Erfolgsfaktoren für Privacy by Design

Sven Türpe, Andreas Poller
Fraunhofer-Institut für Sichere Informationstechnologie SIT
Darmstadt

Fraunhofer SIT

Privacy by Design

Ziele

Intervenierbarkeit,
Nichtverkettbarkeit,
Vertraulichkeit,
Anonymität,
Transparenz, …

Mechanismen, Strategien

Anonymisierung,
Pseudonymisierung,
Differential Privacy,
Datenminimierung,
Verschlüsselung, …

Prinzipien

Proactive,
Preventative,
Privacy by Default,
Embedded into design,
Full functionality,
End-to-end security,
Visibility, Transparency,
User-centric

Beispiele

eGK, nPA

Privacy by Design

Ziele

Intervenierbarkeit,
Nichtverkettbarkeit,
Vertraulichkeit,
Anonymität,
Transparenz, …

Mechanismen, Strategien

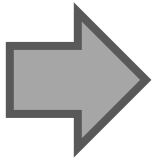
Anonymisierung,
Pseudonymisierung,
Differential Privacy,
Datenminimierung,
Verschlüsselung, …

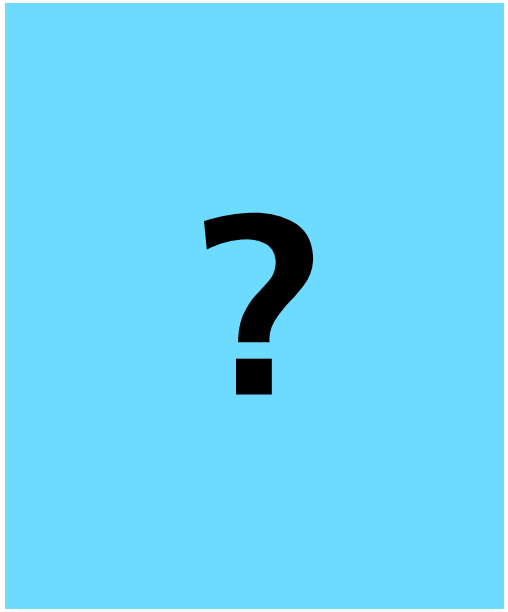
Prinzipien

Proactive,
Preventative,
Privacy by Default,
Embedded into design,
Full functionality,
End-to-end security,
Visibility, Transparency,
User-centric

Beispiele

eGK, nPA





Softwarebürokratie

Big Design Up Front

Prozessmodelle

Management-

Systeme

oder:

