T.I.S.P. TeleTrusT Information Security Professional

TeleTrusT Pioneers in IT security.

T.I.S.P. Community Meeting

Berlin, 02. - 03.11.2015

„Secure Software Engineering“ in der Praxis

Andreas Poller

Fraunhofer Institut SIT, Darmstadt

What we need is to improve the software development process, so we can have some assurance that our software is secure […]. The key word here is "assurance."

Assurance is less about developing new security techniques than about using the ones we already have. It's all the things described in books on secure coding practices.

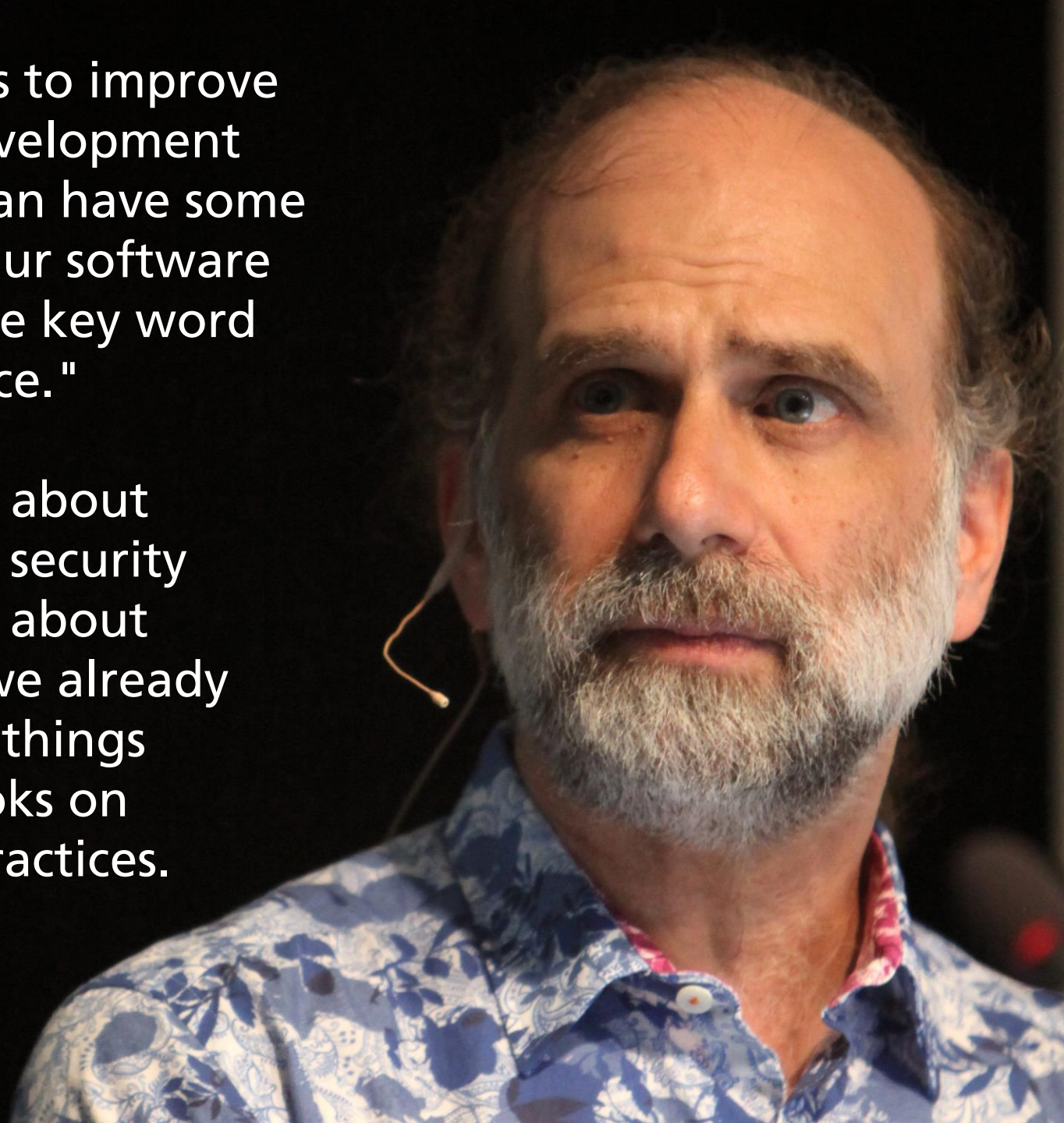
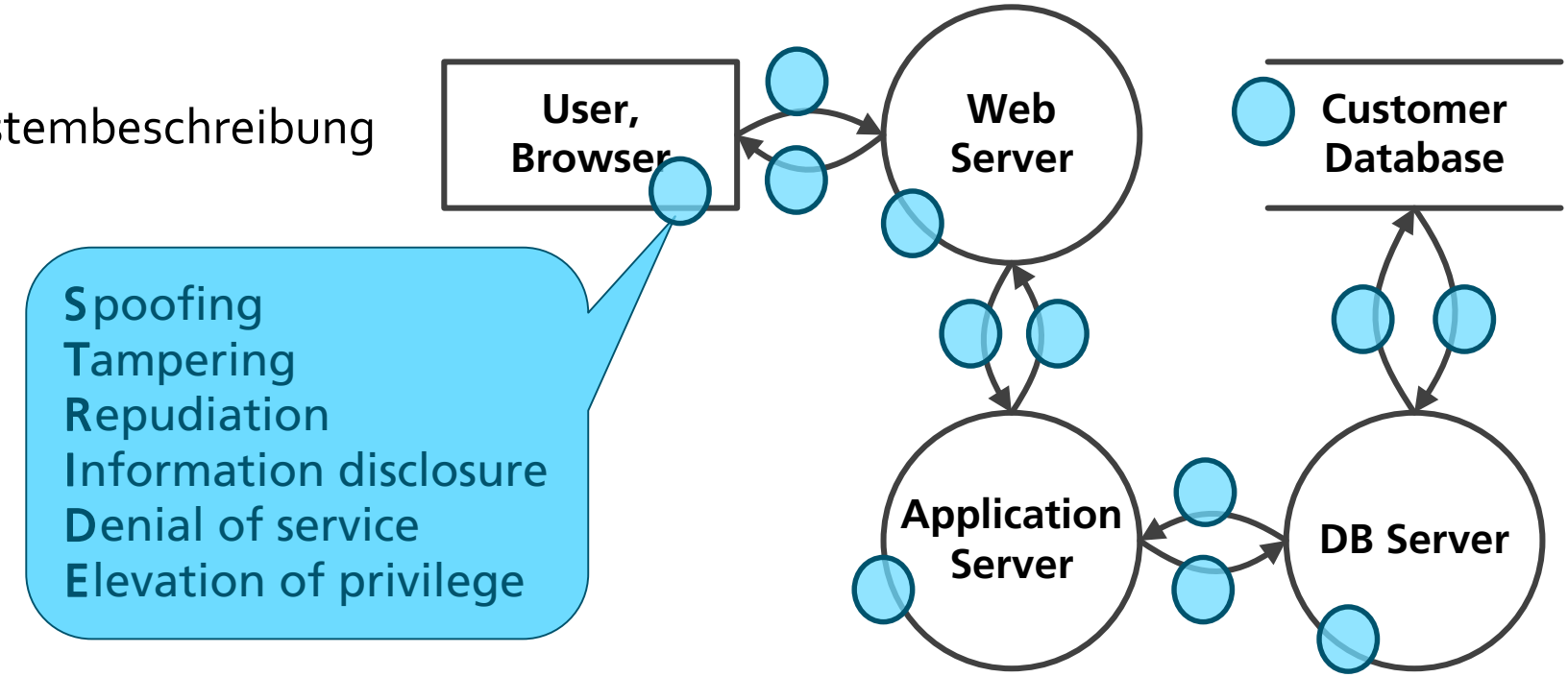


Image: Photograph by Rama, Wikimedia Commons, Cc-by-sa-2.0-fr
Source: schneier.com

