Security Canvas oder Schnellboot statt schwerfälliger Risikoanalyse

Eine agile Methode für eine agile SW-Entwicklung

Agenda

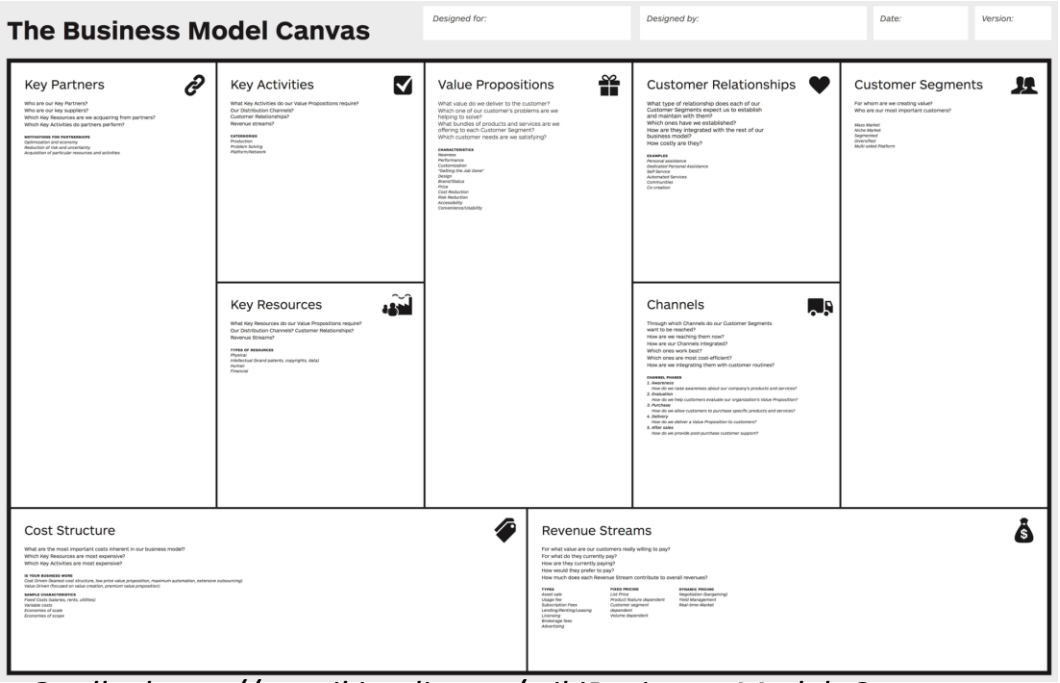
- Security Canvas
  - Was für ein Ding? Wozu?
  - Wie geht das? - Einfach mal machen…
  - Was geht und was nicht?

Security Canvas – Was für ein Ding? Wozu?

Buisness Model Canvas et. al [2005]

- Analysewerkzeug für Geschäftsmodelle
- Einfach und schnell nutzbar
- Strukturiertes, flexibles Vorgehen
- Einheitliches Verständnis im Team
- Diverse Varianten z.B. Projekt Canvas

⇒ Erstellung (meistens) in workshops
⇒ Keine SW Methode (bis jetzt)
⇒ Unterstützt agiles Vorgehen
⇒ Visualisierung der Kernaspekte



Quelle: https://en.wikipedia.org/wikiBusiness_Model_Canvas.png

Security Canvas – Ein Stück Papier

- Übertragung des Canvas Prinzip auf „Security“

⇒ Wie sieht das aus?
⇒ Wozu soll das nützlich/hilfreich sein?
⇒ Wie wendet man es an?

