LEHRSTUHL 14
SOFTWARE ENGINEERING

Compliance Analyse mit Riskfinder

von Christian Riest

Überblick

- Einführung
- Grundlagen
  - Compliance
  - IT-Grundschutz-Kataloge
  - Projekt Wortschatz
  - Stopwords
  - SecReq
- Riskfinder
- Zusammenfassung und Ausblick

Einführung

- Immer mehr Anforderungen an Software
- Verschiedenste Arten
  - Gesetze
  - Bestimmungen
  - Standards
- Unterschiedlichste Formulierungsarten
  - Text (Gesetze)
  - Modell (UML)

Einführung

- Überprüfen, welche Anforderungen relevant sind:
  - Während der Entwicklung
  - Unterstützt durch Software
  - Automatisiert
  - Mit Lösungsvorschlägen
- Betroffene Softwarekomponenten ermitteln
  - Z.B. Komponenten in einem Modell
- Ziel: Software zu entwickeln, die compliant ist

Grundlagen Compliance

- Gesamtheit notwendiger Maßnahmen zum Einhalten von Anforderungen
- Beim Einhalten aller Anforderungen = Compliance
- ~ Regeltreue
- Anwendung in vielen Bereichen
  - Rechts- und Wirtschaftswissenschaft
  - Chemie
  - Medizin
  - Landwirtschaft

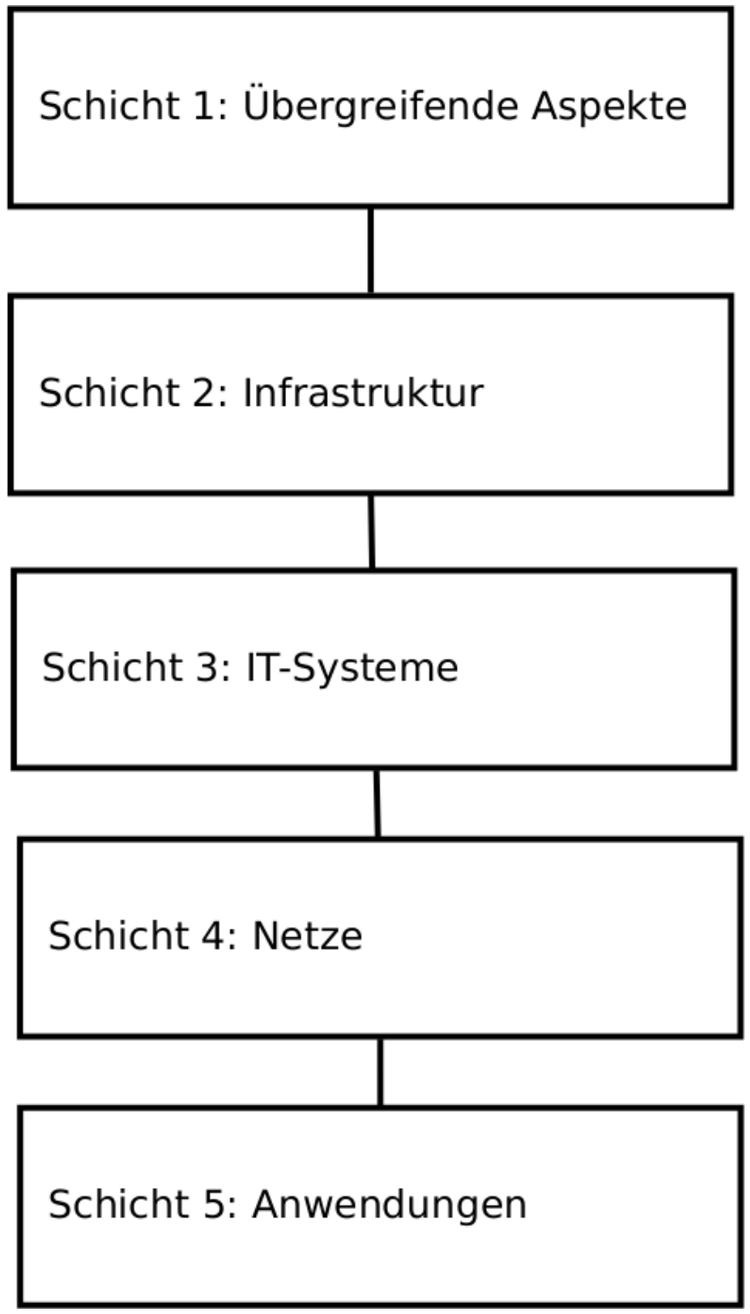
Grundlagen Compliance

- Software in immer mehr Anwendungs- und Lebensbereichen
- Regulierung und Reglementierung notwendig
- Beispiel:
  - In soziale Netzwerke muss Sicherheit der Daten garantiert sein (Bundesdatenschutzgesetz)
- Zahl der Anforderungen wächst
- Meist in Form von Text

Grundlagen IT-Grundschutz-Kataloge

- Vom Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Sammlung von Regeln und Empfehlungen für Software
- Besteht aus Bausteinen
  - Beschreibung
  - Gefahren
  - Maßnahmen
- Gefahren- und Maßnahmenkatalog bilden Grundlage für die Riskfinder-Analyse

- Bausteine werden verschiedenen Schichten des IT-Grundschutz-Modells zugewiesen
- Je höher Schicht, desto relevanter



B 1.5 Datenschutz

Beschreibung

Aufgabe des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen ("informationelles Selbstbestimmungsrecht").

Aufgrund der engen Verflechtung von Datenschutz und Informationssicherheit werden in diesem Baustein zum Thema "Datenschutz" einerseits die Rahmenbedingungen für den Datenschutz praxisgerecht aufbereitet und andererseits die Verbindung zur Informationssicherheit im IT-Grundschutz aufgezeigt.

Gefährdungslage

Gefährdungen im Umfeld des Datenschutzes können vielfältiger Natur sein. Stellvertretend für diese Vielzahl der Gefährdungen werden in diesem Baustein die folgenden typischen Gefährdungen betrachtet:

Organisatorische Mängel

G 2.162	Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten
G 2.163	Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten
G 2.164	Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten
G 2.165	Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten
G 2.166	Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten

Maßnahmenempfehlungen

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen eines Datenschutzmanagements müssen die rechtlichen Rahmenbedingungen beachtet und geeignete technische und organisatorische Maßnahmen getroffen werden, um den Datenschutz sicher zu stellen. Dazu gehören Maßnahmen in der Planungs- und Konzeptionsphase, im Zuge der Umsetzung, sowie beim Betrieb von IT-Systemen und -Verfahren.

Nachfolgend wird das ergänzende Maßnahmenbündel für den Bereich Datenschutz vorgestellt, das für alle IT-Systeme und IT-Verfahren anzuwenden ist, mit deren Hilfe personenbezogene Daten verarbeitet werden:

Planung und Konzeption

M 2.501		Datenschutzmanagement
M 2.502		Regelung der Verantwortlichkeiten im Bereich Datenschutz
M 2.503		Aspekte eines Datenschutzkonzeptes
M 2.504		Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten
M 2.505		Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten

Grundlagen Projekt Wortschatz

- Worte für Rechner schwer vergleichbar
  - Syntax ungleich Semantik
- Lösung: Projekt Wortschatz Universität Leibzig
- Nachschlagewerk für Gebrauch, Assoziation, Synonyme von Worten
- Mehrere Webservices:
  - Grundform
  - SentencesToWord
  - Synonyms
  - RightOccurrences und LeftOccurrences

Grundlagen Projekt Wortschatz

- Worte für Rechner schwer vergleichbar
  - Syntax ungleich Semantik
- Lösung: Projekt Wortschatz Universität Leibzig
- Nachschlagewerk für Gebrauch, Assoziation, Synonyme von Worten
- Mehrere Webservices:
  - Grundform
  - SentencesToWord
  - Synonyms
  - RightOccurrences und LeftOccurrences

Anfrage für Synonyme von „Daten“

Synonyms Client

File

Request | Result

distinct(w2.wort_bin)	r1.typ
Angaben	S
Testdaten	S
Zahlen	S
Dateien	S
Fakten	S
Maße	S
Textdaten	S
Textdateien	S
Einzelheiten	S
Unterlagen	S

Grundlagen Stopwords

- Worte ohne Relevanz für die Aussage eines Satzes
- Beispiel:
  - „Die Daten werden über das Netzwerk verschickt und eine Bestätigung an den Nutzer gesendet“

Grundlagen Stopwords

- Worte ohne Relevanz für die Aussage eines Satzes
- Beispiel:
  - „Die Daten werden über das Netzwerk verschickt und eine Bestätigung an den Nutzer gesendet“