Studie: Microsoft SDL Threat Modeling in der Praxis

MS SDL Threat Modeling

1. Systembeschreibung



2. Checkliste erstellen

3. Auswirkungen bewerten und Gegenmaßnahmen finden

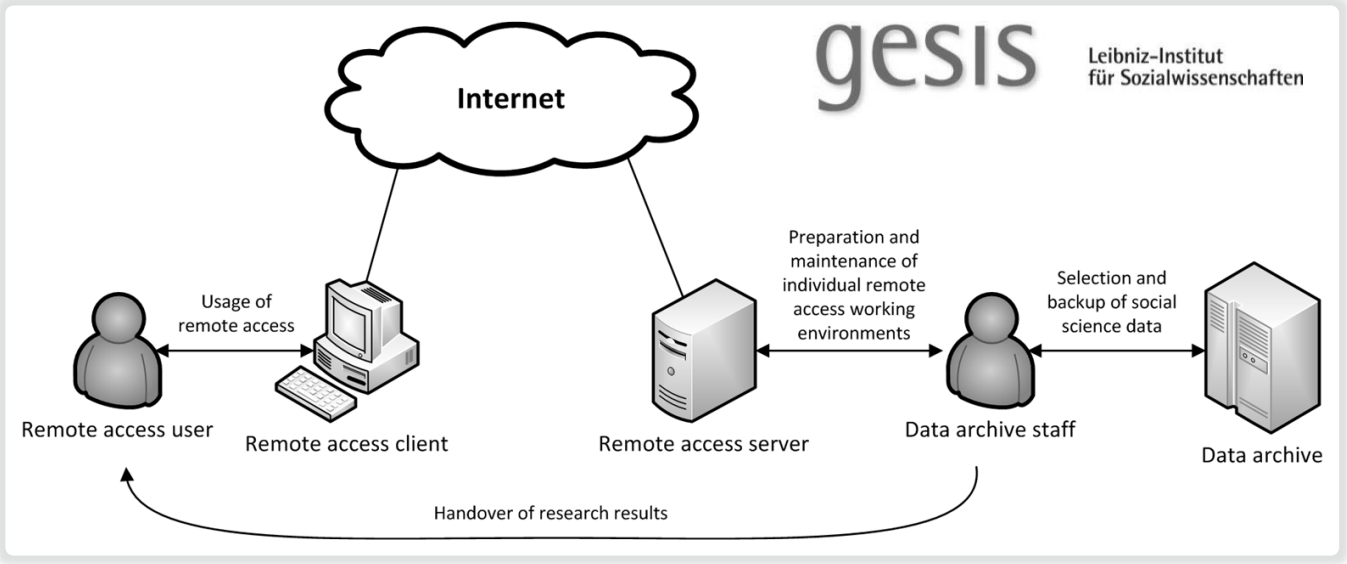
Forschungsdesign

IT-Dienstleister

Sozialwissen-
schaftler

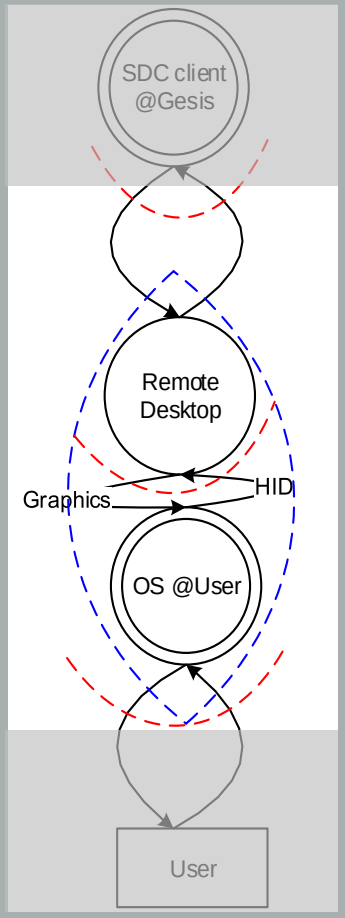
Informatiker

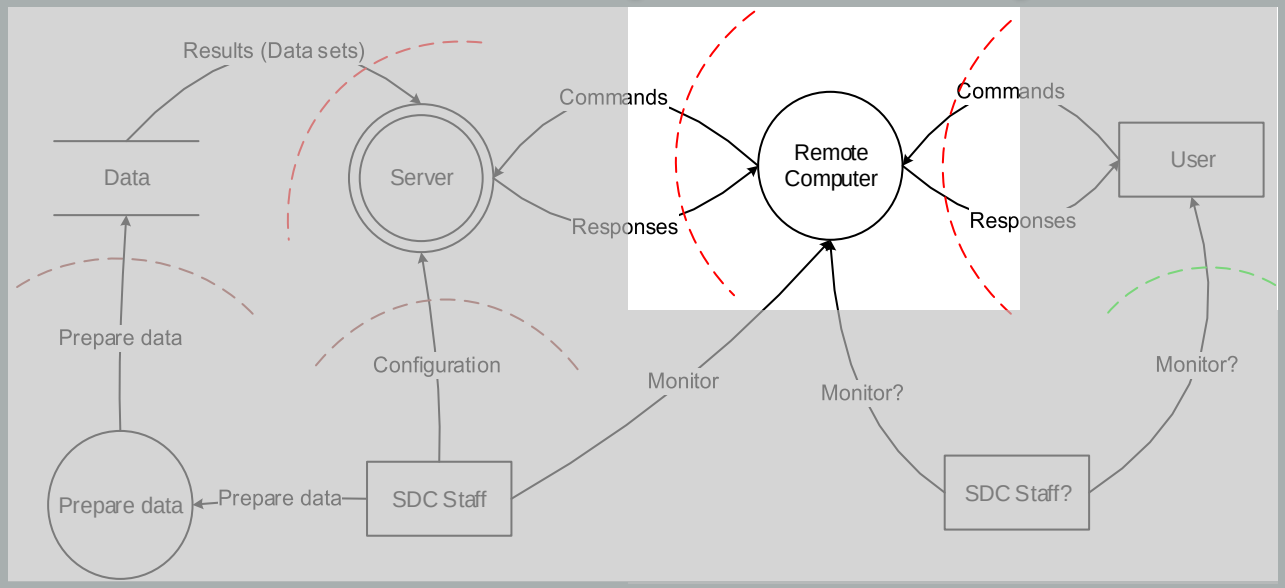
Datenarchiv-
Personal



Individuelle Perspektiven

I5: Lösungsvorschlag





I6: Big Picture

Domänenexperten versus Sicherheitsexperten

Welche Sicherheitsaspekte müssen wir beim Systemdesign berücksichtigen?

Wie soll das System aussehen, welches wir sichern sollen?

