Workshop “Evaluation of Service-APIs – ESAPI 2020“

Motto: APIs als Klebstoff einer allumfassenden Digitalisierung

detaillierter Bericht

Sandro Hartenstein[2], Konrad Nadobny[1, 2, 3],
Steven Schmidt[2, 4], Andreas Schmietendorf[1, 2]

[1]OvG-Universität Magdeburg, [2]HWR Berlin,

[3]Bayer AG, [4]Deutsche Bahn AG

1. Motivation und Themen des Workshops

Die Gartner Group[1] geht davon aus, dass im Jahr 2021 mehr als 60% aller Anwendungsentwicklungen von eingesetzten Web-APIs profitieren. Diese mit Hilfe klassischer Internettechnologien zur Verfügung gestellten Web-APIs bieten die Möglichkeit eines konsistenten Zugriffs auf fachlich begründete Informationen und Funktionen aber auch auf komplette Geschäftsprozesse. Neben einer unternehmens- und branchenübergreifenden Integration existierender Softwarelösungen wird dabei auch die Zielstellung einer kompositorischen und damit agilen Softwareentwicklung verfolgt. Aufgrund der ggf. „ad hoc“ zusammengesetzten Lösungen muss auch der Betrieb mit diesen Herausforderungen umgehen können. Daher kommt der Themenstellung „DevOps“ als Klammer zwischen Entwicklung und Betrieb eine besondere Bedeutung zu.

Der ESAPI-Workshop im Jahr 2020 fokussierte die folgenden Themen:

- Bewertung von Vertrauen und Sicherheit bei Web-APIs.
- Branchenspezifische Ansätze zur Spezifikation von Web-APIs.
- Lowcode bzw. Codeless Softwareentwicklung mit Web-APIs.
- Effiziente Ansätze zur „API-fizierung“ von Altanwendungen.
- Risiken bei über Web-APIs bezogenen KI-Algorithmen.
- Vor- und Nachteile von GraphQL-basierten Web-APIs.
- Elemente eines DevOps-orientierten API-Managements.
- Serverless bereitgestellte Web-APIs – Fiktion oder Wirklichkeit?

Der ursprünglich als Präsenzveranstaltung geplante Workshop wurde im Jahr 2020 erstmals online durchgeführt. Mehr als 40 Teilnehmer hatten sich im Rahmen der virtuellen Konferenz zusammengefunden. Erstmals wurde die Veranstaltung von der Bayer AG in Berlin gehostet.

[1] Quelle: Zumerle, D. et al. 2019. API Security. What You Need to Do to Protect Your APIs [online]. Verfügbar unter https://www.gartner.com/en/documents/3956746/api-security-what-you-need-to-do-to-protect-your-apis

2. Beiträge zum Workshop

Im Vorfeld wurde ein entsprechender Call for Paper innerhalb der Community verteilt, auf dessen Basis 11 Beiträge für den Workshop ausgewählt wurden. Um den speziellen Herausforderungen einer Online-Veranstaltung zu genügen, wurden die Beiträge als Keynote, als 10minütige Themen-Pitches oder mit Hilfe parallel bereitgestellter Poster präsentiert.

Anja Fiegler, Andreas Schmietendorf
: Entwicklung smarter Anwendungen mit Hilfe cloudbasiert angebotener KI-Algorithmen;

Niko Zenker, Daniel Paschek, Marvin Leine
: Einsatz einer gewichteten Graphendatenbank zur Abbildung komplexer Unternehmensarchitekturen;

Konrad Nadobny
: Vergleich von Enterprise API-Management-Lösungen;

Steven Schmidt
: Schaffung eines vertrauenswürdigen, öffentlichen WLAN - Herangehensweise und Teilergebnisse;

Michael Petry, Volker Reers, Frank Simon
: Reaktive, minimal destruktive API-Härtung am Beispiel von GraphQL;

Jens Borchers
: Zero Trust-Architektur und -Kultur;

Daniel Kant, Andreas Johannsen
: Exemplarische API-Schwachstellen bei IoT-Geräten auf der Grundlage von OWASP API Security TOP 10;

Gabriel Landa, Sandro Hartenstein
: Bitcoin Blockchain via Satelliten;

Kadir Ider
: Effective Privacy Management Concepts: Increasing Privacy Control by Reducing Complexity;

Maximilian Müller, Matthias Dobkowicz, Andreas Johannsen, Allan Fodi
: Konzeption eines Objektkonfigurators zur Erstellung von Auszügen einer Objektbibliothek;

Sandro Hartenstein
: Entwicklung vertrauenswürdiger Web-APIs.