Download Canvas über:
https://www.conplement.de
(ggfs. zeitweilig nicht verfügbar da Seite im Umbau, creative commons license)

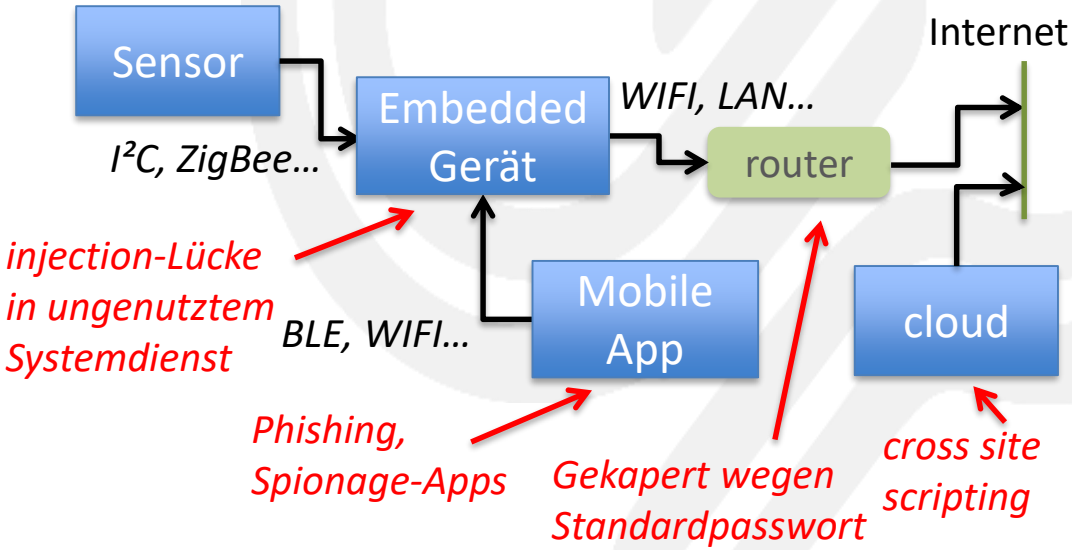
Beispiel: IoT

..vom Sensor bis zur Cloud

- Früher isolierte Eingebettete Systeme werden vernetzt.
- Mobile Apps steigern Bedienkomfort
- Datenaggregation/Übersicht in cloud

⇒ Komplexes Gesamtsystem

⇒ Viele verschiedene Technologien

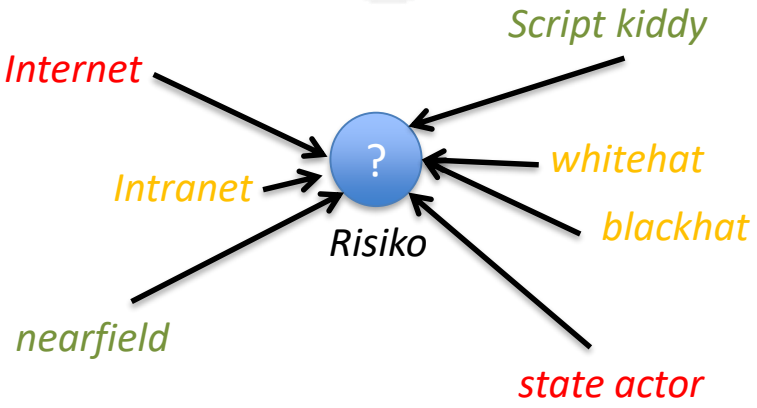


..auf ganzer Linie angreifbar

- Vernetzung eröffnet Zugänge
- Abhören von Kommunikation
- Unerfahrenheit/Bequemlichkeit der Benutzer hebelt security Mechanismen aus

⇒ Gesamtbetrachtung notwendig

⇒ Unterschiedliche Technologien = unterschiedliche Bedrohungen



..vom wem und mit welchen Mitteln?

- Welche Mittel haben reale Angreifer?
- Welche Sicherheitszonen existieren?

⇒ Was ist das angemessene Security-Level?