Erkenntnisse

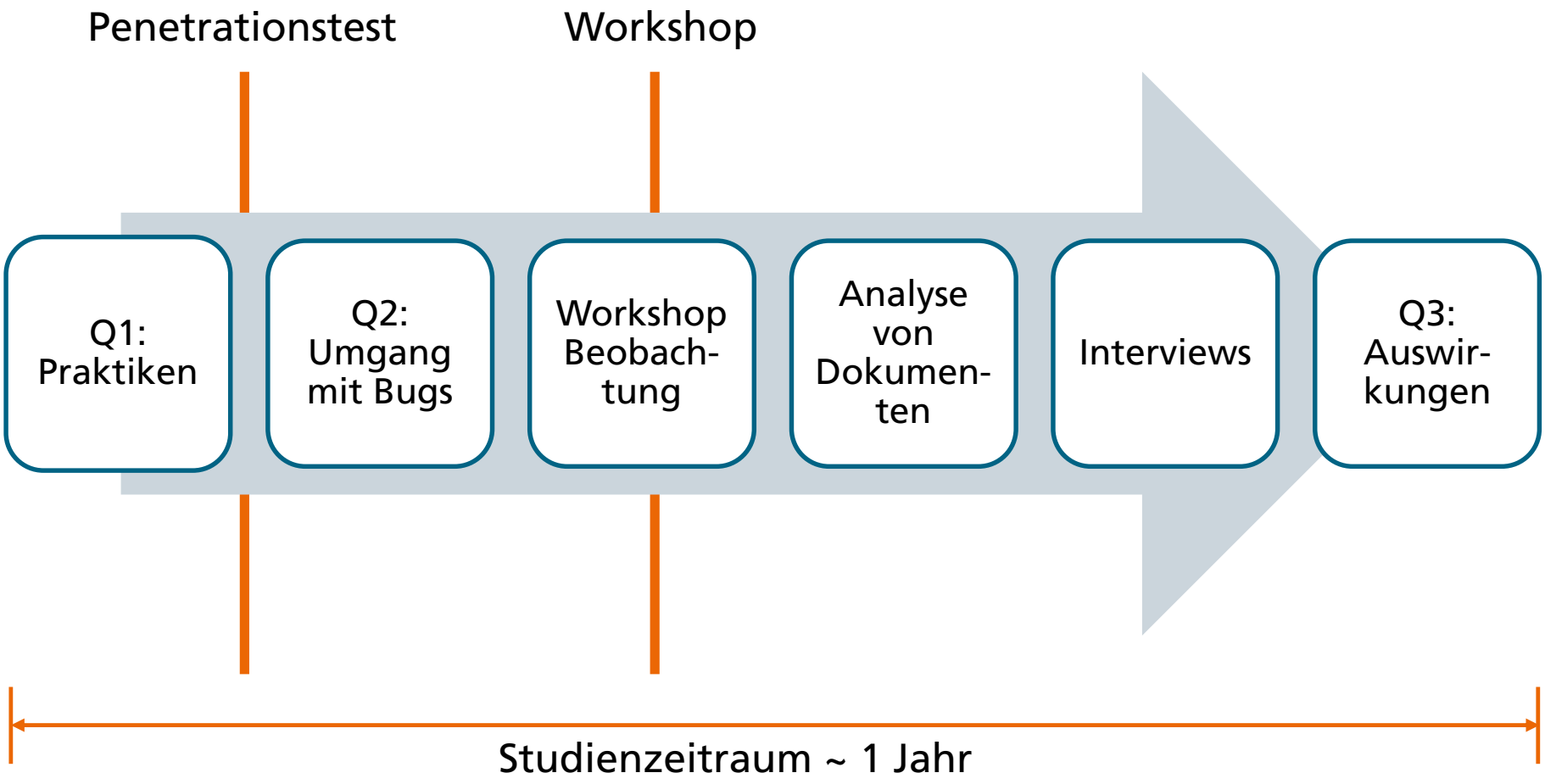
- *Alle* Beteiligten in Bedrohungs- und Risikoanalyse einbinden
- Beteiligte erweitern Wissen mit den Verfahren zunächst kaum
- Kommunikation und Diskurse ermöglichen
- Iterative Herangehensweise bei „unbekanntem Terrain“
