FH·W-S
Hochschule
für angewandte Wissenschaften
Würzburg-Schweinfurt

FHWS SCIENCE JOURNAL
2015 (Jahrgang 3), Ausgabe 2

SONDERAUSGABE
INFORMATION SECURITY DAY

Eine Zusammenfassung von fünf der besten Beiträge des Kongresses zum Thema Informationssicherheit am 12. und 13. November 2015 an der Fakultät Informatik der Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt

https://isd.fhws.de

FHWS Science Journal, 2015 (Jahrgang 3), Ausgabe 2
SONDERAUSGABE INFORMATION SECURITY DAY 2015

INHALT

DER HERAUSGEBER DANKT DEN GUTACHTERN DIESER AUSGABE

Prof. Dr. Frank Deinzer	Hochschule Würzburg-Schweinfurt
Prof. Dr. Jana Dittmann	Universität Magdeburg
Prof. Dr. Ralph Ewerth	Leibniz Universität Hannover
Prof. Dr. Herbert Fischer	TH Deggendorf
Dr. Andreas Gabriel	Ethon GmbH
Dr. Dominik Herrmann	Universität Hamburg
Prof. Timo Kob	HiSolutions AG
Herbert Leitold	A-SIT
Prof. Dr Kerstin Lemke-Rust	Hochschule Bonn-Rhein-Sieg
Prof. Dr. Peter Lipp	TU Graz
Dr. Sebastian Pape	Universität Frankfurt
Prof. Dr. Stefanie Rinderle-Ma	Universität Wien
Frank Schlottke	Applied Security GmbH
Klaus Schmitt	innomenta GmbH & Co. KG
Dr. Steffen Wendzel	Fraunhofer-Institut FKIE
Bernhard Witt	it.sec GmbH & Co. KG

In einer Keynote und einem Workshop behandelte Stefan Schumacher vom Magdeburger Institut für Sicherheitsforschung beim Information Security Day 2015 den Themenbereich Social Engineering. Dabei werden (sozial)typische Verhaltensmuster von Menschen ausgenutzt, um sich in den unerlaubten Besitz von Informationen zu bringen. (Foto: FHWS/Oliver Weidel)

VORWORT

Prof. Dr. Kristin Weber

Wie steht es um die Informationssicherheit in Deutschland, der Europäischen Union, bei Unternehmen und nicht zuletzt auch bei Privatpersonen? Seit dem letztem Jahr können sich Studierende der Fakultät Informatik und Wirtschaftsinformatik in den drei Bachelorstudiengängen Informatik, Wirtschaftsinformatik und E-Commerce mit dieser Frage im Rahmen der Vertiefung „Information Security" auseinandersetzen.
Die Studierenden werden in der Vertiefung mit existierenden und potenziellen Bedrohungen der Informationssicherheit konfrontiert und erarbeiten Abwehrmechanismen und Lösungsstrategien. Die neue Vertiefung wurde auf Anhieb von den Studierenden aller drei Studiengänge gut angenommen.

Prof. Dr. Klaus Junker-Schilling

Um die immer wichtiger werdende Thematik einem größerem Publikum nahe zu bringen, entschlossen wir uns, einen Informationssicherheitskongress zu organisieren. Der Information Security Day fand nach knapp einem Jahr Planung, Organisation und Vorbereitung am 12. und 13. November 2015 am Standort der FHWS am Sanderheinrichsleitenweg in Würzburg statt.

Die Veranstaltung bot den knapp 230 Teilnehmerinnen und Teilnehmern eine Mischung aus Keynotes, wissenschaftlichen und Best-Practice-Vorträgen sowie Workshops.
Neben erprobten Lösungsmöglichkeiten aus der Praxis wurden auch neue Ideen sowie theoretisch fundierte Konzepte vorgestellt und diese gemeinsam diskutiert. Damit wurde ein übergreifender Austausch zwischen Wissenschaft und Praxis unter Einbeziehung der über 120 studentischen Teilnehmerinnen und Teilnehmer erreicht.