Security (nicht nur) für IoT

Secure Software Development Life-Cycle

- Security betrifft den gesamten Lebenszyklus
- Security betrifft den gesamten Entwicklungsprozess

⇒ Security von Anfang an

Security Threats and Risks Analyse / T(A)RA

- Bedrohungen analysieren und bewerten
- Maßnahmen ableiten
- Diverse Vorgehensweisen (STRIDE, IEC 62443…)

⇒ Praktisch immer empfohlen (z.B. OWASP SAMM)

⇒ Oft sehr umfangreich – Fleißarbeit vs. Nutzen?

⇒ Erfüllen einer Norm oder machen, weil nützlich?

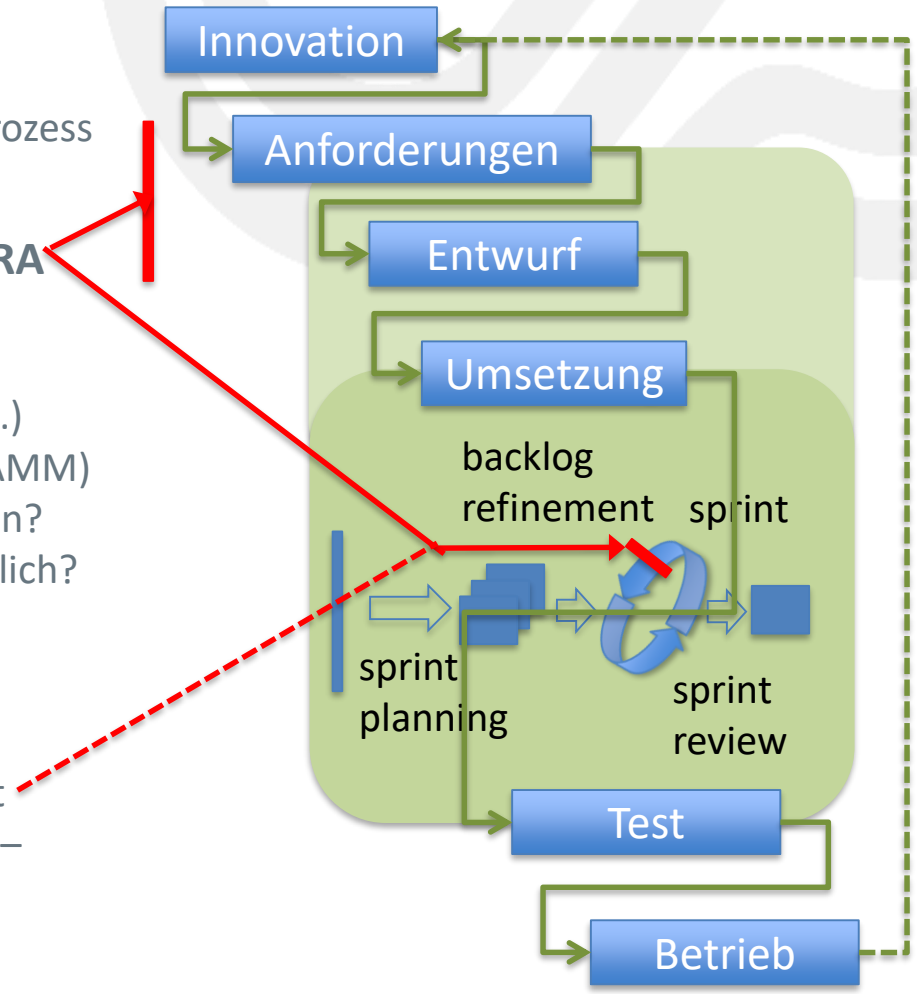
Agil oder doch wieder Wasserfall?

- Vorgehen vs. Dokumentationsmodell
- Inkrementellle Verfeinerung / Feature basiert

⇒ Risikoeinschätzung stellt sich immer wieder – System, Subsystem, Komponente…

⇒ Nicht nur Sache der Architekten, PO,…

⇒ Wie verschafft man sich agil im Team den Überblick? Wie gleiches Verständnis?