Schulung

“Design is what designers do. Clive Dilnot

Kreative Tätigkeit

Gestaltung von Artefakten

Philippe Starck: Juicy Salif

“Design is what designers do. Clive Dilnot

Kreative Tätigkeit

Gestaltung von Artefakten

In verschiedenen Dimensionen

Foto: JeLuF, CC-by-sa, https://commons.wikimedia.org/wiki/File:LemonSqueezer.jpg

Philippe Starck: Juicy Salif

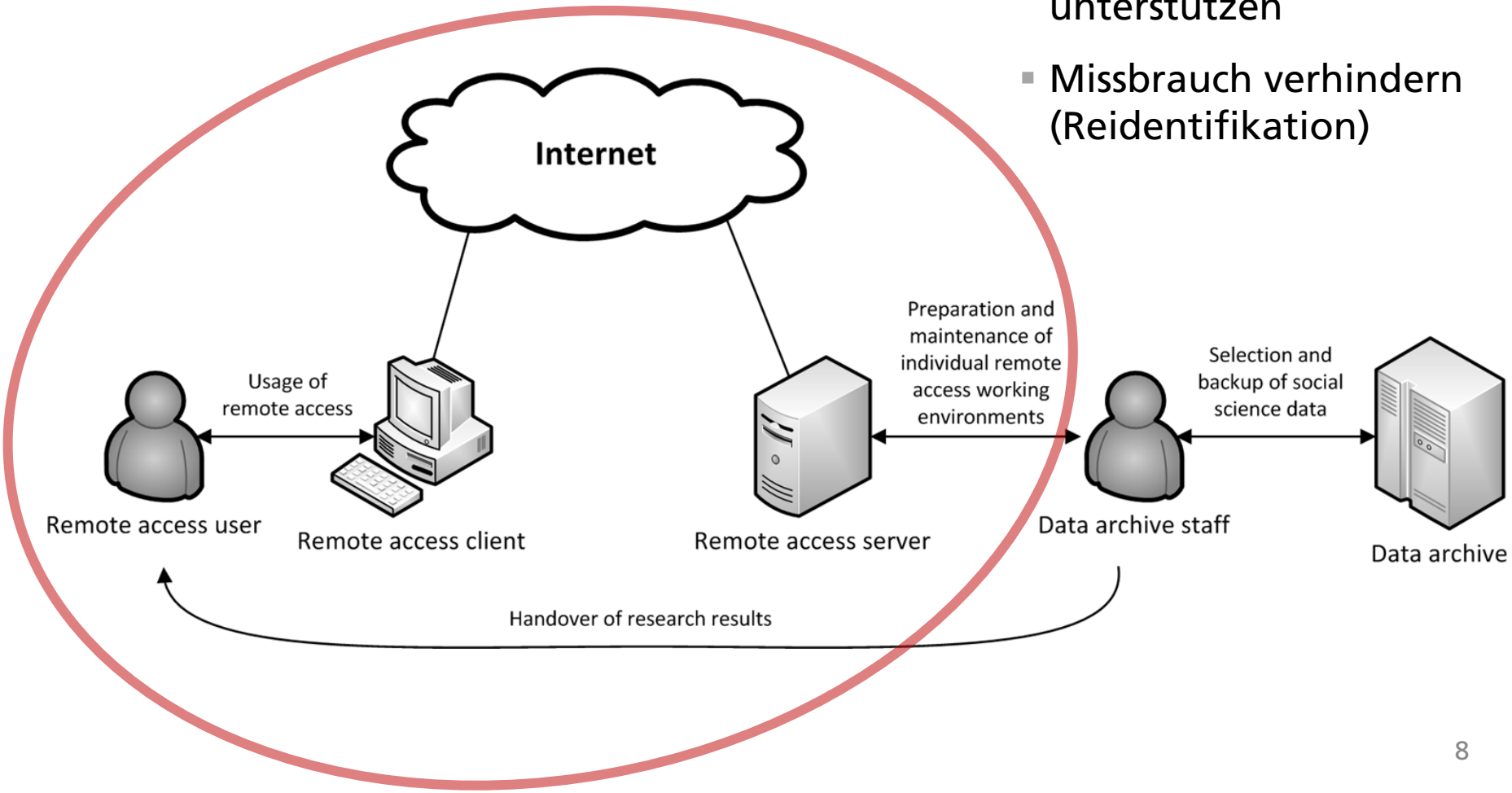
Foto: Niklas Morberg CC-BY-SA 2.0, https://en.wikipedia.org/wiki/File:Juicy_Salif_-_78365.jpg

> “Design is about making decisions, often in the face of uncertainty. It's like running a race where the course keeps splitting. Each fork is a decision.
>
> Joseph Zinter

