



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Praxistransferbericht

Einbindung von Code Compliance Checks in der SAP Software Entwicklung

Justin Becker

vorgelegt am 8. August 9834

•

Fachbereich Duales Studium Wirtschaft / Technik
Hochschule für Wirtschaft und Recht Berlin

| | |
|--------------------------------|-------------------------------|
| Name: | Justin Becker |
| Matrikelnummer: | 1233455 |
| Ausbildungsbetrieb: | SAP SE |
| Fachbereich: | FB2: Duales Studium — Technik |
| Studienjahrgang: | 2023 |
| Studiengang: | Informatik |
| Betreuerin Unternehmen: | Jenny Peter |
| Betreuerin Hochschule: | Lara Maria Stricker |
| Wortanzahl: | 1712 |

Abstract

Das Ziel dieser Arbeit besteht darin den Entwicklungsprozess von SAP Software zu vereinfachen, indem die Dienste des HANA & HANA Cloud Quality Engineering Teams der Common Service Infrastructure (CSI) Abteilung verbessert werden. Diese Dienste stellen sogenannte Code Compliance, also ob Code den SAP-Richtlinien folgt, fest. Dafür führen sie Checks durch, die einen Scan des Codes und die Bewertung der Ergebnisse des Scans umfassen.

Dieser Bericht baut darauf hinaus, wie man die Bewertung der Scan Ergebnisse auf einer technischen Ebenen so gestaltet, dass sie so streng wie nötig und so tolerant wie möglich sind. Dabei soll die Verantwortung für die Bewertung klar in dafür zuständigen Händen liegen

Inhaltsverzeichnis

| | |
|---|------------|
| Abstract | I |
| Inhaltsverzeichnis | II |
| Abbildungsverzeichnis | III |
| Tabellenverzeichnis | IV |
| Akronyme | IV |
| 1 Einleitung | 1 |
| 2 Software Entwicklung bei SAP | 2 |
| 2.1 Cloud Produkte | 3 |
| 2.2 CI/CD | 3 |
| 3 Code Compliance | 5 |
| 3.1 Beispiel | 5 |
| 3.2 Checks | 6 |
| 3.2.1 Scans | 6 |
| 3.2.2 Scan Ergebnis Bewertung | 7 |
| 4 Herausforderungen | 9 |
| 4.1 Externe Tools | 9 |
| 4.2 Code Beispiel | 9 |
| 5 Fazit | 10 |
| Literatur | 11 |
| 6 Ehrenwörtliche Erklärung | 12 |
| Ehrenwörtliche Erklärung | 12 |

Abbildungsverzeichnis

| | | |
|---|--|---|
| 1 | Produktportfolio Übersicht von SAP | 2 |
| 2 | Risikocode, da eine geöffnete Datei nicht richtig geschlossen wird (selbst geschrieben) | 5 |
| 3 | Beispiel Rego Script mit Ein- und Ausgabe (selbst geschrieben) | 7 |

Tabellenverzeichnis

Glossar

Customer Relationship Managemanagement Abteilung in Unternehmen, die sich mit ?????????

Human Resources Abteilung in Unternehmen, die sich mit ?????????

JSON Programmiersprachen unabhängiges Format zum Speicher von Daten durch eine Key-Value-Pair Zuweisung

Pipeline Abfolge von Prozessen, die aufeinander aufbauen

Policy As Code Prinzip, Richtlinien als Code mit einer Programmiersprache aufzuschreiben

Public Cloud Cloud, die von mehreren Unternehmen genutzt wird

Software as a Service komplettes Software Programm in der Cloud mit Nutzung über einen Browser

