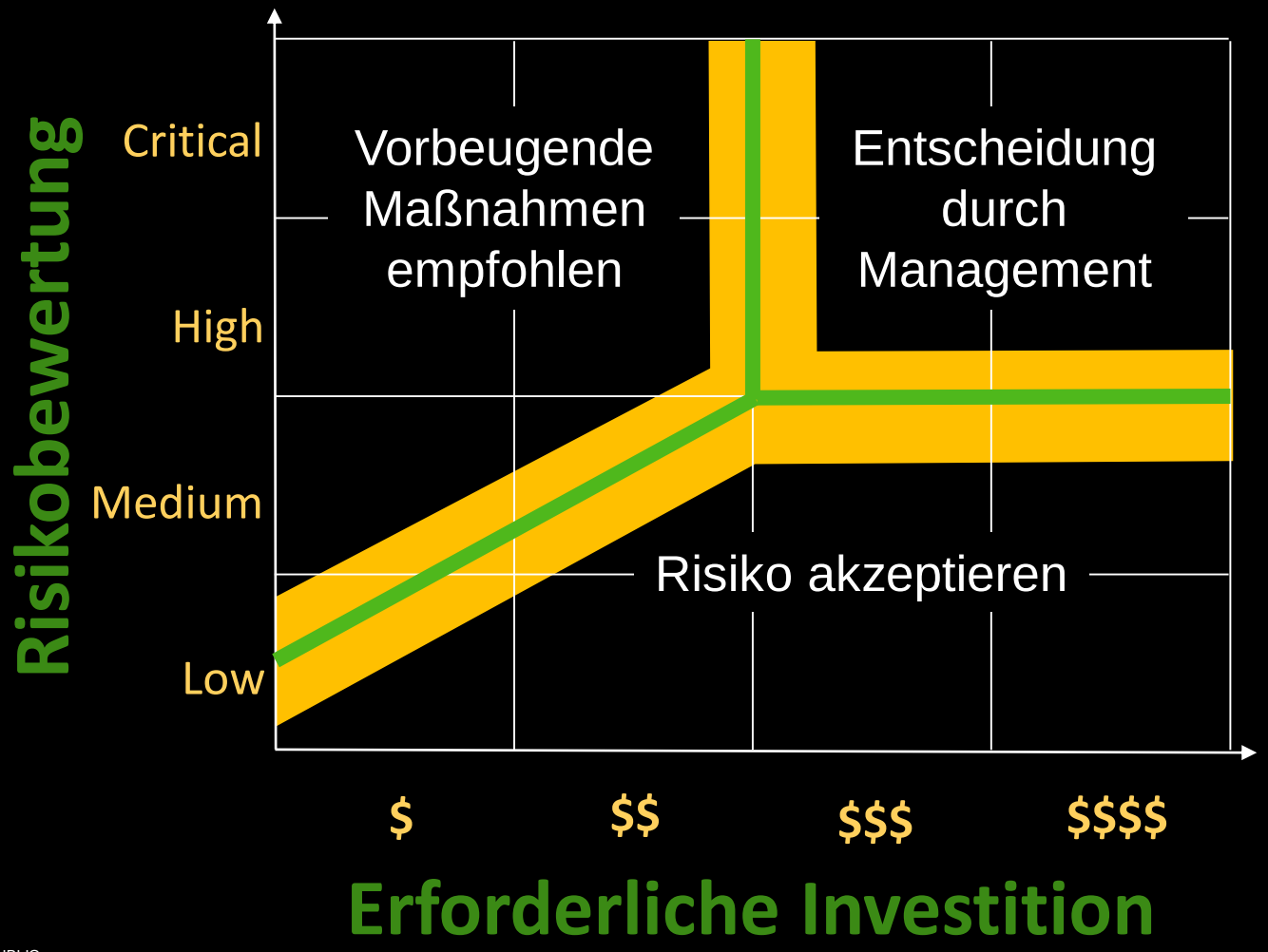
$
- Manipulationssichere Protokollierung aller Konfigurationsänderungen der Zugriffskontrollsysteme
- …