Security Canvas – einfach mal machen…

Anwendungsbeispiel: „Smart Terrarium“

- Idee: Umgebungskontrolle eines Terrariums (z.B. Tag/Nachtzyklus,als IoT-System)

⇒ „smart home“ für Reptilien

Features

- Automatischer Tag/Nacht-Zyklus (Kontrollrechner steuert Lampe, Heizstrahler, Temperaturfühler…)
- Definition der Schaltzeiten des Tag/Nacht/Zyklus sowie der Mittagstemperatur per App
- Soll/Ist Temperaturverlaufszeiten per App
- Trending Langzeitanalyse in der cloud
- Lifezugriff per App von überall

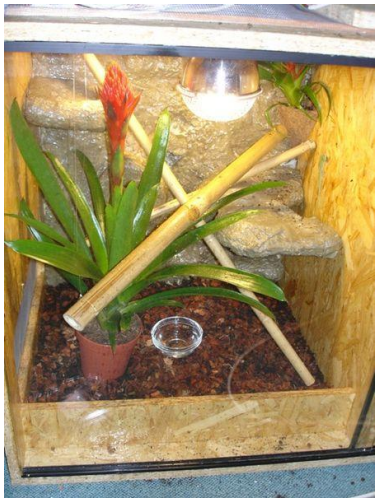
⇒ Cloud features brauchen Konto (Premium-Service)

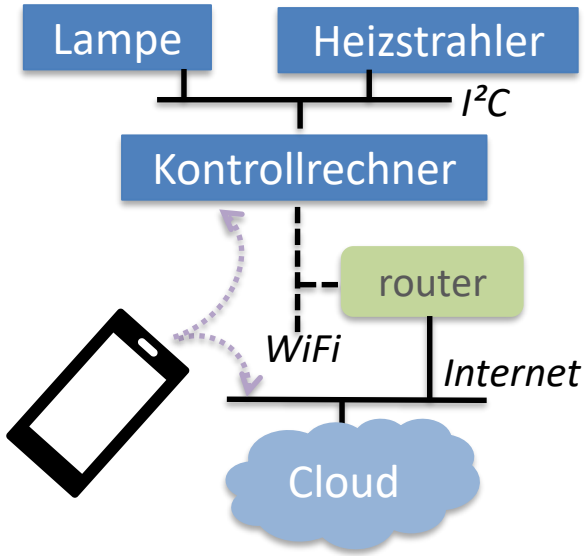
Architektur/Komponenten

- Kontrollrechner
  - Aktoren: Lampe, Heizstrahler,
  - Sensoren: Temperaturfühler
- Mobile App
- Benutzerkonto in der Cloud