3. Ergebnisse der Breakaout-Diskussionen

Der Tradition des Workshops entsprechend galt es, ein World Cafe erstmals virtuell, mit Hilfe von „Breack Out Sessions durchzuführen. Die Teilnehmer wurden zunächst in drei Gruppen aufgeteilt und dann jeweils einem Diskussionsraum zugeteilt. Jedem dieser Diskussionsräume war ein fester Moderator zugeteilt, welcher den Austausch leitete und die Ergebnisse auf einem gemeinsamen Whiteboard dokumentierte. Nach 15 Minuten wechselten die Gruppen den Diskussionsraum, so dass sie sich nun zu einem weiteren Thema austauschen konnten. Dabei bauten sie auf den Ergebnissen der vorherigen Gruppe auf. Nach weiteren 15 Minuten wurde der Diskussionsraum abermals gewechselt.

Massive APIfizierung von Legacy Applikationen

Das Thema der massiven APIfizierung von Legacy Applikationen wurde kontrovers diskutiert, wobei das Ergebnis in der Abbildung auf der folgenden Seite dargestellt ist. Das Thema gliedert sich in die Teilbereiche Standardisierung, Vernetzung und Verschlankung. Im Laufe der Diskussion wurde zudem herausgearbeitet, dass auch Aspekte wie Kultur und Innovation in diesem Kontext eine große Rolle spielen. So bedarf es einer offenen, kollaborativen Kultur mit dem Ziel, dass möglichst alle Daten und Funktionalitäten als API angeboten und standardkonform implementiert und dokumentiert werden (Open API). Die Zielvorstellung ist somit ein Konnektivitäts-Ökosystem, in dem alle Akteure sich einfach und effizient austauschen können. Systeme sind im Idealfall in Echtzeit integierbar und ermöglichen ein Agieren ohne Medienbrüche und Inkonsistenzen.

Die Motivation für eine API-getriebene IT-Architektur im Allgemeinen und die dementsprechend benötigte massive APIfizierung von Altsystemen im Speziellen begründet sich im folgenden Sachverhalt:

Etablierung gemeinsamer Standards und Normen zur Reduktion der Komplexität. Auf dieser Grundlage lassen sich Standardlösungen einfacher und vor allem effizienter bereitstellen. Darüber hinaus bietet sich die Möglichkeit, historisch gewachsene Systemlandschaften zu entwirren (d.h. entkoppeln) und die Strukturen sukzessive zu modernisieren.

In Bezug auf Legacy-Applikationen muss beachtet werden, dass die Systeme oftmals über komplexe, historisch gewachsene Businesslogiken verfügen, die nicht verloren gehen dürfen. Mithilfe eines API-Wrappers können diese zum Beispiel hinter einer API-Fassade verborgen werden, so dass das Altsystem modernisiert und endkoppelt werden kann. Die ursprüngliche Kernfunktion bleibt dabei erhalten, so dass es wie gehabt weiter betrieben werden kann. API-Wrapper können somit als Brückentechnologie genutzt werden, um monolithische Systeme

zunächst mit einer Standardschnittstelle zu ertüchtigen und dann nach und nach aufzubrechen. Dies erleichtert nicht nur die Systemintegration, sondern ermöglicht auch einen Wandel weg von lokal optimierten Lösungen (Best of Breed) hin zu ganzheitlichen, integrierten Systemlandschaften (Best of Suite).