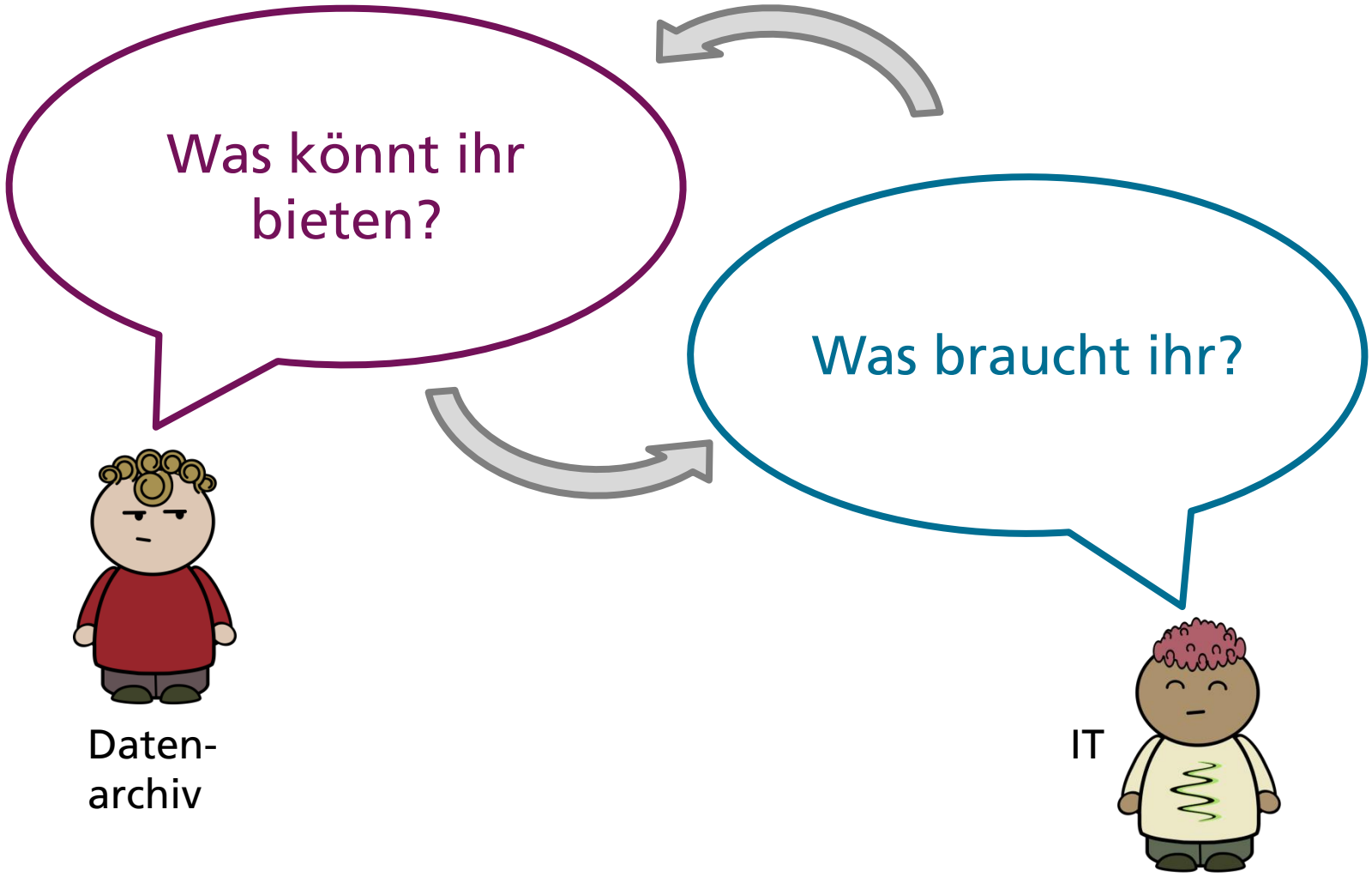
Privacy by Design:
Prozessintervention

Projekt:
Fernzugriff auf ein Datenarchiv

- Legitime Auswertungen unterstützen
- Missbrauch verhindern (Reidentifikation)

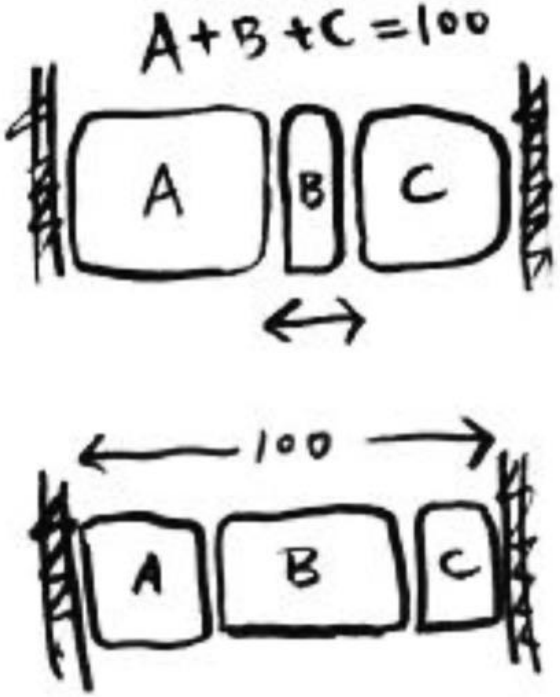


Entwurfsentscheidungen?