Grundlagen Stopwords

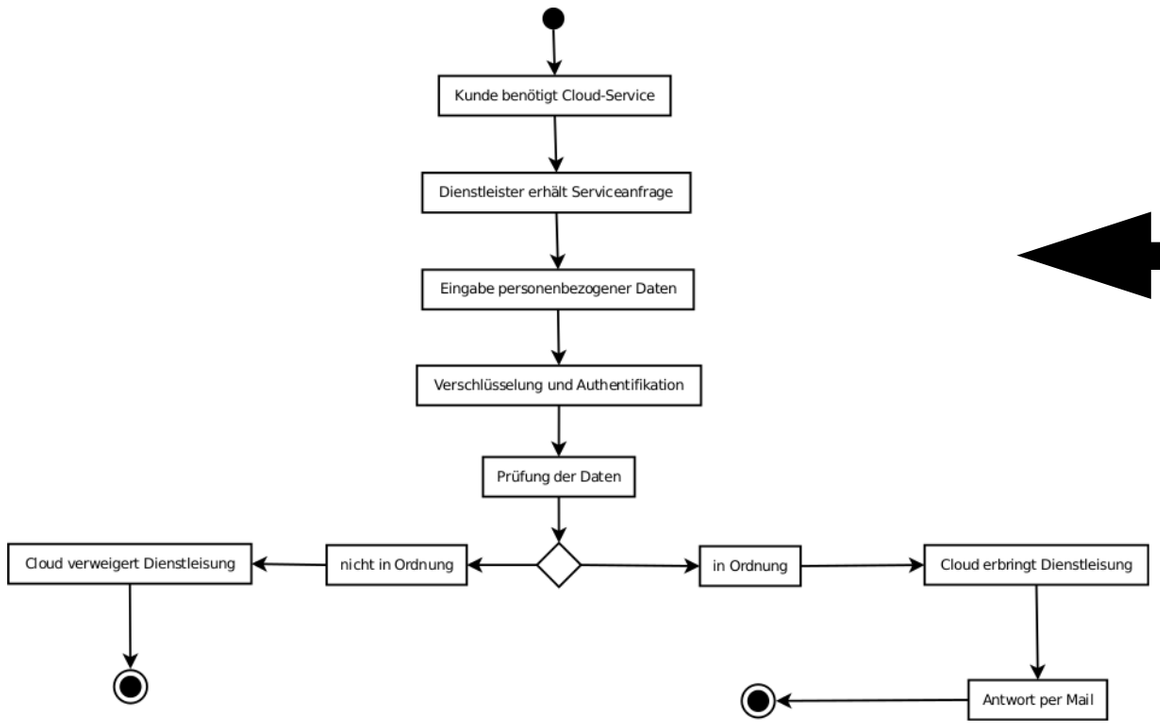
- Worte ohne Relevanz für die Aussage eines Satzes
- Beispiel:
  - „Daten werden über Netzwerk verschickt, Bestätigung an Nutzer gesendet“
- Selber Inhalt, fünf Wörter weniger

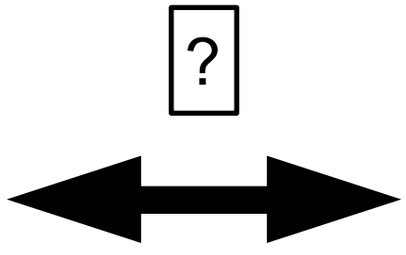
  ➡ schnellere und bessere Analyse

Grundlagen SecReq

- Projekt der Universität Hannover
- Ziel: die besten Sicherheitskonzepte und -praktiken für Entwickler verständlich zu machen
- Unterstützung für Entwickler durch
  - Werkzeuge
  - Dokumentation
- In diesem Rahmen:
  - Tool, das die Wahrscheinlichkeit ermittelt, ob ein Wort im Bereich Sicherheit relevant ist

Problem: Wie überprüfen, ob Anforderung relevant?

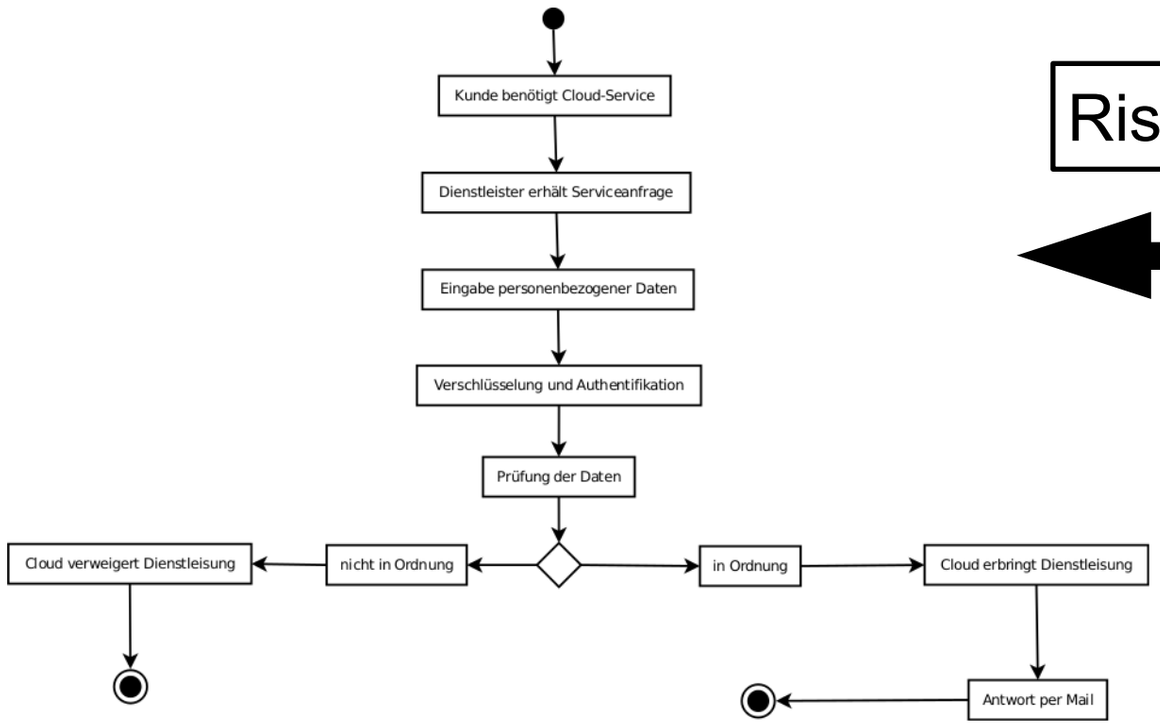




Gesetz

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Problem: Wie überprüfen, ob Anforderung relevant?



Gesetz

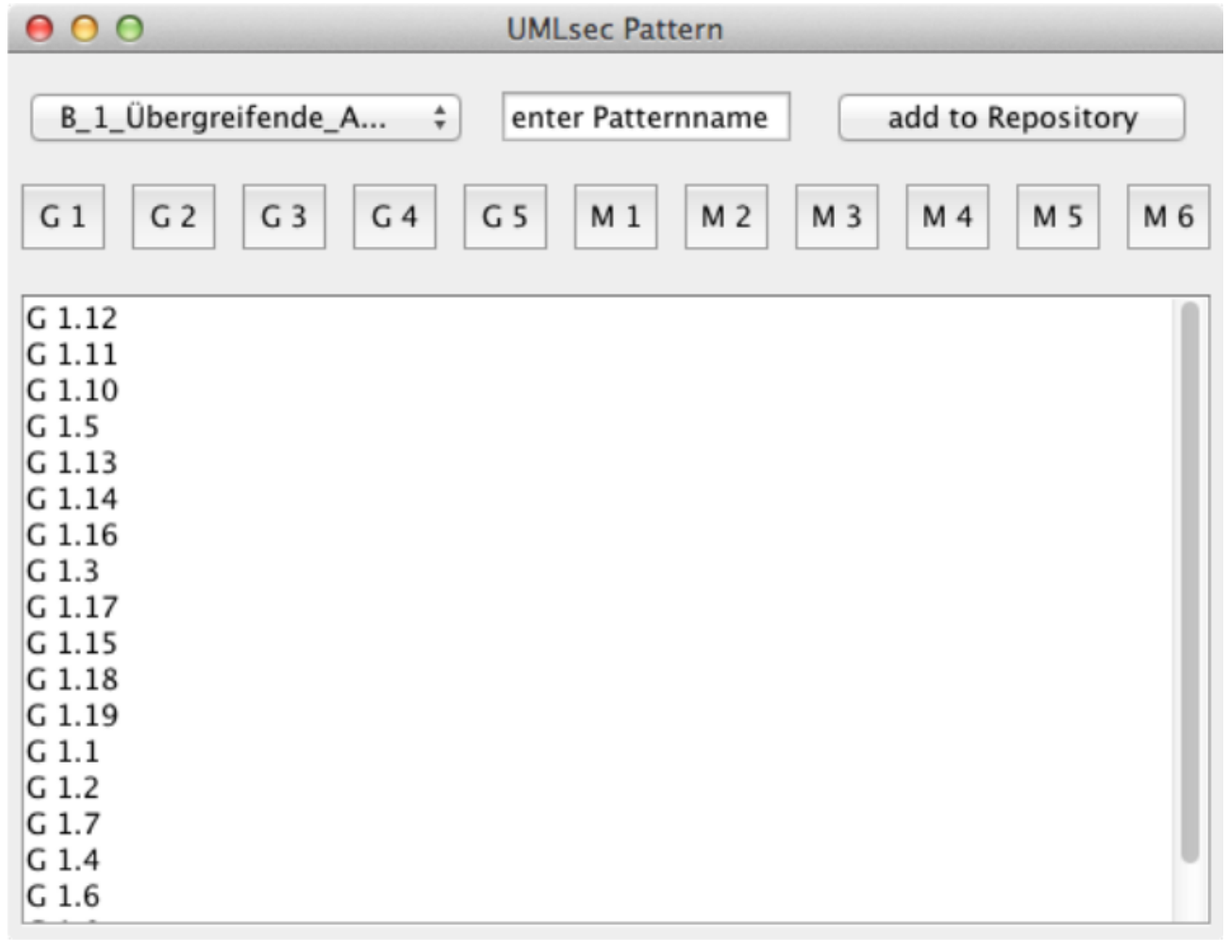
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Riskfinder