Daumenregel zum Priorisieren

Praxis

Beispiel

Einführung



Ergebnisse eines Workshops

Praxis

Beispiel

Einführung

- Identifizierte Gefahrenpunkte
- Security-Anforderungen im Backlog
- Vorschläge für gezielte Testen
- Ansatzpunkte für effizientes Code-Audit
- Erhöhte Fachkompetenz im Team

➔ **TM ist kein Audit!**

Threat Modelling …

Praxis

Beispiel

Einführung

- … eine Einführung
- … ein konkretes, einfaches Beispiel
- **… einige Erfahrungen aus der Praxis**
- … Ihre Fragen, Erfahrungen & Meinungen

Threat Modelling-Workshop: Setup

Praxis

Beispiel

Einführung

- Bis zu 8 Teilnehmer: Architekt, Entwickler, Product-Owner, Security Experte, (Operations), Moderator(en)
- Bis zu 3 Treffen á 3-4h + Auswertung
- Ergebnis und Annahmen unmittelbar dokumentieren
- Optionaler Fast-Track bei geeigneten Rahmenbedingungen

Einführung von Threat Modelling …

- Einfach anfangen
- Schlank halten
- Erfahrung sammeln, Methodik anpassen

- … später: Formalisierung, Anbindung an Risiko-Management , ISO 9001 / 27034

Praxis

Beispiel

Einführung

Erfolgsfaktor: eigene „Best Practise“ Liste

Praxis

Beispiel

Einführung

Die auf den eigenen Rahmen zugeschnittene „Best Practise“ Frageliste ist ein Erfolgs- und Akzeptanzfaktor.

Eine Feedbackschleife auf die Frageliste muss im Prozess vorgesehen sein!

Lebenszyklus berücksichtigen

Risiken liegen nicht nur in der Softwareentwicklung, sondern auch in

- Software Deployment
- Wartung & Korrektur
- Operations (DevOps!)
- Einbettung in bestehende IT-Infrastruktur
- …

Bedrohung weit denken …

- Angriff über Dienstleister
- Angriff über Software Supply Chain
- Innentäter
- Missbrauch als Mining Platform (Apps)
- Neuer Use Case
- …

„Schwarze Schwäne“ nicht ignorieren …

Praxis

Beispiel

Einführung

potentielle Auswirkung

	Very complex	Complex	Advanced	Easy	Regulation
Severe		high	critical	critical	critical
Significant	medium	medium	high	critical	high
Moderate	low	medium	medium	high	medium
Minor	low	low	medium	medium	low