“Design is to redesign.

Jan Michl

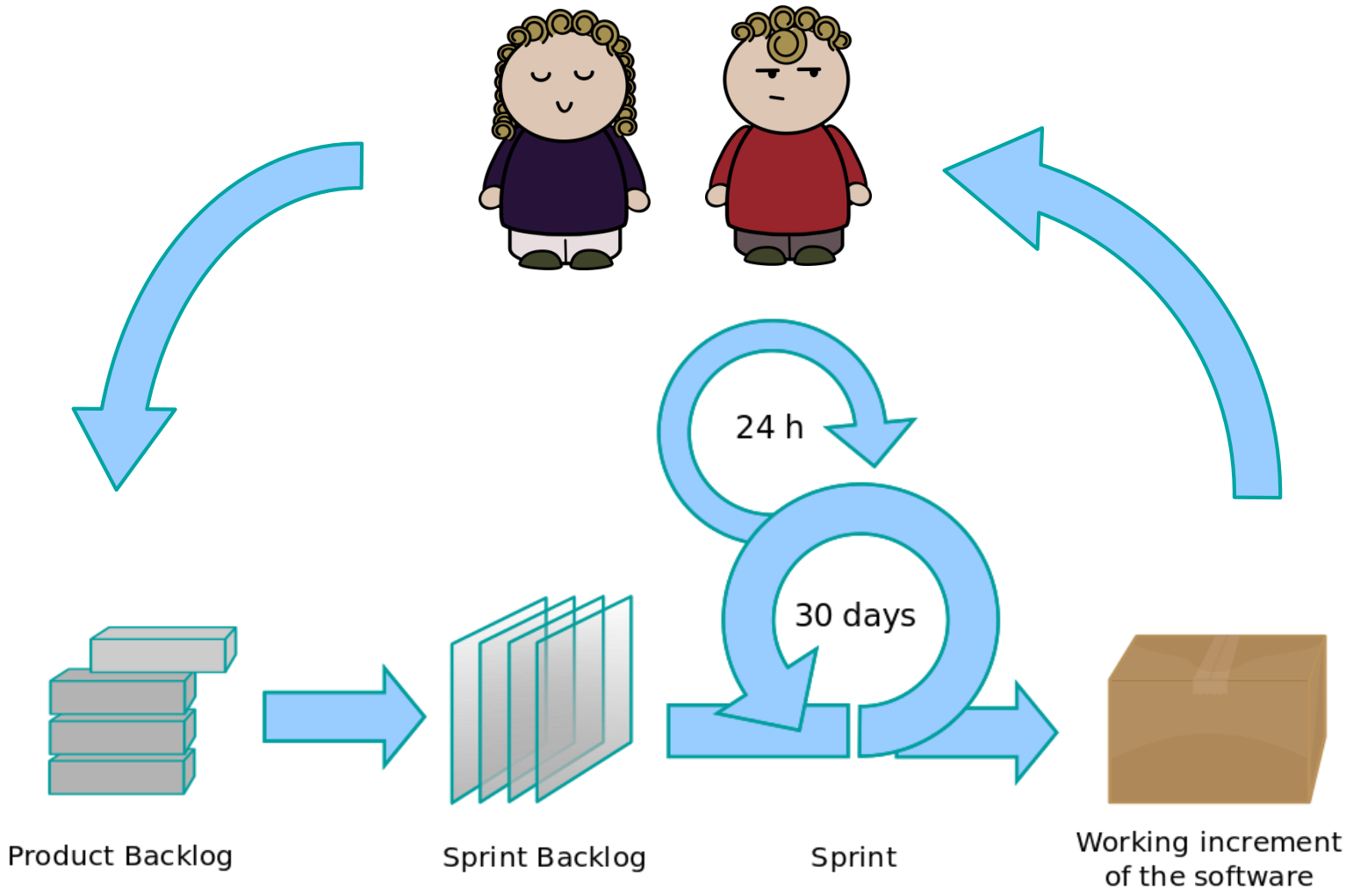


Versuch

Bewertung

Revision

Agile Entwicklung: Scrum



Source: https://en.wikipedia.org/wiki/File:Scrum_process.svg by Lakeworks, CC-BY-SA