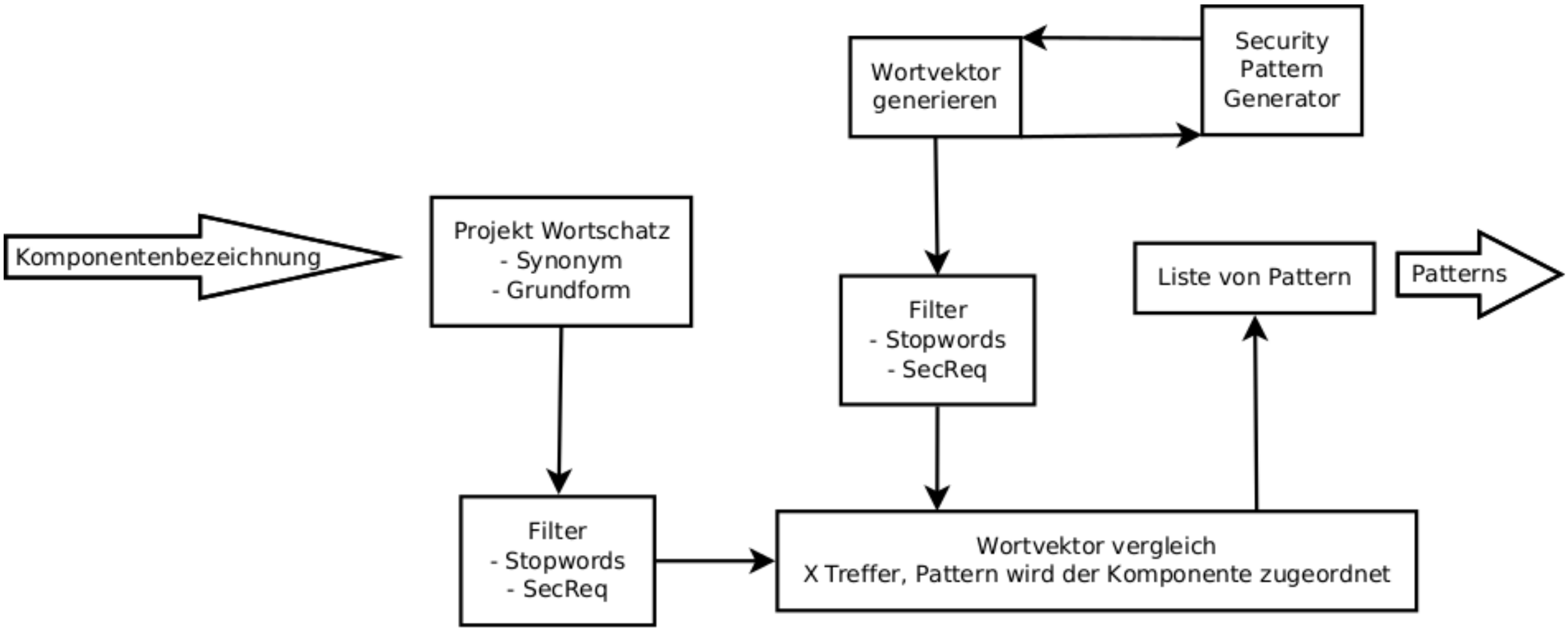
- Im Rahmen der Diplomarbeit von Marc Peschke entwickelt
- Erweiterung für das UMLsec Tool
- Analyse von UML-Modellen im Kontext sicherheitsrelevanter Eigenschaften (Patterns)
- Markierung von Risikobereichen im Modell
- Patterns von Nutzer selbst definierbar auf Basis des IT-Grundschutz-Katalogs
- Idee: Patterns den einzelnen Modellkomponenten zuordnen

Riskfinder Patterns

- Neues Pattern erstellen
- Name und Modellschicht zuweisen
- Gefahren und Maßnahmen aus IT-Grundschutzkatalog durch Markierung auswählen