- (Achtung: Verfügbare Verfahren unterstützen all diese Schritte nicht)

Studie: Penetrationstests in Unternehmen

Forschungsfrage

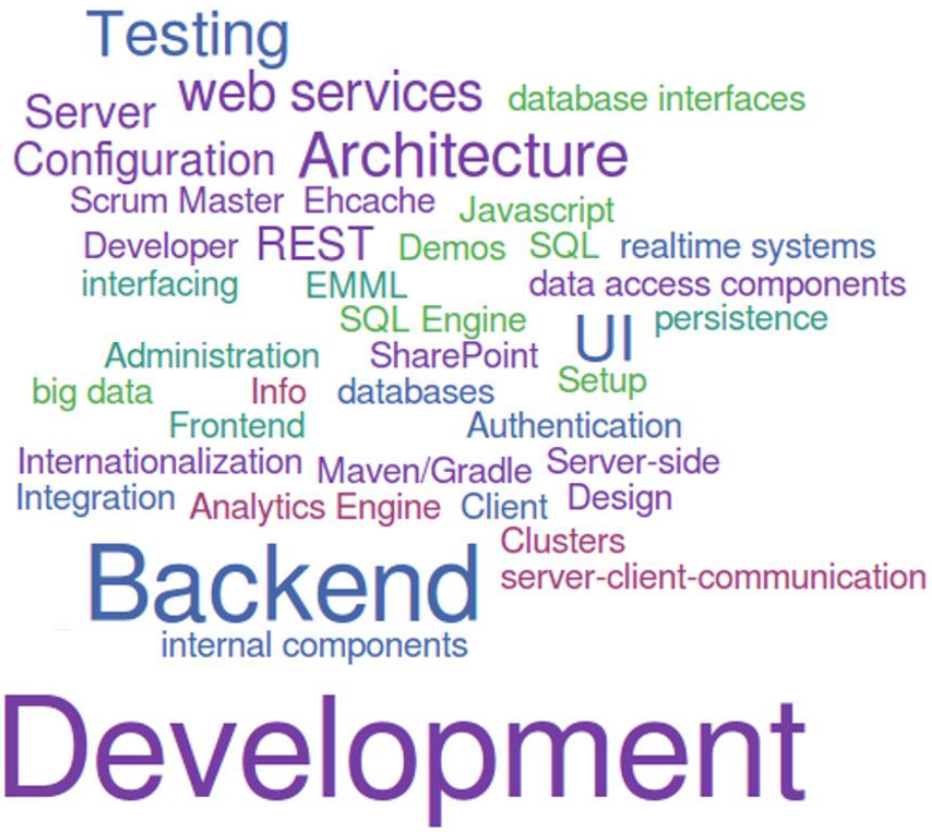
Was sind mögliche mittel- und langfristige Auswirkungen von Penetrationstests auf die Softwareentwicklungspraktiken in Unternehmen?