Agile Entwicklung

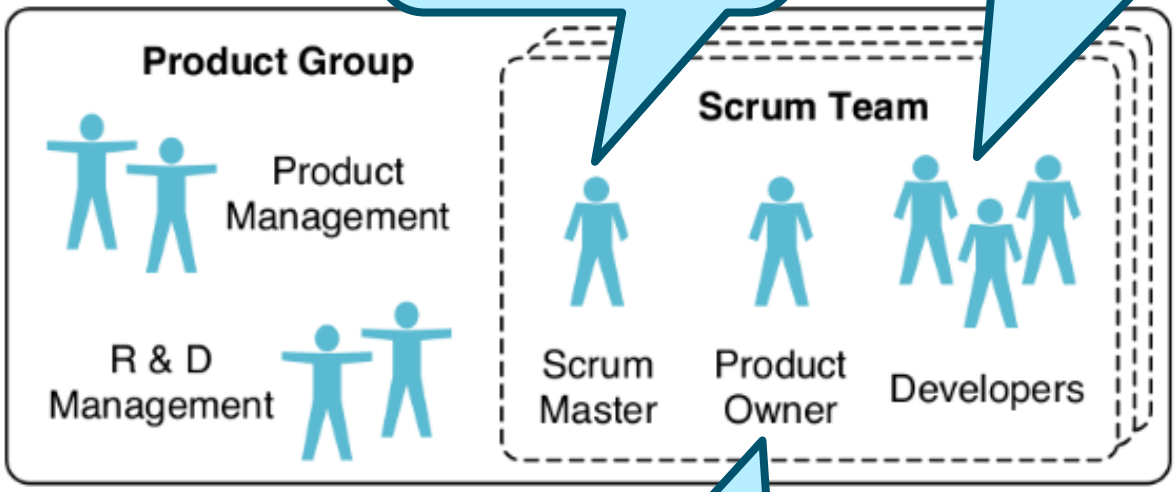
Prinzipien

- Kontinuierliche Lieferung nützlicher Software
- Empirische Prozesssteuerung
- Keine Softwarebürokratie, kein Mikromanagement
- Selbstorganisierende Teams

Scrum: Rollen

Scrum Master:
- Organisiert
- Moderiert
- Unterstützt

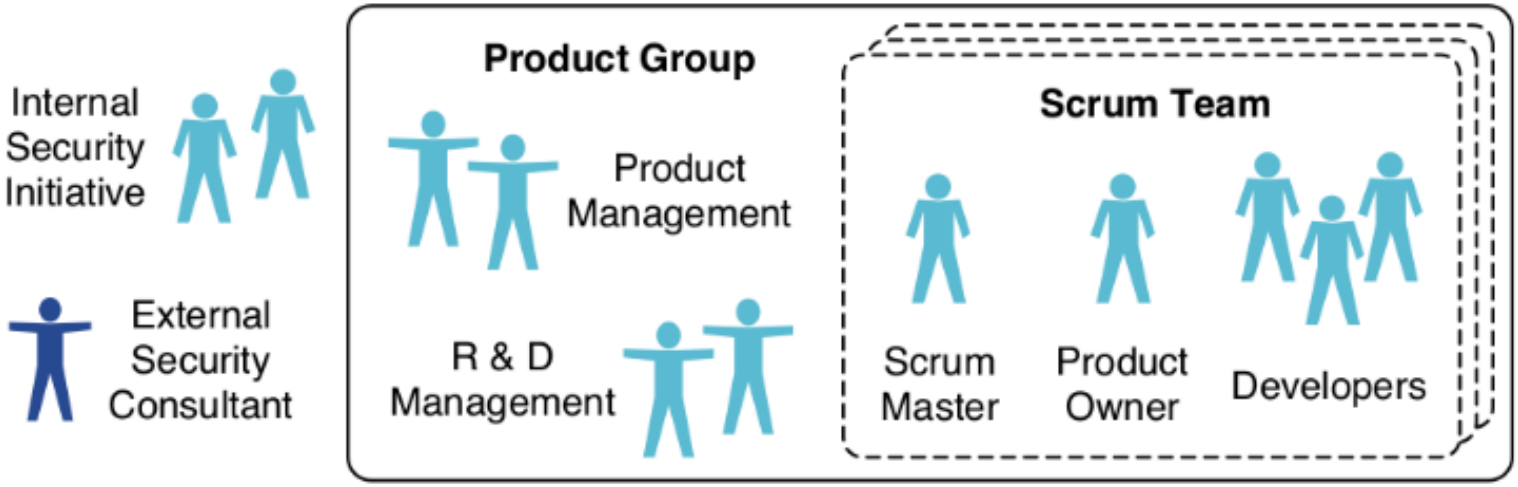
Development Team:
- Selbstorganisierend
- Crossfunktional