Akronyme

CCC Code Compliance Check

CI/CD Continuous Integration / Continuous Delivery

CRM Customer Relationship Managemanagement

CSI Commen Service Infrastructre

EU Europäischen Union

HHCQE HANA & HANA Cloud Quality Engineering

HR Human Resources

OPA Open Policy Agent

SaaS Software as a Service

1 Einleitung

Im Unternehmen SAP SE besteht die Notwendigkeit, dass alle Software-Entwickler die globale Entwicklungsrichtlinie von SAP und insbesondere die in dieser Richtlinie festgelegten Regeln befolgen. Die Einhaltung dieser Regeln und damit die Einhaltung der SAP Global Development-Richtlinie für alle Entwicklungseinheiten ist ungemein wichtig und obligatorisch, um jegliche rechtlichen und finanziellen Risiken, sowie Ansehensverluste für das Unternehmen zu vermeiden.

Die SAP-Abteilung CSI unterstützt Service- und Produktteams beim Programmieren, Versenden und Ausführen ihrer Services und Produkte in der Cloud. Es bietet ein Portfolio von Diensten, die eine Plattform für die Entwicklung, Veröffentlichung und den Betrieb von Cloud-nativen, konformen und produktionsbereiten Diensten und Anwendungen bilden.

Die Dienste zur Überprüfung der SAP-Entwicklungsrichtlinien werden vom Team HANA & HANA Cloud Quality Engineering (HHCQE) entwickelt und betreut. Mit sogenannten Code Compliance Checks (CCCs) werden die Richtlinien in automatisierten Entwicklungs- und Bereitstellungsprozessen überprüft und die SAP konforme Auslieferung neuer oder aktualisierter Software, z.B. zur Fehlerbehebung, gewährleistet.

In diesem Praxistransferbericht wird erarbeitet, wie solche Checks gestaltet werden, damit sie alle genannten Anforderungen erfüllen und gleichzeitig so minimalistisch bleiben, dass kein Entwickler mehr als nötig durch negative Check Ergebnisse aufgehalten wird.

2 Software Entwicklung bei SAP

Um den Umfang der Anforderung an die CCCs zu verstehen, muss erst ein Verständnis für die Entwicklung der SAP Produkte und damit auch für die Produkte selbst entstehen.

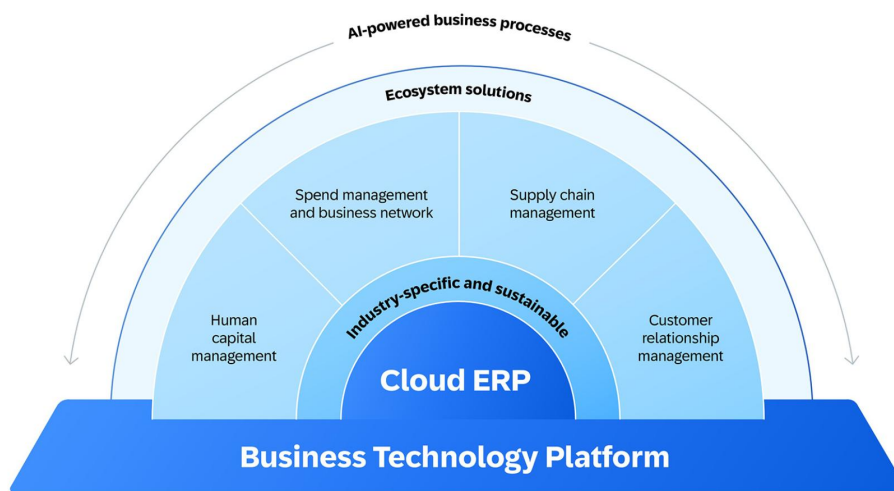


Abbildung 1: Produktportfolio Übersicht von SAP

Quelle: https://www.sap.com/intelligent-enterprise.html?url_id=banner-glo-homepage-row3-cta-who-we-are-230510