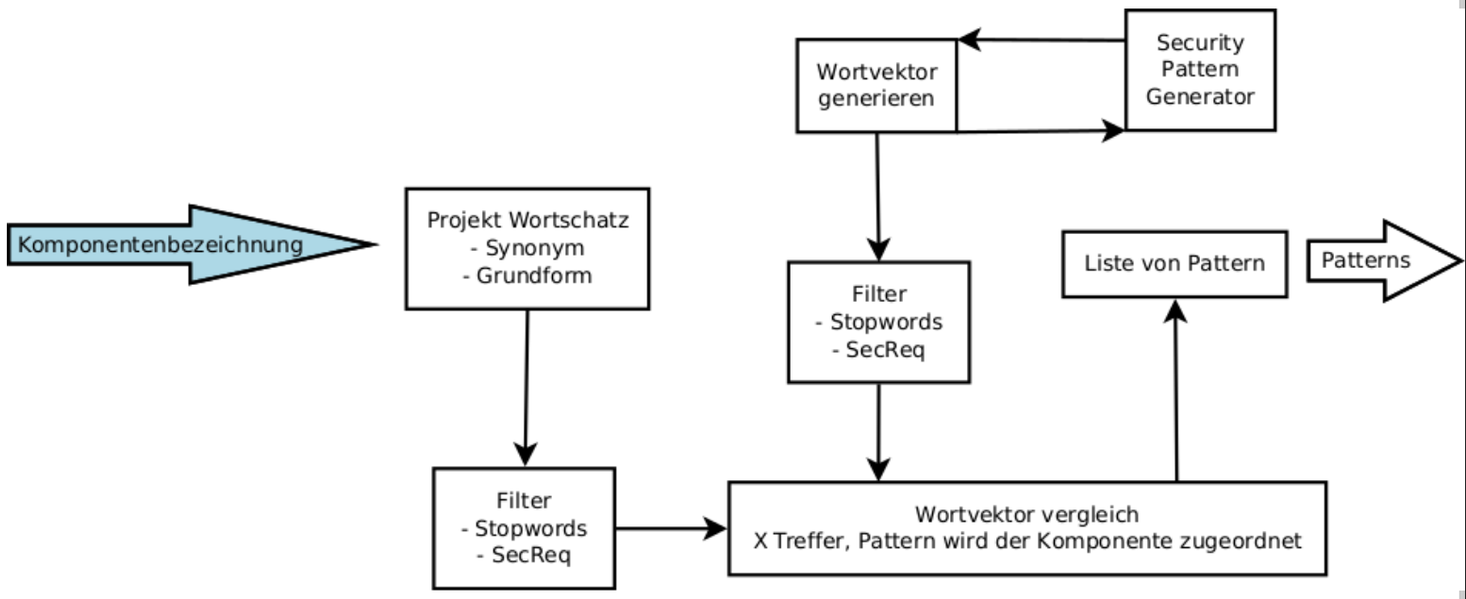
Riskfinder Algorithmus



Riskfinder Algorithmus

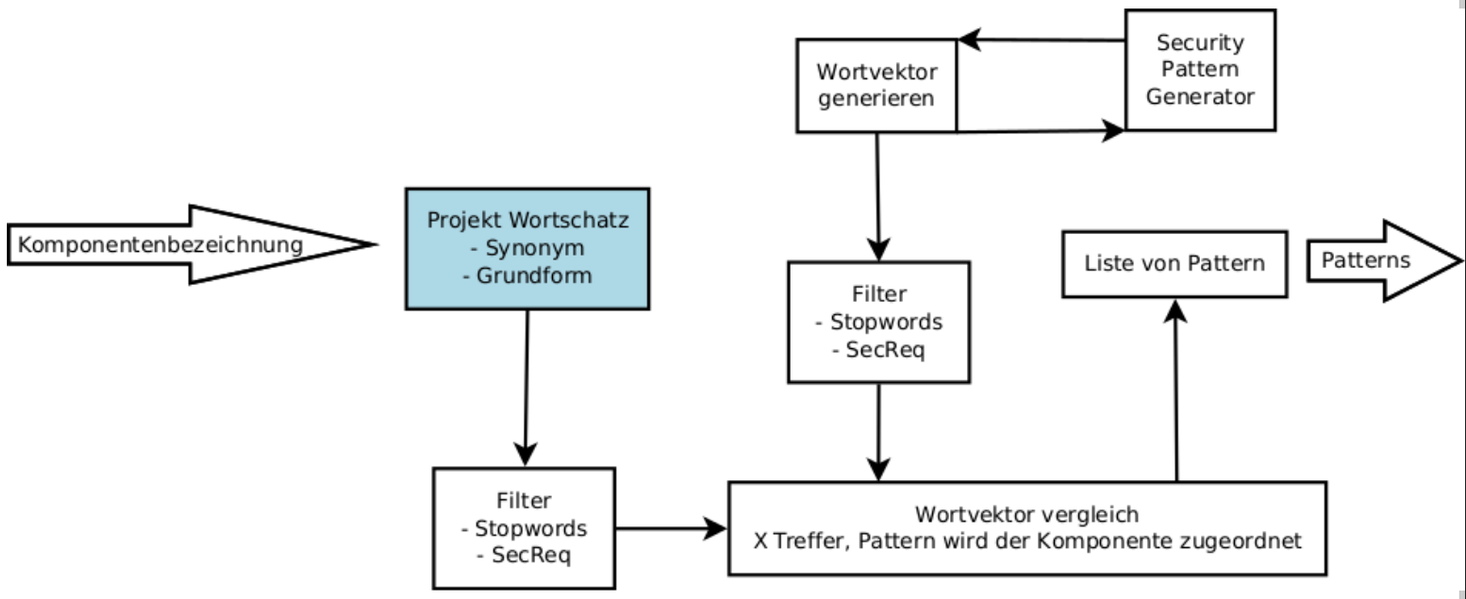
Eingabe:

- Beschreibung der Modellkomponente
- Wird in Wortvektor gespeichert



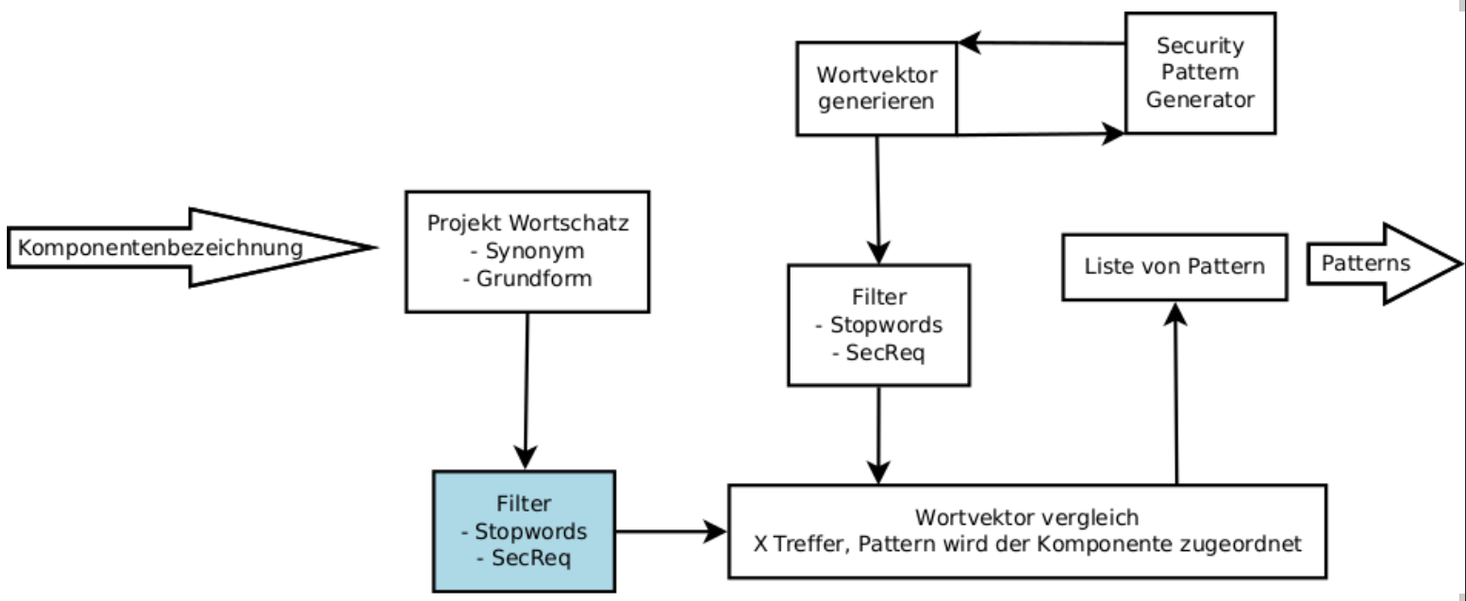
Riskfinder Algorithmus

- Zu allen Worten des Vektors wird bestimmt:
  - Grundform
  - Synonyme



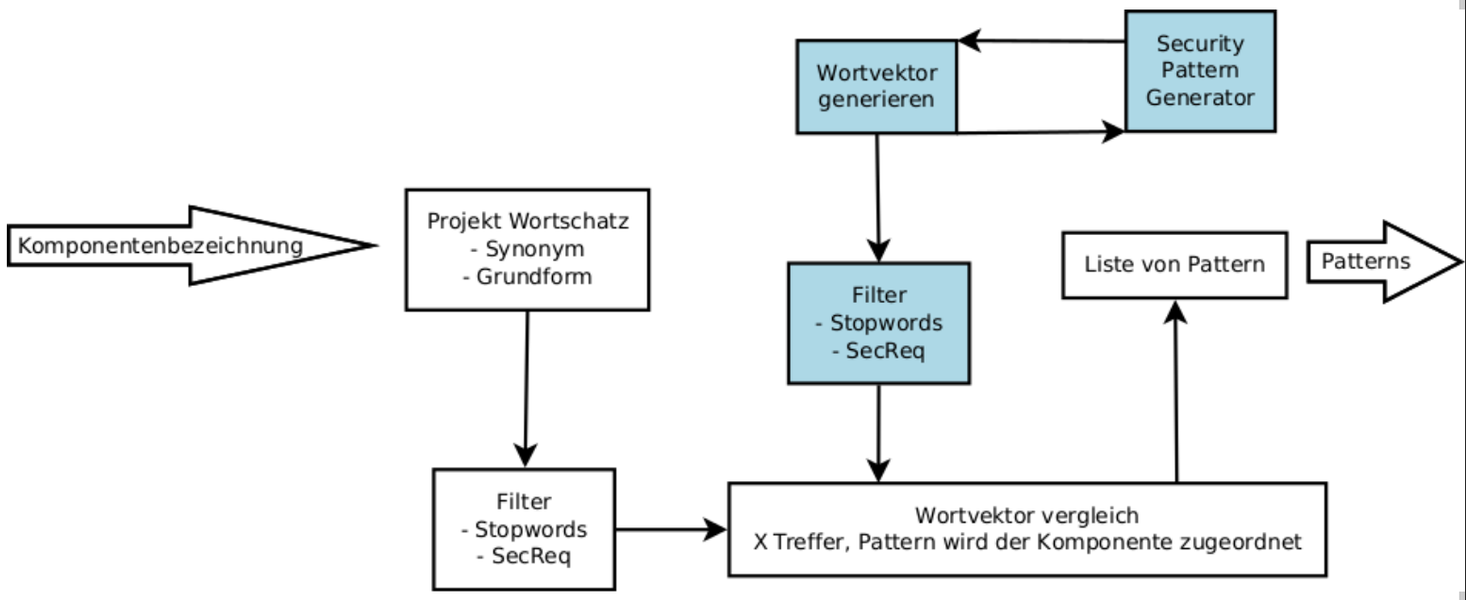
Riskfinder Algorithmus

- Filter
  - Stopwords
  - Worte die keine Sicherheits-relevanz besitzen (SecReq)