Studienablauf



Ausgangssituation

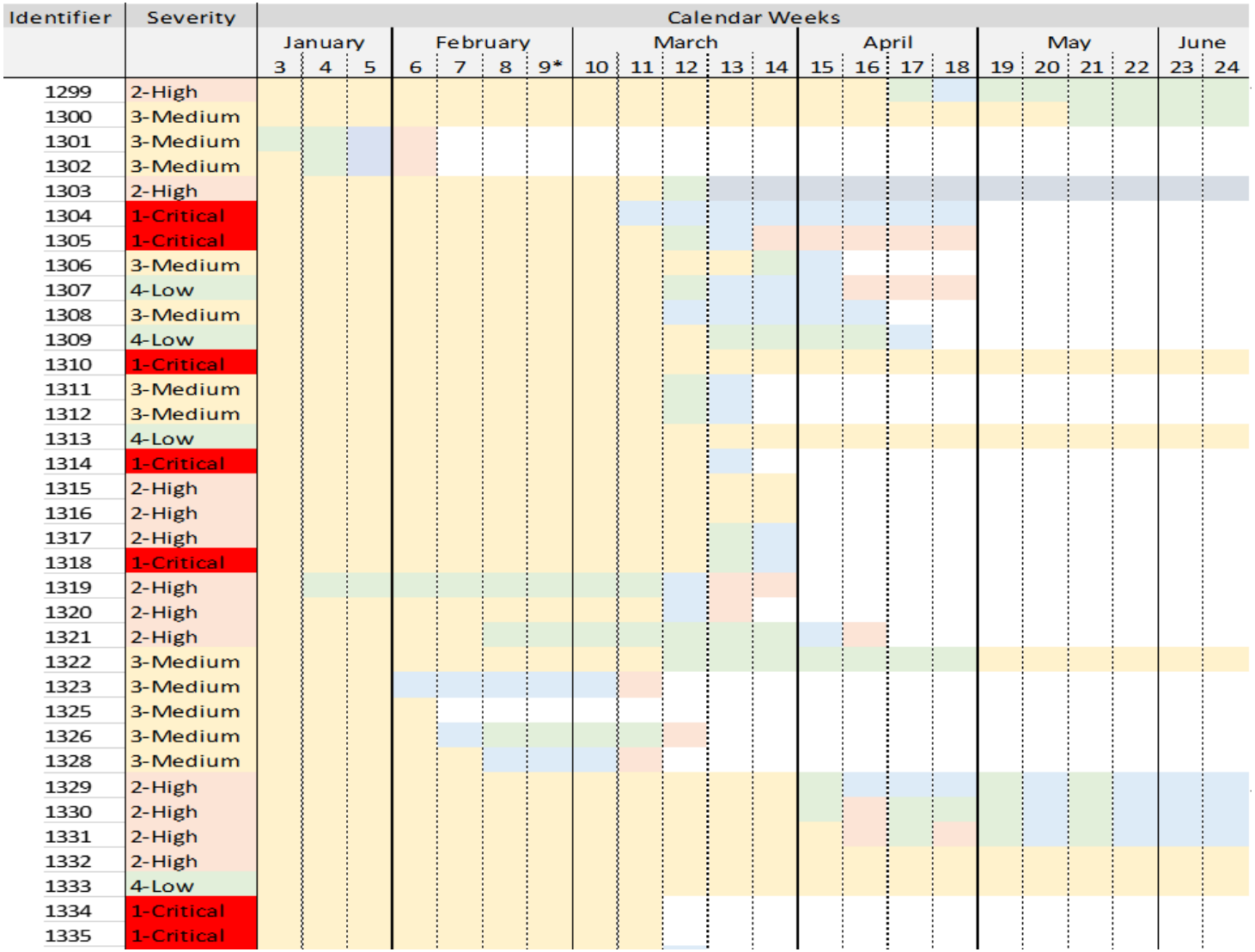
- Vielfältige SCRUM-Teams
- Sicherheit nicht kohärent im Entwicklungsprozess verankert
- Individuelle Praktiken überwiegen
- Neugierig auf den Penetrationstest
- Wille zur Verbesserung
- Globales Sicherheitsteam