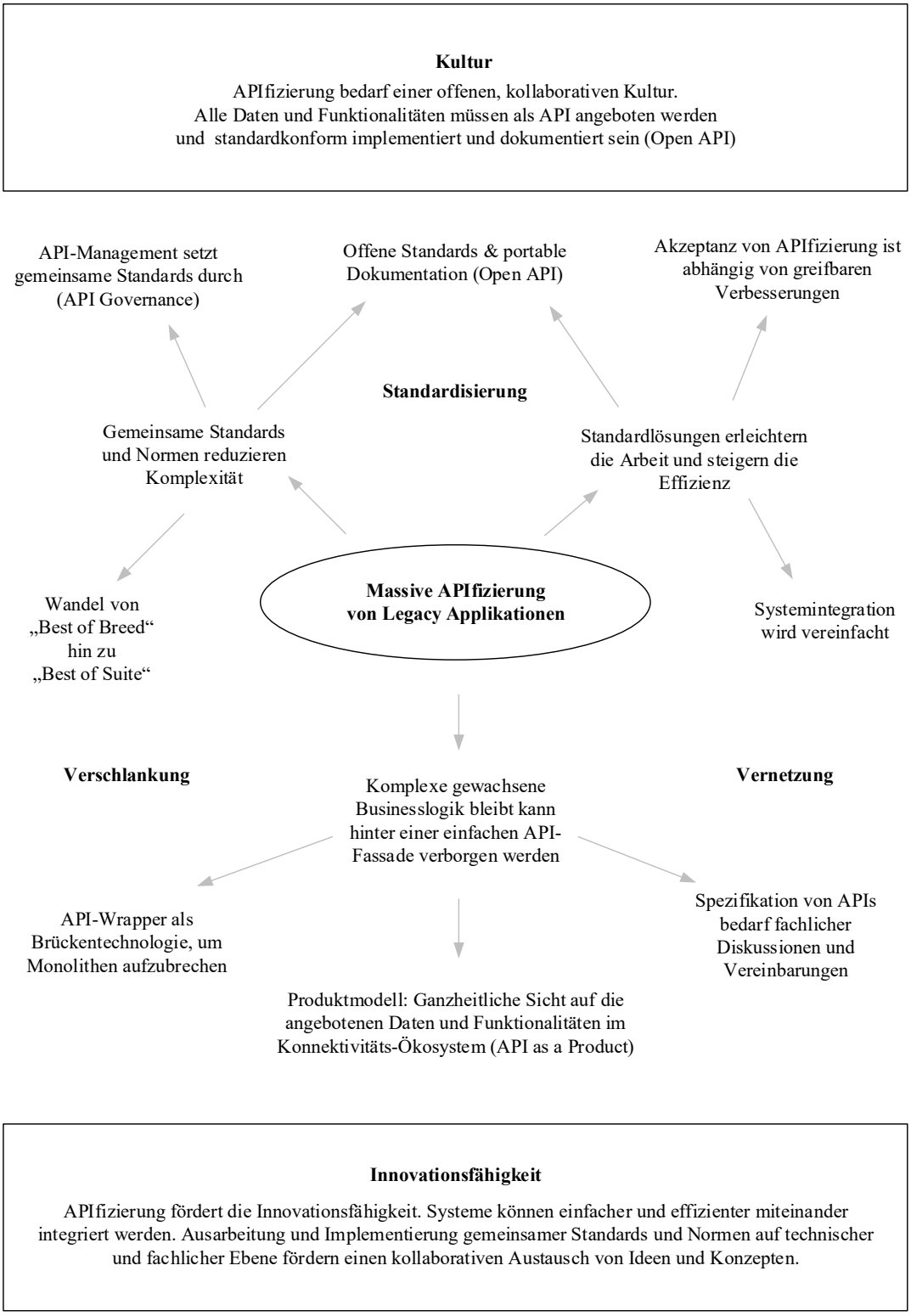

Abbildung 1: Ergebnis der Diskussion

Die Akzeptanz einer API-getriebenen Transformation ist abhängig von greifbaren Verbesserungen. Aus technischer, betrieblicher und organisatorischer Sicht ist

zunächst ein professionelles API-Management zum Durchsetzen der gemeinsamen Standards unerlässlich (API Governance). In Bezug auf Daten und Funktionalitäten müssen diese Standards auf fachlicher Ebene diskutiert und vereinbart werden. Diese gemeinsamen Standards, Regeln und Normen reduzieren im Nachgang die Komplexität und vereinfachen den späteren Austausch. Idealerweise werden dabei bereits existierende Industriestandards, wie zum Beispiel domänenspezifische Datenmodelle, implementiert.