Die SAP ist eine der größten Software-Entwicklungsunternehmen weltweit und hat, wie in Abbildung 1 dargestellt, ein sehr breites Produktportfolio für ein sehr breites Kundenfeld. [2] Diese Produkte umfassen Bereiche wie Human Resources (HR), Customer Relationship Management (CRM), Branchenspezifische Lösungen und noch vieles mehr. Damit Kunden in der Benutzung eine klare und einheitliche Handhabung erfahren können, muss auch jeder — Code des Produktes, jedes Produkt als Software Komponente — genauso gestaltet sein. Nicht nur das – sämtliche SAP Produkte sollten kongruent zueinander sein, da bei Kunden nicht das Gefühl entstehen darf, sie müssten mit jedem Produkt etwas komplett neuartiges erlernen. Dies würde Kunden davon abhalten in weitere SAP Produkte zu investieren. [Hier ne passende quelle waere cool]

2.1 Cloud Produkte

Die Strategie der SAP sieht es vor, dass möglichst viele dieser Produkte in einer Public Cloud als Software as a Service (SaaS) verfügbar sind [5]. Die Entwicklung von Cloud Produkten hat unter anderem den Vorteile, dass Kunden nicht in eigen Hardware und Infrastruktur investieren müssen und damit flexibel bleiben. Da Cloud Produkte meist in einem Abonnement Modell verkauft werden, ist ein Vorteil für die SAP konstante und kalkulierbare Einnahmen. Deshalb bauen aktuelle SAP Produkte auf diesem Prinzip auf wie in Abbildung 1 zu sehen. [4]

Damit die Entwicklung der Produkte entsprechend der erklärten Prinzipien abläuft, gibt es Abteilungen, die sich darauf fokussieren den Cloud Entwicklungsprozess zu vereinfachen. So bietet CSI eine einheitliche Infrastruktur für diese Entwicklungsprozess. So kann als Teil dieser Infrastruktur überprüft werden, ob alle Anforderungen an den Code des Produktes erfüllt sind, ob der Code compliant ist.

Umgesetzt werden diese Anforderungen als Teil des Continuous Integration / Continuous Delivery (CI/CD) Prozesses.

2.2 CI/CD

Da die Cloud Produkte komplett von SAP verwaltet werden, ergibt sich außerdem der wichtige Vorteil für die SAP und die Kunden, dass die Entwicklungsteams bei SAP den Code von Produkten jederzeit anpassen und an den Kunden ausliefern kann. Somit können schnell Fehler verbessert, Feedback des Kunden umgesetzt und agil gearbeitet werden. So entsteht mehr Produktwert für die Kunden und ihre Zufriedenheit steigt.

Diesen Prozess wird CI/CD genannt. Jeder Entwickler integriert kontinuierlich neue Änderungen in den Code, welche dann kontinuierlich an den Kunden geliefert werden. Umgesetzt wird dieser Prozess durch die Automatisierung mit sogenannten CI/CD Pipelines. Diese Pipelines übernehmen alle für die Auslieferung nötigen Schritte wie zum Beispiel die Build-, Test- und Deploy-Vorgänge und ermöglichen damit erst CI/CD. [6]

Durch den schnellen Entwicklungsprozess entsteht schnell Code der nicht mehr compliant ist. Deshalb ist es ein unerlässlicher Schritt die Code Compliance vor dem

Ausliefern als Teil der CI/CD Pipelines festzustellen. Deshalb werden CCCs als eben solch ein Schritt eingeführt.

3 Code Compliance

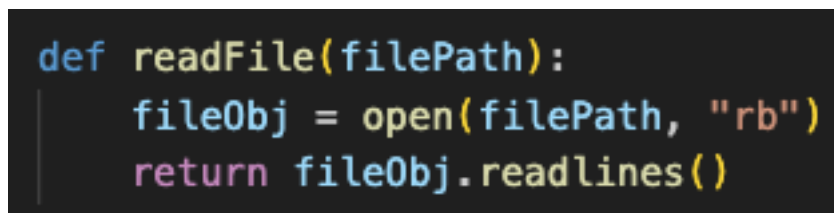
In den CCCs geht es darum die Compliance von Code festzustellen, aber es wurde noch gar nicht geklärt, was damit gemeint ist.