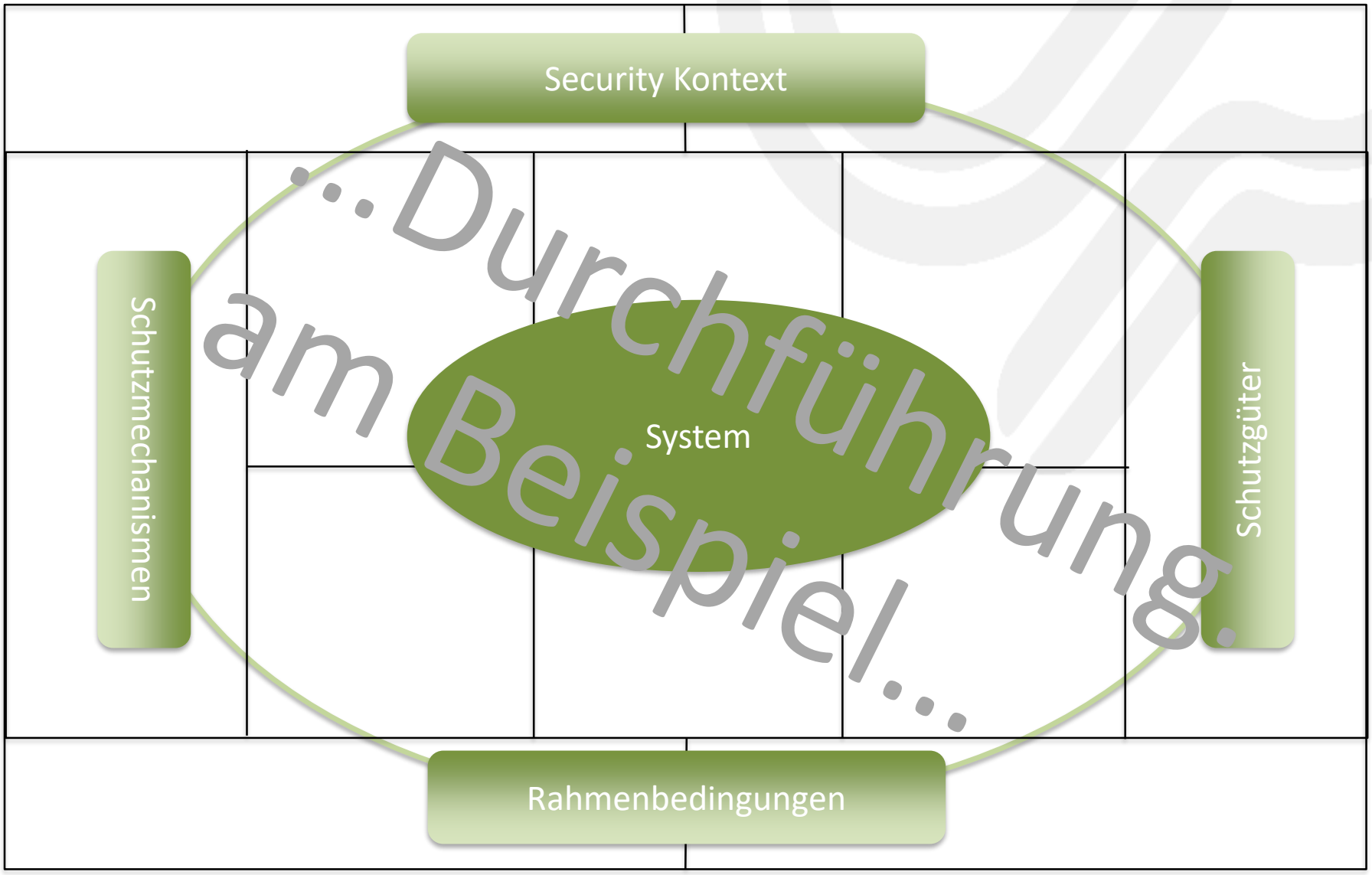
⇒ Was sind die maßgeblichen security Aspekte?

Quelle: commons.wikimedia.org/wiki/File:Terra_guttata_2.JPG





Security Canvas – „Smart Terrarium“



Security Canvas – Was geht? Was nicht?

Was kann der Security Canvas?

- Frühzeitig einen Überblick zu security schaffen

⇒ Verständnis auch bei „Nicht“-SW Experten

- Vorbereitung einer (System-)Risikoanalyse

⇒ Relevante Angreifer identifizieren

⇒ Schutzgüter bestimmen…

⇒ Risikoprofil verstehen

- Auch auf Architektur/Komponenten-Design oder API Ebene anwendbar

⇒ Security Aspekte visualisieren

⇒ Passt als agile Methode zu agiler SW-Entwicklung

Was kann der Security Canvas nicht?