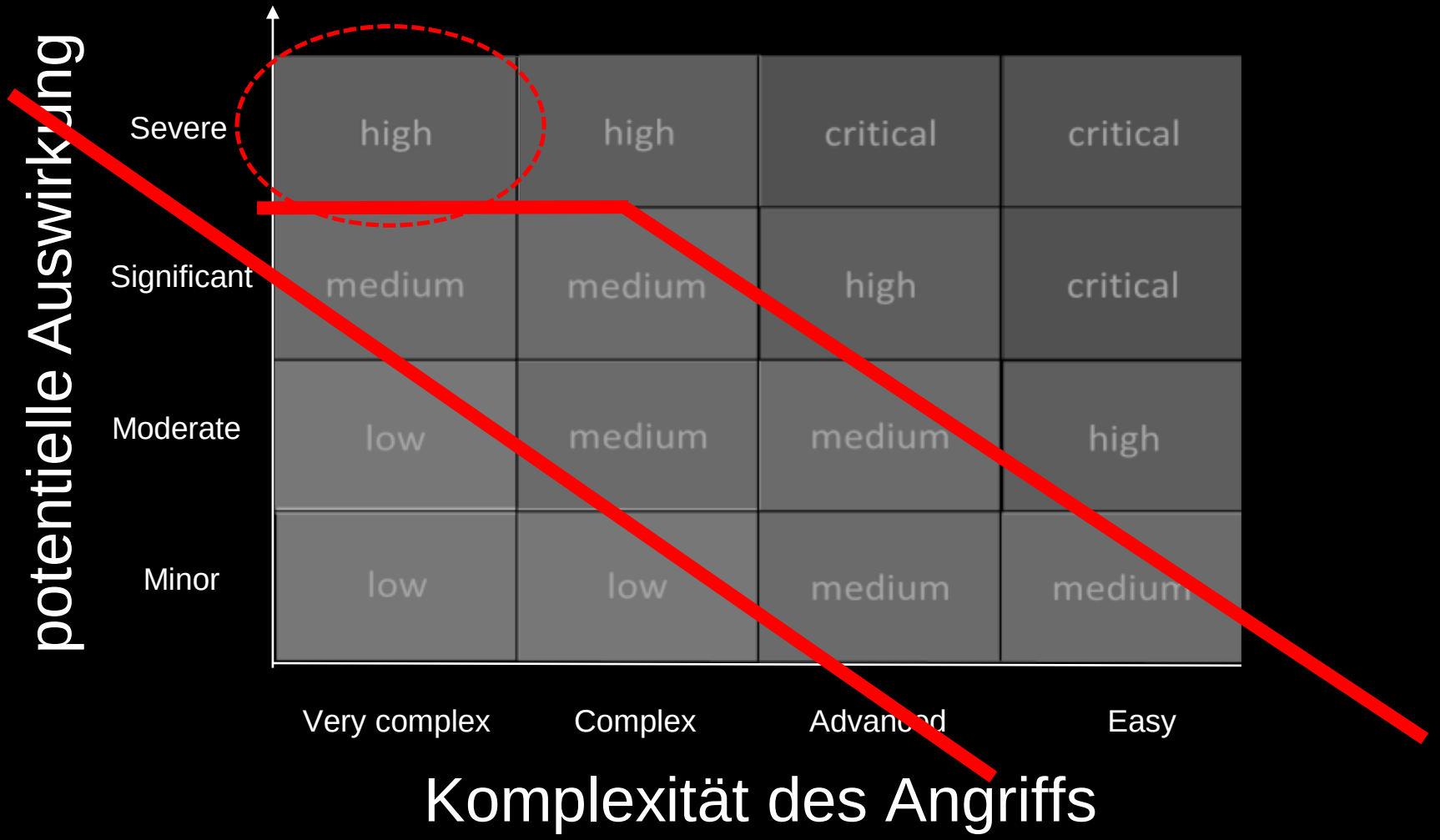
Komplexität des Angriffs

Abgeknickter Risikokorridor …

Praxis

Beispiel

Einführung



Akzeptierte Risiken

Akzeptierte Risiken mit einem Kontrollverfahren absichern.

Praxis

Beispiel

Einführung

Anregung: „Assume the breach“

Indikatoren für die Kompromittierung eines Systems/Services suchen oder künstlich einbauen.