Damit ist gemeint, dass der Code alle ihn betreffenden Richtlinien erfüllt. Das können Richtlinien von Staatlichen Institutionen wie der Europäischen Union (EU) oder Deutschland sein, Richtlinien, die für das ganze Unternehmen, hier SAP, gelten, aber auch Richtlinien die nur für bestimmte Abteilungen gelten.

Deshalb ist für diese Arbeit interessant, wie die Richtlinien von SAP genutzt werden können. Diese umfassen unter anderem Regeln zum Qualitätsmanagement, zur Export Kontrollklassifizierung, Opensource Lizenzvalidierung und diverse Überprüfungen der Sicherheitsanforderungen.

3.1 Beispiel

Ein konkretes Beispiel Code der ein Sicherheitsrisiko ist und damit eventuell für nicht compliance verantwortlich ist, ist die in Abbildung 2 dargestellte Funktion.



```
def readFile(filePath):  
    fileObj = open(filePath, "rb")  
    return fileObj.readlines()
```

Abbildung 2: Risikocode, da eine geöffnete Datei nicht richtig geschlossen wird (selbst geschrieben)

Solche Fehler könnten zu unerwartetem Verhalten während der Laufzeit führen. Deshalb müssen sie bereits davor erkannt werden. Da eine Überprüfung per Hand fehleranfällig und langsam ist, braucht es hierfür eine Automatisierung. Diese Automatisierung wird Check genannt.

3.2 Checks

Damit ergibt sich als Ziel von den CCCs in den CI/CD Pipelines, dass sie das Ergebnis liefern sollen, ob der Code, der mit der Pipeline ausgeliefert werden soll, allen gegebenen Richtlinien folgt und damit compliant ist. Außerdem müssen sie eine Begründung für diese Entscheidung an die Entwickler liefern, damit dieser seinen Code entsprechend verbessern kann.

Dafür sind CCCs in zwei Teile aufgeteilt:

- ein Scan, der den Code analysiert und feststellt welche —Richtlinien relevante Risikostellen—— u.ä. existieren
- die Bewertung von den Ergebnissen diesen Scans nach den Richtlinien

Da die Richtlinien Anforderungen unterschiedlichster Themenbereich wie zum Beispiel der Export Kontrollklassifizierung bis zu Sicherheit enthalten, wird die Gesamtfeststellung - compliant oder nicht - in mehrere Teilchecks unterteilt, sodass solch ein Check einen Aspekt der Richtlinien übernimmt.

3.2.1 Scans

Das Scannen von Code wird von externen Tools übernommen. Zum aufrufen dieser Tools wird eine interne Version des Project Piper genutzt. Piper vereinfacht unterschiedlichste Schritte, die in einer Pipeline ausgeführt werden können – so zum Beispiel auch das aufrufen von eben solchen externen Scan Tools.

Es gibt zum Beispiel in dem Bereich der Sicherheitsanalyse von Code eine Reihe geeigneter Tools wie Checkmarx oder Fortify, die unter anderem in dem HHCQE Team genutzt werden. [3] Solche Tools würden ein Risikostelle wie in Abbildung 2 erkennen und als „Improper_Resource_Shutdown_or_Release“ einordnen. [1]

Dann wird von dem Scan eine Datei erzeugt, die enthält welche Risikostellen gefunden wurden. Zudem ist in solcher Datei meist eine Priorisierung, wie schwerwiegend die Risikostellen sind, enthalten.

Diese Datei stellt nun das Ergebnis des Scans da und liegt im JSON Format vor.

Außerdem besitzen externe Tools wie Checkmarx oft eine Weboberfläche, in der Details eines Scans mit den genauen Zeilen an Code, die Risikostellen sind, eingesehen werden können. In diesen Rahmen gibt es dann die Möglichkeit diese Risikostellen als unbedenklich zu markieren. Richtlinien beziehen sich oft darauf, wie viele von den Risikostellen als unbedenklich eingestuft werden müssen.