- Kein formales Ergebnis

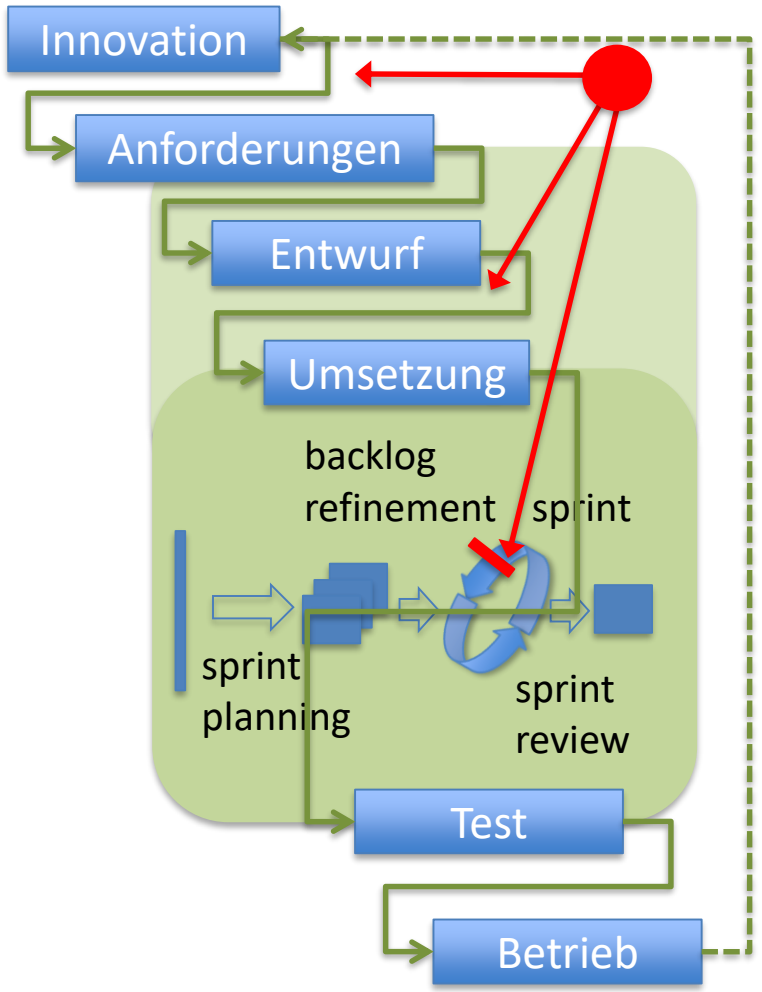
⇒ Erfüllt keine Norm

- Keine Risikoanalyse

⇒ Wahrscheinlichkeiten nirgends enthalten

- Kein „Kochrezept“

⇒ Wichtig ist, die richtigen Fragen zu stellen



Security Canvas oder Schnellboot statt schwerfälliger Risikoanalyse

Das Schnellboot reicht, wenn

- Keine formale, normgerechte Dokumentation gebraucht wird
- Keine Wahrscheinlichkeiten oder andere Quantifizierung gebraucht wird
- Keine nachverfolgbare, formale Anforderungen definiert werden sollen

⇒ Die Risiken und deren Bewertung nicht im Vordergrund stehen

- Eine Ersteinschätzung des sinnvollen/notwendigen security-levels gebraucht wird
- Das Gesamtbild bzgl. security nicht SW-Experten zugänglich gemacht werden soll
- Architekturentwürfe hinsichtlich security diskutiert werden
- Das Design von Systemkomponenten hinsichtlich security Auswirkungen zu bewerten

⇒ Einheitliches Verständnis im Projekt-Team zu schaffen

⇒ Im Team Design/Architektur Entscheidungen diskutiert werden

…ansonsten braucht es doch eine ‚schwerfällige Risikoanalyse'

⇒ Security Canvas als Vorbereitung (lässt auch Abschätzung für TRA-Aufwand zu)

Kontakt: juergen.acker@conplement.de

Wir machen Digitalisierung nutzbar.

conplement AG
Südwestpark 92
90449 Nürnberg
Tel.: +49 911 25 50 976 0

www.conplement.de