Product Owner:
- Priorisiert Anforderungen
- Vertritt Stakeholder

Studie

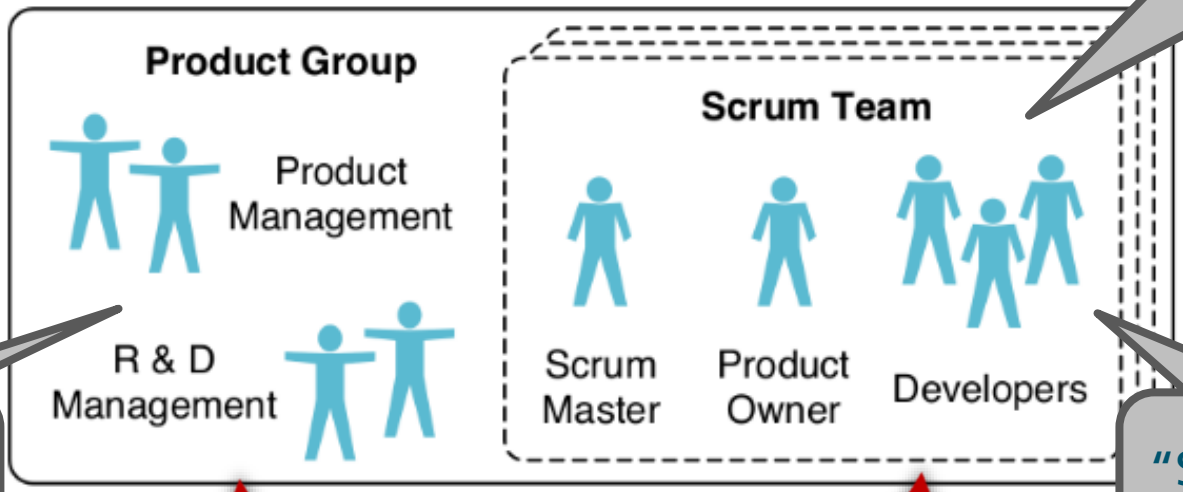
Globesoft Corp.



- ca. 40 Entwickler in 5 Scrum-Teams
- Intervention: Pentest + Schulung
- Langzeiteffekte?

Rollen und Sichten

Awareness – aber kein Raum für Sicherheitsarbeit



"Sicherheit ist Qualität"