Annahmen immer wieder Verifizieren

- Beispiel: Spectre & Meltdown

Threat Modelling …

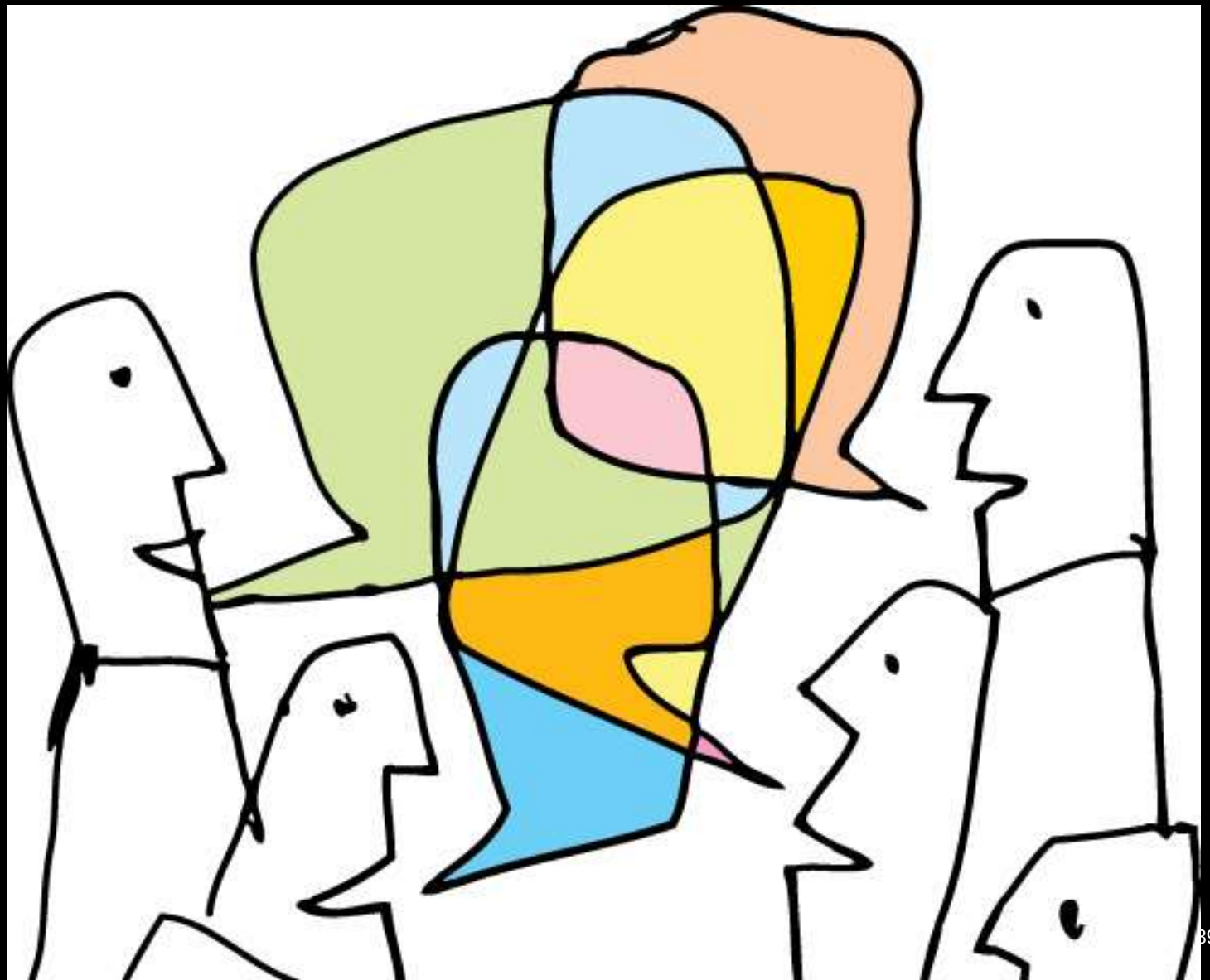
Praxis

Beispiel

Einführung

- … eine Einführung
- … ein konkretes, einfaches Beispiel
- … einige Erfahrungen aus der Praxis
- **… Ihre Fragen, Erfahrungen & Meinungen**

… Fragen & Meinungen



Vielen Dank.

Kontakt:

Roland Brethauer
M: roland.brethauer@sap.com

SAP Run Simple

Literatur

[FMC06] Knoepfel, Andreas; Groene, Bernhard; Tabeling, Peter; Fundamental Modelling Concepts: Effective Communication of IT Systems; Chichester; 2006 ; http://www.fmc-Modelling.org

[GUT12] Gutbrod, Roger; Wiele, Christian; The Software Dilemma – Balancing Creativity and Control on the Path to Sustainable Software; Heidelberg; 2012

[PMB17] PMI (Hrsg.); A Guide to the Project Management Body of Knowledge / Sixth Edition; Newton Square; 2017

[SAP16] SAP‘s Secure SDL: https://www.sap.com/documents/2016/03/a248a699-627c-0010-82c7-eda71af511fa.html

[SHO14] Shostack, Adam; Threat Modelling – designing for security; Indianapolis; 4. Auflage; 2014

[SOP08] Hampp, Tilmann; Knauß, Markus; Eine Untersuchung über Korrekturkosten von Software-Fehlern; 28(2), Gesellschaft für Informatik, ISSN 0720-8928, S. 7-12.

[TAB06] Tabaka, Jean; Collaboration explained; Addison-Wesley Professional; 2006

[TISP14] Secorvo GmbH (Hrsg.); Zentrale Bausteine der Informationssicherheit – Das Begleitbuch zum T.I.S.P.; Karlsruhe; 2. Auflage 2014

[VER03] Versteegen, Gerhard (Hrsg.); Risikomanagement in IT-Projekten; Berlin Heidelberg; 2003

© 2018 SAP SE or an SAP affiliate company. All rights reserved.

© 2018 SAP SE oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.