3.2.2 Scan Ergebnis Bewertung

In der Bewertung der Ergebnisse muss nun auf Grundlage der erzeugten Datei die Entscheidung getroffen, ob der Code compliant oder nicht ist. Bisher wurde diese Entscheidung nicht klar nach den Richtlinien getroffen. Stattdessen wurde sie von Piper übernommen. Problem ist, dass dieser Prozess mit Piper nicht durchsichtig ist und keine Verantwortungen eindeutig geklärt sind. Es bedarf einer Lösung, die flexibel, falls sich die Anforderungen an Code und damit die Richtlinien ändern, und nachvollziehbar, sodass immer klar ist auf welcher Grundlage die Entscheidung getroffen wurde, ist.

Von der SAP Abteilung Hyperspace werden seit neusten Richtlinien in einem Policy As Code Format bereitgestellt. Diese Richtlinien sind in der sogenannten Rego Programmiersprache formuliert, die mit dem Open Policy Agent (OPA) angewandt werden können. Dieser OPA wird wiederum von Hyperspace genutzt.

| <pre>package example import rego.v1 default compliant := false compliant if { input.vulnerabilities < 10 }</pre> | <table><tr><th colspan="2">INPUT</th></tr><tr><td>1</td><td>{</td></tr><tr><td>2</td><td> "vulnerabilities": 10</td></tr><tr><td>3</td><td>}</td></tr><tr><th colspan="2">DATA</th></tr><tr><th colspan="2">OUTPUT</th></tr><tr><td colspan="2">Found 1 result in 89µs.</td></tr><tr><td>1</td><td>{</td></tr><tr><td>2</td><td> "compliant": false</td></tr><tr><td>3</td><td>}</td></tr></table> | INPUT | | 1 | { | 2 | "vulnerabilities": 10 | 3 | } | DATA | | OUTPUT | | Found 1 result in 89µs. | | 1 | { | 2 | "compliant": false | 3 | } |
|--|--|-------|--|---|---|---|-----------------------|---|---|------|--|--------|--|-------------------------|--|---|---|---|--------------------|---|---|
| INPUT | | | | | | | | | | | | | | | | | | | | | |
| 1 | { | | | | | | | | | | | | | | | | | | | | |
| 2 | "vulnerabilities": 10 | | | | | | | | | | | | | | | | | | | | |
| 3 | } | | | | | | | | | | | | | | | | | | | | |
| DATA | | | | | | | | | | | | | | | | | | | | | |
| OUTPUT | | | | | | | | | | | | | | | | | | | | | |
| Found 1 result in 89µs. | | | | | | | | | | | | | | | | | | | | | |
| 1 | { | | | | | | | | | | | | | | | | | | | | |
| 2 | "compliant": false | | | | | | | | | | | | | | | | | | | | |
| 3 | } | | | | | | | | | | | | | | | | | | | | |

Abbildung 3: Beispiel Rego Script mit Ein- und Ausgabe (selbst geschrieben)

Das in Abbildung 3 zu sehende Script ist immer eindeutig, transparent und schnell anzupassen. Die verwendete Rego Programmiersprache ist außerdem dafür optimiert Richtlinien anzuwenden. Damit ist der OPA mit Rego für die genannten Anforderungen geeignet. [7]

Genutzt werden können diese Richtlinien von Hyperspace in zwei Schritten.

Als erstes wird die Ergebnisdatei des Scans auf einen Server von Hyperspace hochgeladen. Außerdem ist in dem Upload noch eine sogenannter Policy Key (Deutsch: Richtlinien Schlüssel) enthalten, der eindeutig zuordnet, welche Richtlinie für das Ergebnis genutzt werden soll. So können dann die Ergebnisse des Scans bei Hyperspace mit Hilfe von OPA ausgewertet werden.