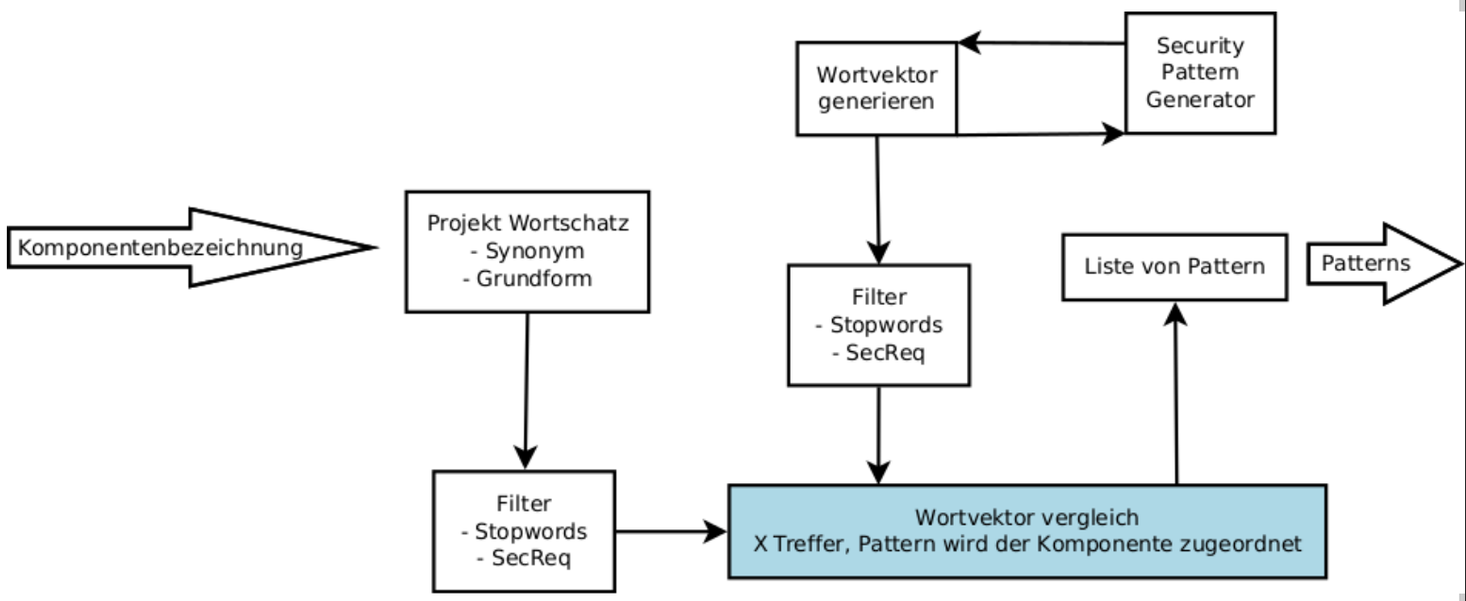
Riskfinder Algorithmus

- Aus textueller Beschreibung der Pattern (Risiken und Maßnahmen) Vektor erstellen
- Filer
- Stopwords
- SecReq



Riskfinder Algorithmus

- Wortvektoren vergleichen
- Bestimme Anzahl von Worten, die in beiden Vektoren
- bei Anzahl >= X Pattern relevant für Komponente
- Pattern der Komponente zuordnen

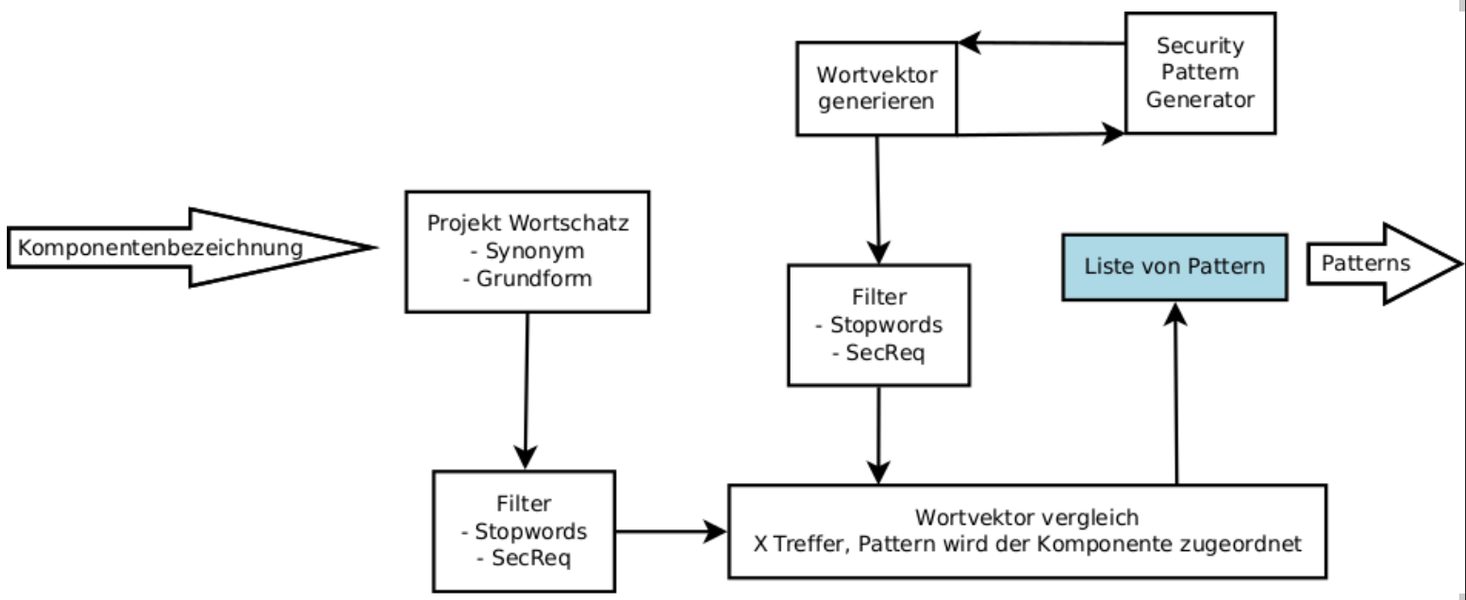


Riskfinder Algorithmus

- Ausgabe:

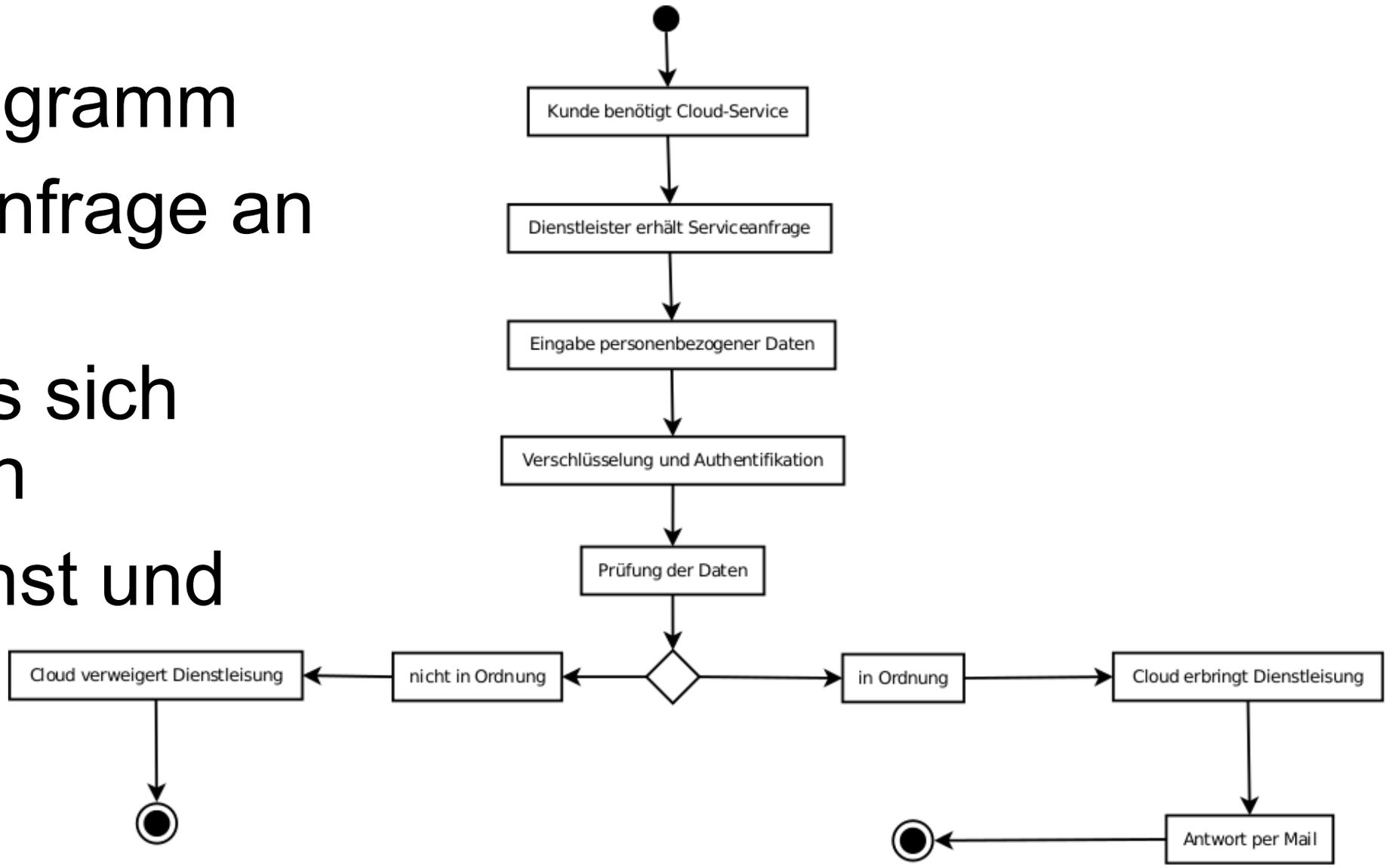
  Liste aller Modellkomponenten mit zugeordneten Patterns