Wirkung des Penetrationstests und Workshops

- Vor dem Workshop:
  “I am a developer and sure I can hack things“ (CL)
- Nach dem Workshop:
  “Offen wie ein Scheunentor”(PH)
  “peinlich[e] [Lücken]”
- “eye opener”

Umgang mit Schwachstellen



Verantwortlichkeiten

- “Everyone responsible” versus “Nobody responsible”
- “No consideration how to avoid that in future; who do we make the expert, no kind of follow-up type of thing” (CL)
- “if it is not on the list is it worth the time and extra energy?” (CL)

Rolle der Organisationsstrukturen

- “management has to prioritize where security is, even passively by not deciding” (CL)
- “developers can be trained but their hands are tied as long as management does not decide” (CL)
- “it is like other any software practice but services need to be asked to”, “developers want to keep management happy” (CL)

Produktmanagement versus Entwicklung

We don‘t get the resources to do security seriously.

We don‘t wanna push product security as a selling point.

Erkenntnisse

- Testergebnisse „über den Zaun werfen“ wenig effektiv und effizient
- Externe Berater können (kurzfristig) fehlendes „Ownership“ für Sicherheit ersetzen
- Wichtig: Bewusstsein für Sicherheit auf allen Ebenen, aber auch nach *außen* gelebt
- Entwickler fühlen sich verantwortlich für den Code den sie schreiben, aber alles weitere eine Frage der Prioritäten

Erkenntnisse

- Strukturen in der Softwareentwicklung entscheidend:
  - Welche Spieler?
  - Welche Perspektive? Welche Interessen? Welches Wissen? Welche Fähigkeiten?
  - Existieren Blockadesituationen?
- Schulung und Bewusstseins-Schärfung der Entwicklern wichtig, aber nicht „kriegsentscheidend“
- Gezielt Wissensstrukturen schaffen

Kontakt

Andreas Poller

Fraunhofer Institut für Sichere Informationstechnologie SIT

Rheinstraße 75

64295 Darmstadt

E-Mail: andreas.poller@sit.fraunhofer.de

Telefon: 06151 869 170

CAST-Workshop:
“Sichere Software entwickeln”
12. November, Darmstadt

http://www.cast-forum.de/workshops/infos/209

Unser Team

- Interdisziplinäres Team aus Informatiker und Sozialwissenschaftlern
- Zusammenarbeit Fraunhofer SIT mit GESIS – Leibniz-Institut für Sozialwissenschaften und Goethe-Universität Frankfurt am Main
- Projekte u.a. für SAP, IBM, Software AG

Publikationen

- Andreas Poller, Sven Türpe, Katharina Kinder-Kurlanda: An Asset to Security Modeling?: Analyzing Stakeholder Collaborations Instead of Threats to Assets. NSPW 2014: 69-82
- Jim Whitmore, Sven Türpe, Stefan Triller, Andreas Poller, Christina Carlson: Threat analysis in the software development lifecycle. IBM Journal of Research and Development 58(1) (2014)