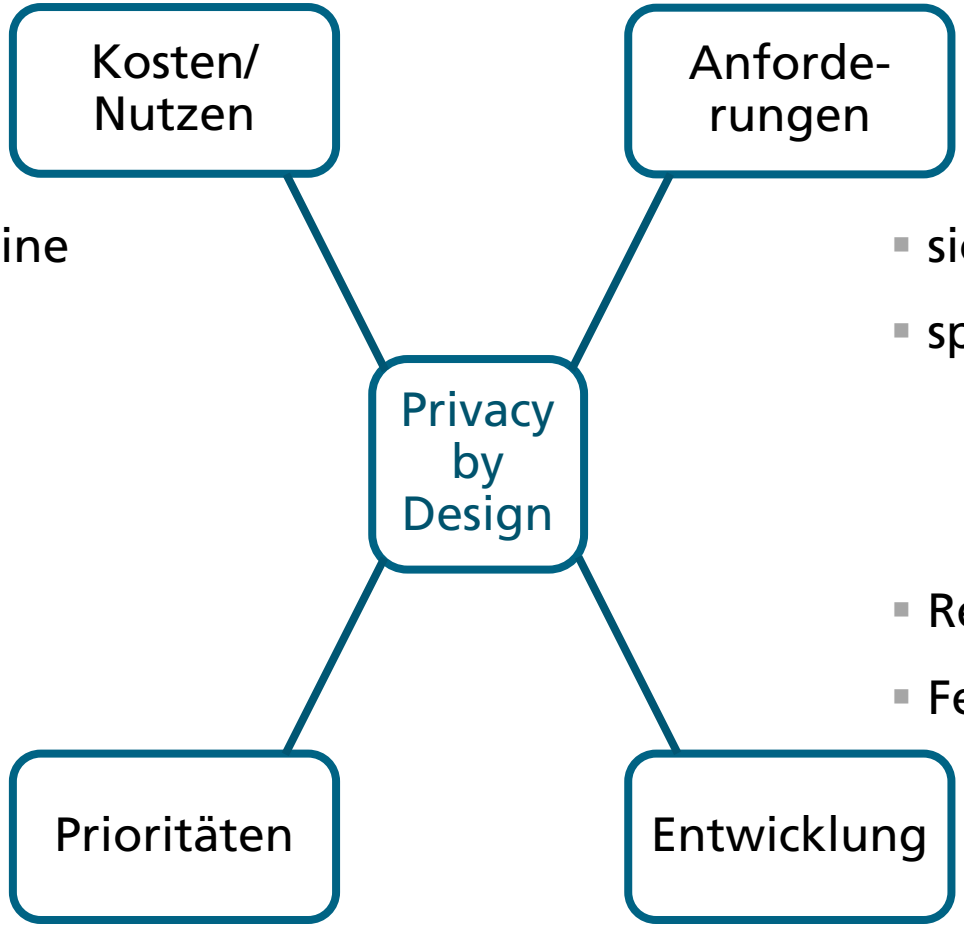
"Security nicht gefordert"

- Management bestimmt Richtung
- Entwickler liefern selbstorganisiert

Features verkaufen Produkt

Unsichtbares Merkmal

Fazit



- Lösungsbausteine
- Ökosystem

- sichtbar, explizit
- spezifisch

- Business Case
- Stakeholder

- Rechtfertigung
- Feedback

WERBUNG

CAST-Workshop:
„Sichere Software entwickeln“
22. März 2018

http://www.cast-forum.de/workshops/infos/244

https://testlab.sit.fraunhofer.de

Sven.Tuerpe@sit.fraunhofer.de

https://plus.google.com/+SvenTürpe

https://erichsieht.wordpress.com/

Veröffentlichungen

A. Poller, L. Kocksch, S. Türpe, F. Epp, K. Kinder-Kurlanda:
"Can Security Become a Routine? A Study of Organizational Change in an Agile Software Development Group." (CSCW 2017)

S. Türpe:
"The Trouble With Security Requirements." (RE 2017)

S. Türpe, A. Poller:
"Managing Security Work in Scrum: Tensions and Challenges." (SecSE 2017)

A. Poller, S. Türpe, K. Kinder-Kurlanda:
"An Asset to Security Modeling? Analyzing Stakeholder Collaborations Instead of Threats to Assets." (NSPW 2014)

J. Whitmore, S. Türpe, S. Triller, A. Poller, C. Carlson:
"Threat analysis in the software development lifecycle." (IBM J. Res. Dev., Jan. 2014)

S. Türpe:
"Point-and-Shoot Security Design: Can We Build Better Tools for Developers?" (NSPW 2012)