- Modell je nach Relevanz der zugeordneten Patterns einfärben



Riskfinder Beispiel

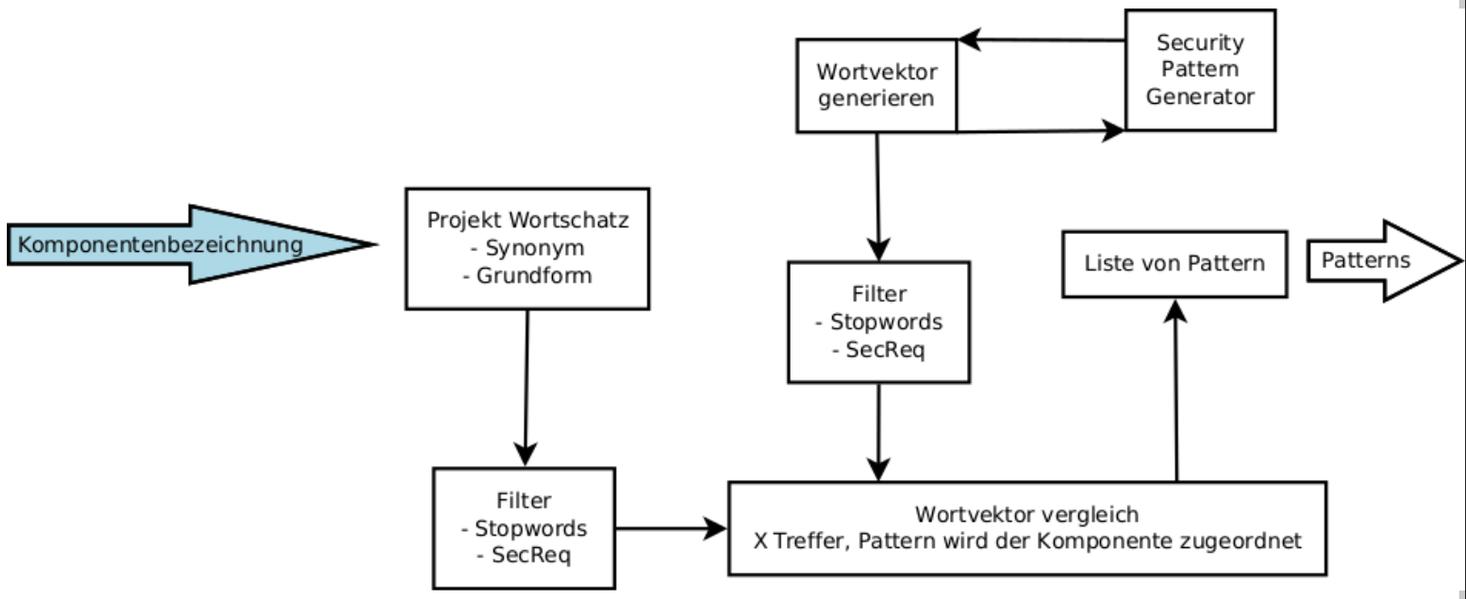
- UML Aktivitätsdiagramm
- Modelliert Anfrage an Cloud
- Nutzer muss sich Identifizieren
- Positiv: Dienst und Antwortmail