Im zweiten Schritt müssen die Auswertungsergebnisse dann innerhalb der Pipeline nutzbar gemacht werden. Dafür wird eine Anfrage an den Hyperspace Server geschickt, der eine Datei mit der Auswertung zurückgibt. Diese Datei enthält im JSON Format die Information, ob der gescannte Code der Richtlinie mit gegebenen Policy Key entspricht oder nicht.

Da die Evaluation auf dem Hyperspace Server asynchron läuft und nicht klar ist, wann die Auswertung zur Verfügung steht, wird ein Fallback-Mechanismus implementiert, der diese zweite Anfrage in größer werdenden Zeitabständen bis zu fünf Mal wiederholt. Wenn es nach dem fünften Versuch kein Ergebnis gibt, bricht die Bewertung ab und das Check Gesamtergebnis wird als unbekannt gesetzt.

Damit für den Endbenutzer dieser Entscheidungsfindungsprozess nachvollziehbar bleibt, werden mit einer dritten Anfrage an den Hyperspace Server Details zu der Auswertung abgerufen. Diese Details werden dem Benutzer zusätzlich zu dem eigentlichen Auswertungsergebnis - compliant oder nicht - angezeigt. Sie enthalten Informationen wie den Namen der Richtlinie, eine Kurzbeschreibung, die URL zu der genutzten Richtlinie im Policy As Code Format sowie noch einiges mehr.

4 Herausforderungen

Es kommt immer zu viele vielen Herausforderungen die da sind...

4.1 Externe Tools

Kommunikation ist key!

4.2 Code Beispiel

Es ist wirklich nicht leicht anständigen Code zu schreiben.

5 Fazit

Und das beste kommt zum Schluss di da du. . .

Literatur

- [1] Dharmendra Ahuja. *Python Security Made Easy: Fixing Security Vulnerabilities with Checkmarx !* 2023. URL: <https://medium.com/@dharmendradevops11/python-security-made-easy-fixing-security-vulnerabilities-with-checkmarx-aa7b3ff28b7a> (besucht am 19.03.2024).
- [2] SAP Globale Corporate Communications. *SAP Corporate Fact Sheet*. Techn. Ber. SAP SE, 2024. URL: <https://www.sap.com/documents/2017/04/4666ecdd-b67c-0010-82c7-eda71af511fa.html>.
- [3] Florian Maler John Breeden. *Die besten DAST- und SAST-Tools*. 2024. URL: <https://www.csoonline.com/de/a/die-besten-dast-und-sast-tools,3673878> (besucht am 19.03.2024).
- [4] Sebastian Minnich. *Die Vorteile und Nachteile des Cloud-Computing*. 2017. URL: <https://www.heise.de/download/blog/Die-Vorteile-und-Nachteile-des-Cloud-Computing-3713041> (besucht am 17.03.2024).
- [5] o.V. *SAP Cloud Strategy*. URL: <https://sapinsider.org/topic/sap-platform-technology/sap-cloud-strategy/> (besucht am 17.03.2024).
- [6] o.V. *What is CI/CD?* 2023. URL: <https://www.redhat.com/en/topics/devops/what-is-ci-cd> (besucht am 17.03.2024).
- [7] *Policy Language*. URL: <https://www.openpolicyagent.org/docs/latest/policy-language/> (besucht am 19.03.2024).

6 Ehrenwörtliche Erklärung

Ich erkläre ehrenwörtlich:

1. dass ich meine Bachelor-Thesis selbstständig verfasst habe,
2. dass ich die Übernahme wörtlicher Zitate aus der Literatur sowie die Verwendung der Gedanken anderer Autoren an den entsprechenden Stellen innerhalb der Arbeit gekennzeichnet habe,
3. dass ich meine Bachelor-Thesis bei keiner anderen Prüfung vorgelegt habe.

Ich bin mir bewusst, dass eine falsche Erklärung rechtliche Folgen haben wird.

Ort, Datum

Justin Becker