Vertrauen in Public WIFI-Infrastrukturen

In diesem World Cafe wurden zentrale Fragen zur Einstellung der Diskussionsteilnehmer gegenüber der Vertrauenswürdigkeit öffentlicher WLANs diskutiert. Einstiegspunkt war dabei die Grundsatzfrage, inwiefern überhaupt öffentlichen WLANs vertraut wird. Das Feedback über die verschiedenen Diskussionsrunden hinweg war stark diversifiziert. Im Wesentlichen wird öffentlichen WLANs nicht vertraut. Häufige Antworten haben aber teilweise nach Anbieter bzw. angebotenem Serviceumfang unterschieden, oder die Entscheidung einer eigenen, kurzen Prüfung verschiedener Datensicherheitseigenschaften vorbehalten.

Im Hinblick auf die Fragestellung zur Relevanz der Vertrauenswürdigkeit für die Nutzung des jeweiligen WLAN-Angebotes müsse nach Meinung der Teilnehmer grundsätzlich zwischen beruflicher und privater Verwendung unterschieden werden. Im privaten Kontext war die Auswirkung auf die tatsächliche Nutzung häufiger irrelevant, im beruflichen oder professionellen Kontext gab es jedoch starke Abhängigkeiten.

Der dritte Diskussionsgegenstand bewegte sich im Bereich vertrauensschaffender Maßnahmen, welche der Service aufweisen müsste, um als relativ vertrauenswürdig zu gelten. Hierbei war in allen Diskussionsrunden der grundsätzliche Konsens erkennbar, dass sich Maßnahmen nicht auf eine rein technische Dimension beschränken dürfen. Kommunikative Aspekte zur transparenten Darstellung von Nutzungsrisiken und entsprechenden - gegebenenfalls betreiberseitigen – Lösungen sind hier sehr häufig genannt worden. Auch die Rolle des Staates als Aufklärer über diese Sachverhalte kam zum Tragen, ebenso wie eine Zertifizierung einer relativen Vertrauenswürdigkeit seitens einer unabhängigen Institution. Eine Anmeldung im öffentlichen WLAN mit einem durch den Betreiber gestellten Zertifikat auf dem eigenen Endgerät ist abhängig von der Anbieterreputation zur Etablierung einer verschlüsselten Kommunikation dabei weitläufig akzeptiert.

Die abschließende Frage für die Teilnehmer des World Cafes befasste sich mit einer potenziell gesteigerten Nutzungsrate öffentlicher WLANs bei eventueller Umsetzung der zuvor diskutierten Maßnahmen und Eigenschaften. Hier war das

Feedback überwiegend positiv. Eine Anmerkung bestand darin dass ein Belohnungssystem für die Nutzung eines sichereren Angebots einen zusätzlichen Anreiz darstellen könnte.

Herausforderungen beim KI-Bezug via Web-APIs

Das Angebot von webbasierten APIs, die KI-Algorithmen zugänglich machen, wächst täglich. Aufgrund der zumeist cloudbasierten Bereitstellung dieser Ansätze wird häufig auch von einer Demokratisierung der KI gesprochen, da die technischen Hürden für einen Einsatz von Algorithmen der künstlichen Intelligenz enorm sinken. Entsprechende Angebote finden sich z.B. bei Microsoft im Rahmen der Azure-Plattform oder auch bei der IBM im Rahmen der Bluemix-Plattform. Die Bedenken von Seiten der Anwender, entsprechende Angebote produktiv zum Einsatz zu bringen, sind in Deutschland allerdings enorm. In anderen Regionen wie z.B. im asiatischen oder auch nordamerikanischen Raum steht man dem Einsatz weitaus unkritischer gegenüber. Dementsprechend profitieren innovative Lösungen im Zusammenhang mit fachlichen Anwendungsszenarien, die eher durch den Endanwender bzw. durch potentielle Kunden getrieben werden. Die eher abwartende Haltung in Deutschland impliziert die Gefahr, den Anschluss zu verlieren.