Riskfinder Beispiel

- Aktivitätsbeschreibung

< Eingabe, personenbezogener, Daten >



Riskfinder Beispiel

< Eingabe,

Antrag,

Bitte,

Gesuch,

personenbezogener,

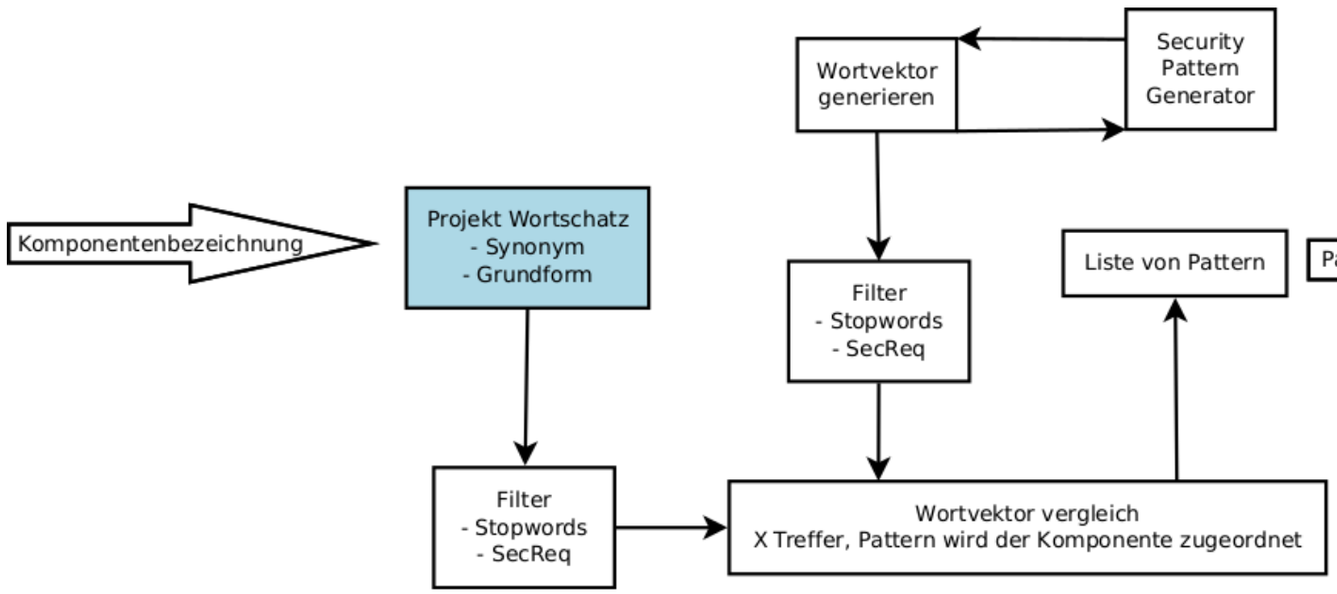
personenbezogen,

Daten,

Angaben,

Testdaten,

Dateien >



Riskfinder Beispiel

< Eingabe,

Antrag,

Bitte,

Gesuch,

personenbezogener,

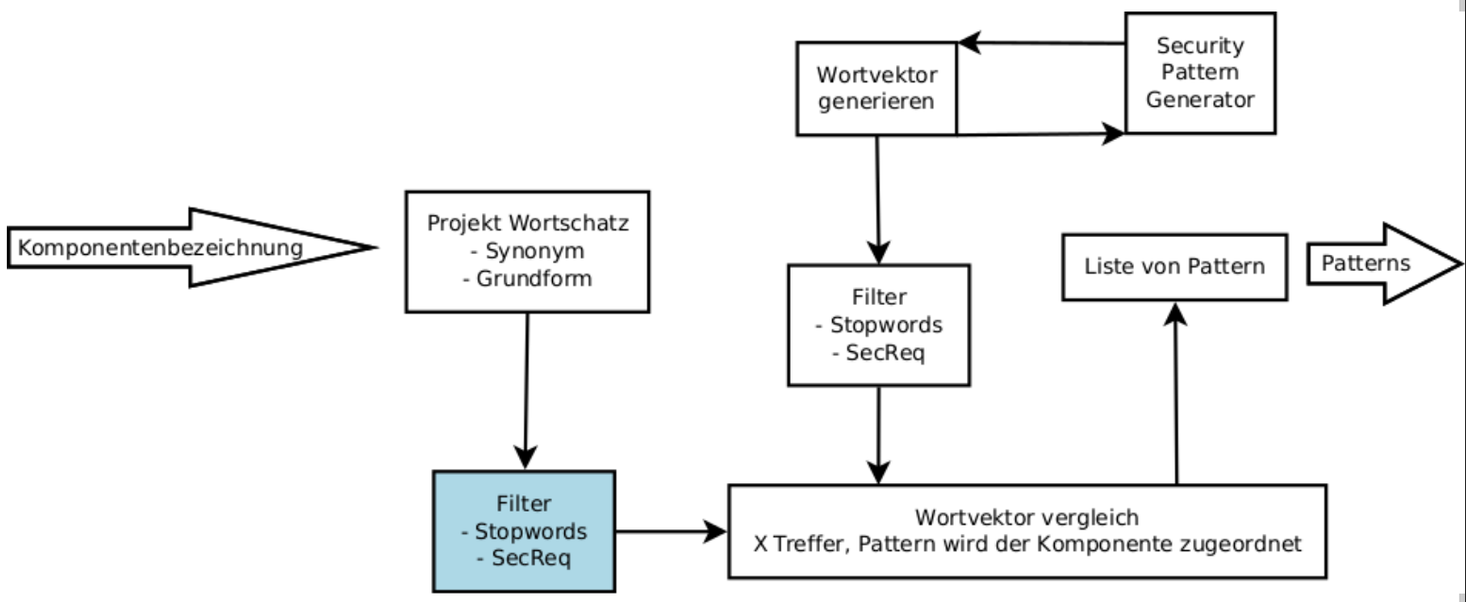
personenbezogen,

Daten,

Angaben,

Testdaten,

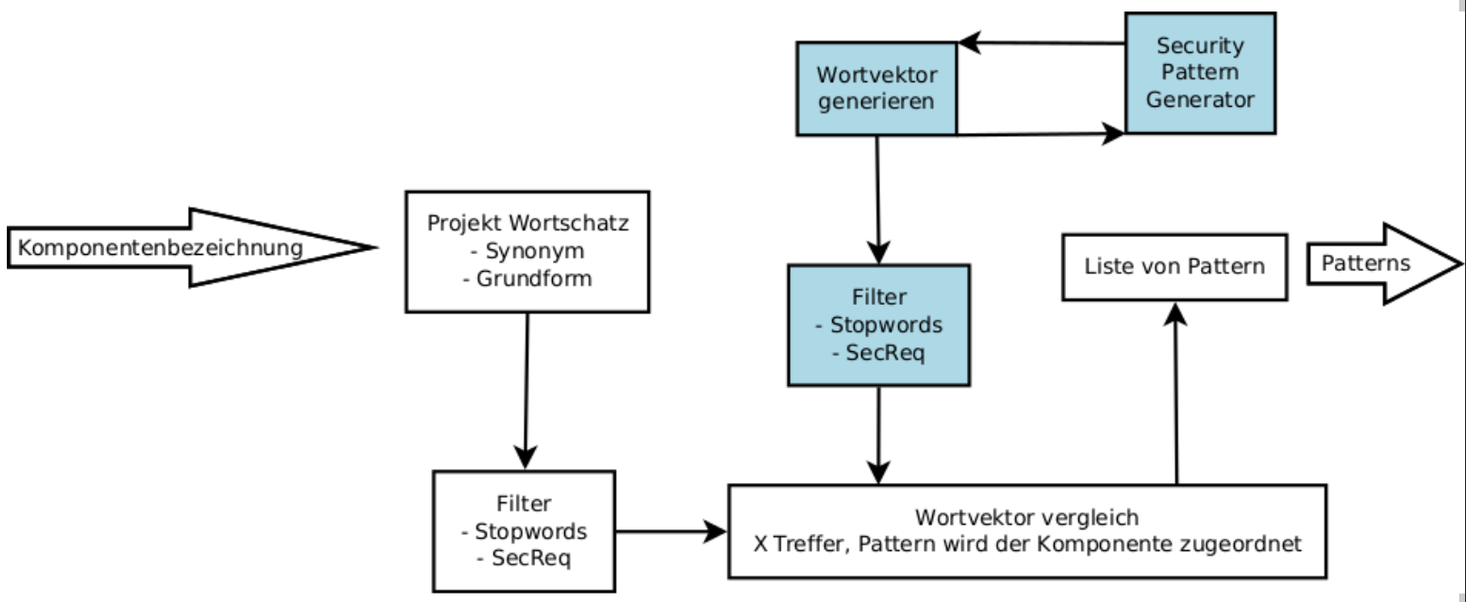
Dateien >



Riskfinder Beispiel

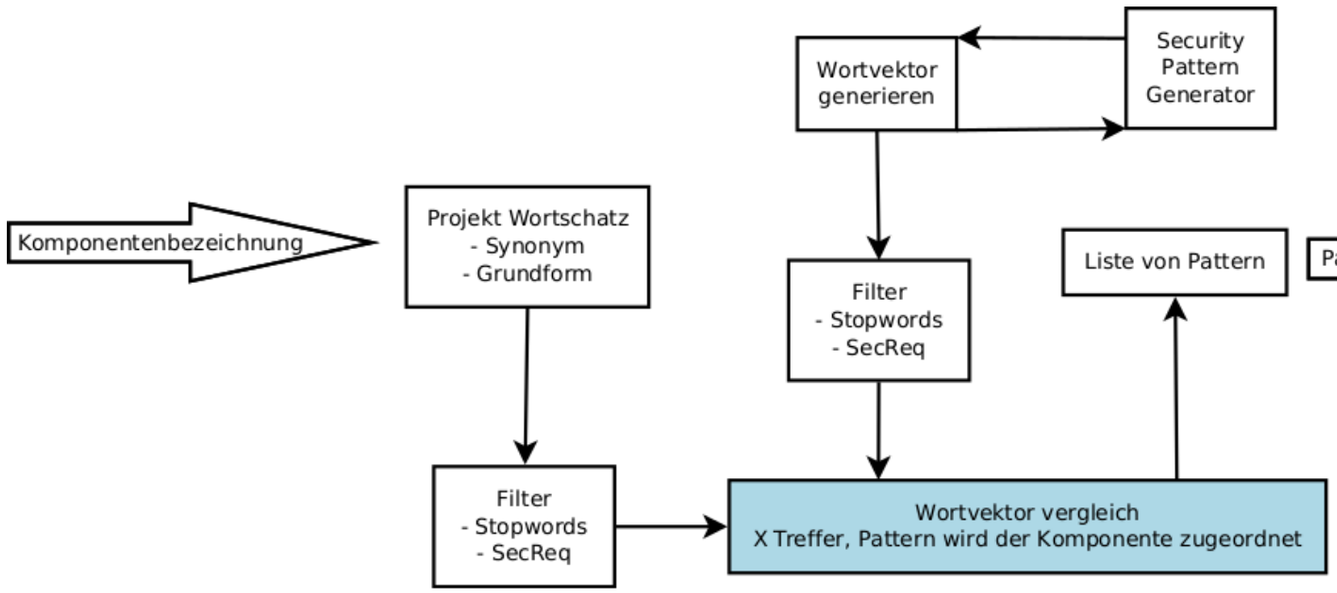
- Pattern: Datenschutz

< Dateien,
Vorgängen,
beteiligen,
Planungen,
Umgang,
personenbezogen,
betreffen,
Kenntnisse
[…] >



Riskfinder Beispiel

Vergleich der beiden Vektoren
< Eingabe,
Antrag,
[…] >
und
< […]
Dateien,
Vorgängen,
beteiligen,
[…] >



Riskfinder Beispiel

< Eingabe,
Antrag,
Bitte,
Gesuch,
personenbezogener,
personenbezogen,
Daten,
Angaben,
Testdaten,
Dateien >

Zwei Treffer

< […]
Dateien
Vorgängen,
beteiligen,
Planungen,
Umgang,
personenbezogen,
betreffen,
Kenntnisse
[…] >

Riskfinder Beispiel

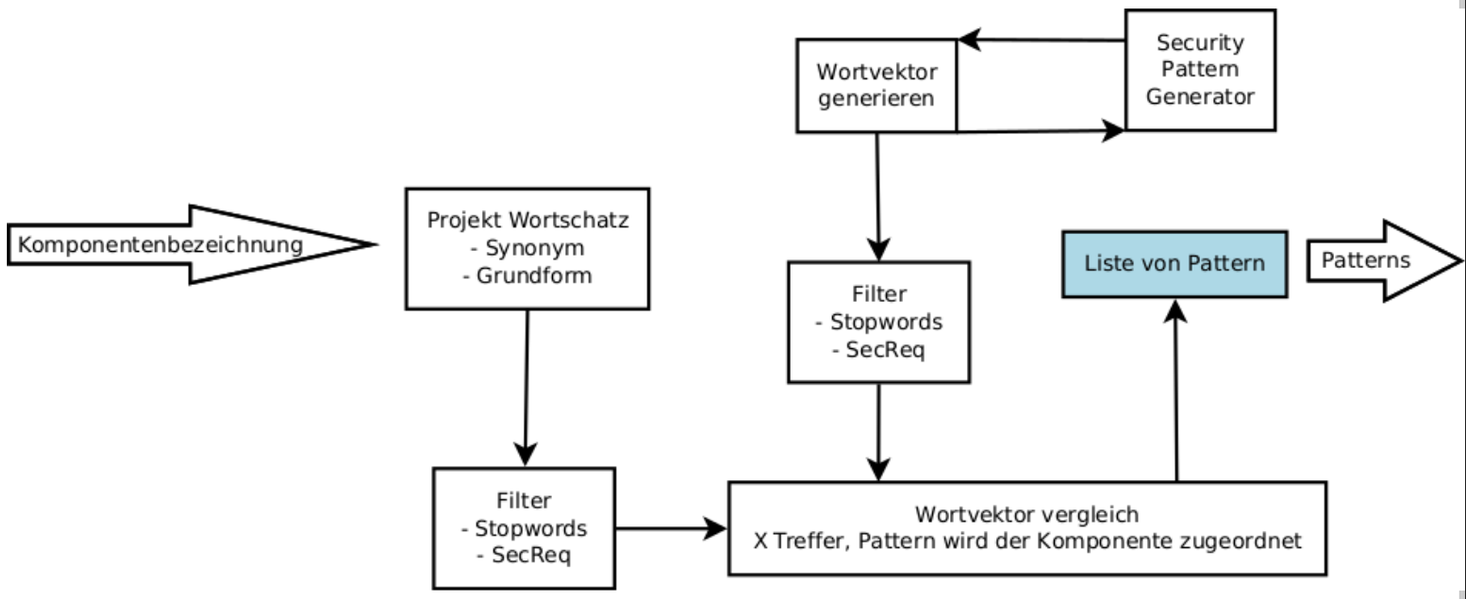
- Liste von Pattern:

[…]

[Eingabe personenbezogener Daten]:

1| B_1.5_Datenschutz

[…]



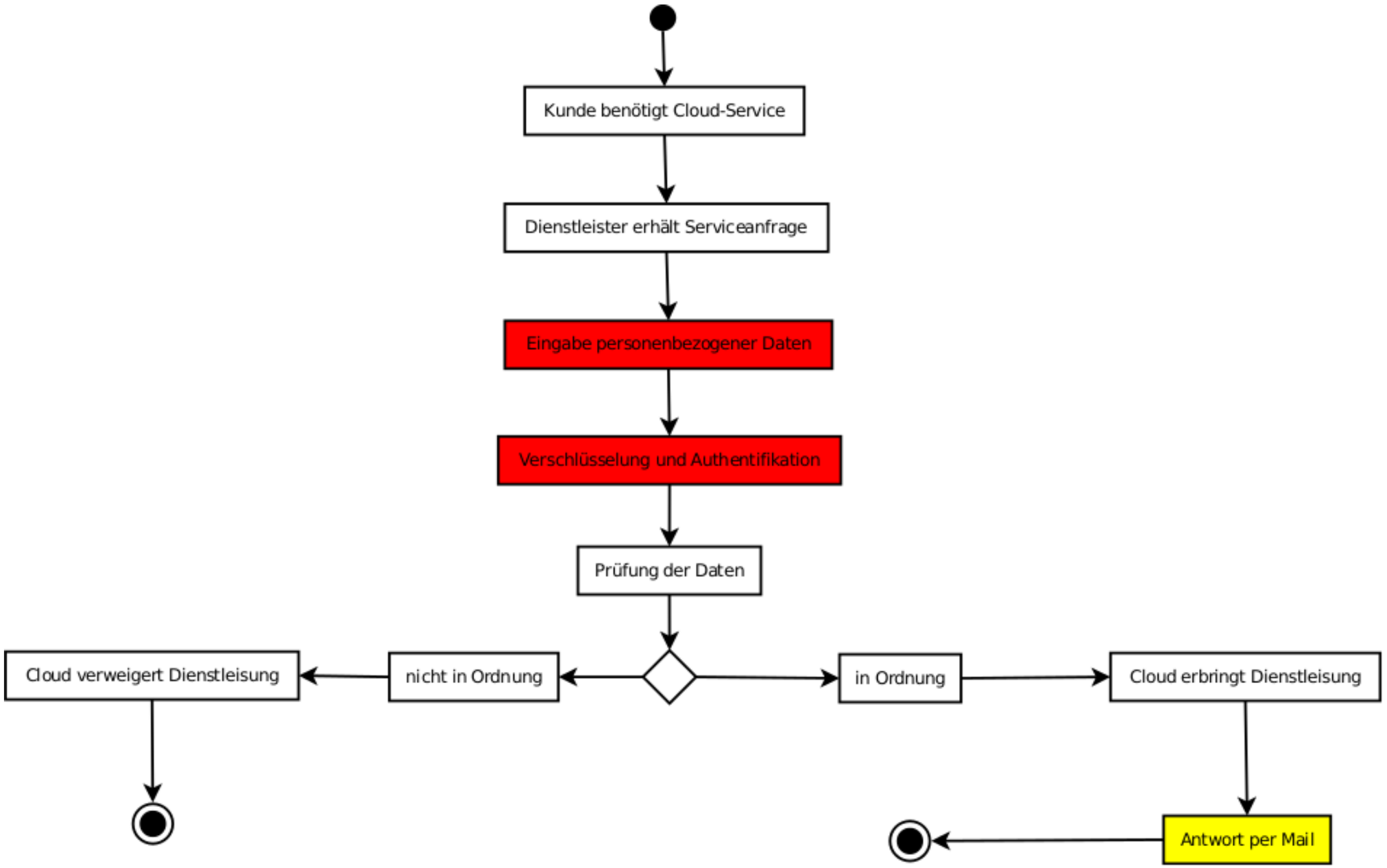
Riskfinder Beispiel

Risikoverdacht bei [Eingabe personenbezogener Daten]:
1 | B_1.5_Datenschutz
2 | B_1.7_Kryptokonzept
3 | B_1.11_Outsourcing
4 | B_1.15_Löschen_und_Vernichten_von_Daten
5 | B_2.10_Mobiler_Arbeitsplatz
6 | B_3.201_Allgemeiner_Client
7 | B_3.301_Sicherheitsgateway_Firewall
8 | B_3.302_Router_und_Switches
9 | B_4.6_WLAN
10 | B_4.4_VPN
11 | B_5.3_E-Mail

Risikoverdacht bei [Antwort per E-Mail]:
1 | B_5.3_E-Mail

[...]

Riskfinder Beispiel



Persönliche Stellungnahme

+ Simple und effektive Analyse
+ Bittet schnellen Überblick
+ Ordnet den Modellkomponenten relevante Patterns zu

- Analysiert nur Modellkomponenten
- Strukturanalyse findet nicht statt
- Kann zu redundanten/ falschen Ergebnissen führen

Zusammenfassung und Ausblick

- Compliance wird in der Softwareentwicklung immer wichtiger
- Ständig neue Anforderungen
- Werkzeugunterstützung notwendig, um diese zu Ermitteln und den Komponenten zuzuordnen
- Riskfinder bietet einen Ansatz dafür auf Grundlage der IT-Grundschutz-Kataloge
- Erweiterungen sowie weitere Einsatzgebiete möglich
  - Strukturanalyse
  - Anforderungen außerhalb des IT-Grundschutz-Katalogs
  - Standardisierung

Literatur

- Compliance-Magazin, *Compliance-Lexikon,* URL: http://www.compliancemagazin.de/compliancelexikon/
- Siv Houmb u.a., *SecReq,* URL: http://www.se.uni-hannover.de/pages/en:projekte_re_secreq/
- Bundesministerium für Justiz und für Verbraucherschutz, *Bundesdatenschutzgesetz,* URL: http://www.gesetze-im-internet.de/bdsg_1990/
- Dietmar Mueller, *Regeltreue statt Compliance,* URL: http://www.silicon.de/41502486/regeltreue-statt-compliance/
- *Oxford Advaned Learner's Dictionary 7. Auflage,* Oxford Universität, 2005
- Marc Peschke, *Werkzeuggestützte Modell-basierte Sicherheitsanalyse für IT-Sicherheitsmanagement,* TU Dortmund, 2010

Literatur

- Helma Quentmeier, *Praxishandbuch Compliance: Grundlagen, Ziele und Praxistipps für Nicht-Juristen,* Gabler, 2012
- Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutz-Katalog,* URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
- Arthur Strasser und Michael Wittke, *IT-Compliance,* URL: http://www.gi.de/nc/service/informatiklexikon/detailansicht/article/it-compliance.html
- Wortschatz Universität Leibzig, *Projekt Wortschatz,* URL: http://wortschatz.uni-leipzig.de