Die folgenden Ausführungen charakterisieren die wesentlichen Eckpunkte der innerhalb des World Cafes durchgeführten Diskussion:

Die Erwartungen der Web-API-Consumer (d.h. Entwickler) sind zum einen eine hohe Security-Grundabsicherung. In diesem Zusammenhang wird typischerweise auf die Authentifizierung und Autorisierung, die netzwerkorientierte Verschlüsselung, das Versionsmanagement sowie ein transparentes Vertragsmanagement Bezug genommen. Zum anderen erwarten die Anwender spezielle Transparenz hinsichtlich des konkret eingesetzten KI-Algorithmus. Die Nachvollziehbarkeit, Verständlichkeit, Genauigkeit und das Vertrauen in die vortrainierten Modelle sind wichtige Anforderungen der Nutzer. Sie können und sollten vom Service Provider adressiert werden. Das Vertrauen in die trainierten Modelle und die Absicherung gegen „böses“ Training sollte von unabhängigen Dritten geprüft und mit Hilfe anerkannter Zertifikate bestätig werden. In diesem Zusammenhang sollten sich auch Standards hinsichtlich des API-Managements bzw. der Spezifikation (Beschreibung) etablieren. Grundsätzlich wurde durch die Teilnehmer festgestellt, dass eine ausschließlich technische Sicht auf die Vertrauenswürdigkeit von Web-APIs nicht ausreicht. Darüber hinaus bedarf es einer Entmystifizierung eingesetzter KI-Algorithmen.

4. Tagungsband und weitere Informationen

Auch für das Jahr 2021 ist die Durchführung eines ESAPI-Workshops vorgesehen. Aktuell gehen wir davon aus, das dieser in Köln (angefragter Gastgeber: Zurich Versicherungsgruppe Deutschland, HS Köln) durchgeführt werden kann. Weiterführende Informationen werden zeitnah unter der folgenden URL im Internet bereitgestellt:

https://blog.hwr-berlin.de/schmietendorf/

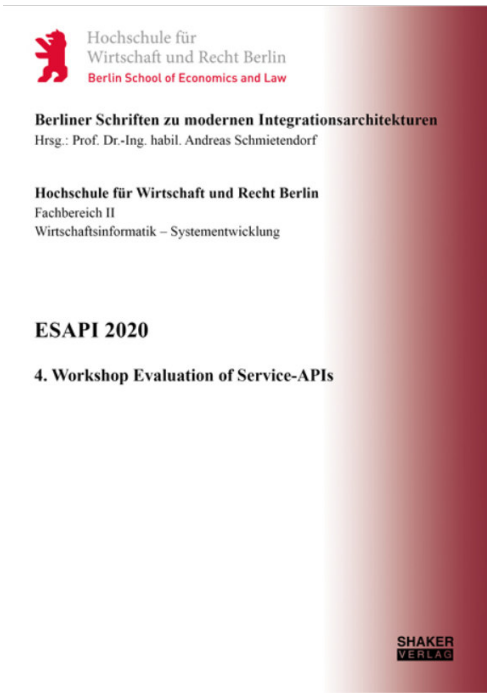

Abbildung 2: Tagungsband zum Workshop ([Schmietendorf/Nadobny 2020])
Quelle: https://www.shaker.de/de/content/catalogue/index.asp?lang=de&ID=8&ISBN=978-3-8440-7515-1

5. Quellenverzeichnis

[Schmietendorf/Nadobny 2020] Schmietendorf, A.; Nadobny, K. (Hrsg.): ESAPI 2020 – 4. Workshop Evaluation of Service-APIs, Berlin – 03. November 2020, 140 Seiten, in Berliner Schriften zu modernen Integrationsarchitekturen, Shaker-Verlag, Düren, November 2020, ISBN 978-3-8440-7515-1

Dank

Unser Dank gilt den Referenten und Teilnehmern, aber auch den Partnern (HWR Berlin, OvG-Universität Magdeburg), Sponsoren (Bayer AG Berlin, Deutsche Bahn AG, Delivery Hero) und Unterstützern im Programmkomitee, die eine solche Veranstaltung ermöglicht haben. Ein herzlicher Dank geht auch an die beteiligten Medienpartner SIGS DATACOM GmbH aus Köln und an den Shaker Verlag GmbH aus Aachen.