Für den wissenschaftlichen Track wurden Beiträge über einen Call for Papers eingeworben. Alle eingegangen Beiträge wurden in einem Doppel-Blind-Verfahren durch das Programmkomitee begutachtet. Für die Teilnahme am Programmkomitee konnten wir über 40 renommierte Wissenschaftlicher und Praktiker mit langjähriger Erfahrung gewinnen. Die besten fünf Beiträge wurden am Information Security Day präsentiert und werden nun durch diese Sonderausgabe des FHWS Science Journal einem noch breiteren Publikum vorgestellt.

Prof. Dr. Kristin Weber und Prof. Dr. Klaus Junker-Schilling im Dezember 2015

Sicherheit von Cloud-basierten Plattformen zur Anwendungsintegration: eine Bewertung aktueller Angebote

Dr. Nico Ebert, Prof. Dr. Kristin Weber

Cloud-basierte Plattformen zur Anwendungsintegration versprechen die einfache und kostengünstige Integration zwischen Anwendungen in der Cloud und bestehenden „On-Premise"-Anwendungen. Sie bieten zahlreiche Anwendungsadapter und erlauben den grafischen Entwurf, die Ausführung und die Verwaltung von komplexen Integrationsprozessen in der Cloud. Allerdings sind sie sicherheitskritische Elemente innerhalb der IT-Architektur, da sie Zugriff auf unterschiedliche Anwendungen und Daten des Unternehmens haben können. Daher stellt sich die Frage, inwiefern notwendige Sicherheitsanforderungen durch die Anbieter Cloud-basierter Plattformen erfüllt werden. In diesem Artikel werden sieben ausgewählte Integrationsplattformen detaillierter betrachtet und anhand der Sicherheitsanforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bewertet.

Zusätzliche Schlüsselwörter: Cloud-basierte Integrationsplattform, Integration-Platform-as-a-Service, Sicherheitsanforderungen, Informationssicherheit, Datenschutz

1 EINLEITUNG

Eine Alternative zur direkten Anbindung zwischen Anwendungen und zu Enterprise-Application-Integration-Plattformen (EAI) sind Cloud-basierte Integrationsplattformen. Sie versprechen die Vorteile von Cloud-Lösungen (z. B. geringe Kapitalbindung, hohe Flexibilität, wenig erforderliches Betriebs-Know-how) in Kombination mit dem Nutzen von EAI-Plattformen (z. B. Reduktion der Schnittstellen-Anzahl durch zentralen Hub, standardisierte Anwendungsadapter). Das Schweizer Logistikunternehmen Kardex ist ein Beispiel für die Verwendung einer Cloud-basierten Integrationslösung, um ERP, SaaS und mobile Anwendungen zu integrieren [Boillat und Legner (2014)].

Da die Plattformen auf verschiedene Unternehmensanwendungen in der Cloud („SaaS") und innerhalb des Unternehmens („On-Premise") zugreifen und deren Daten zum Teil in der Cloud verarbeiten, stellen sich insbesondere Fragen nach Informationssicherheit und Datenschutz der Plattformen. Besonders kritisch ist die Anbindung der Bestandssysteme innerhalb

Dr. Nico Ebert
Schuberstrasse 9,
8037 Zürich, Schweiz

Prof. Dr. Kristin Weber
Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt,
Fakultät Informatik und Wirtschaftsinformatik,
Sanderheinrichsleitenweg 20,
97074 Würzburg
http//fiw.fhws.de

der Unternehmensinfrastruktur, weil potentielle Angreifer über die Plattform Zugriff auf diese Systeme erhalten könnten. Gleichzeitig sind die Einfluss- und Kontrollmöglichkeiten für die Nutzer der Plattformen aufgrund des „Plattform als Service" jedoch geringer als bei selbstbetriebenen EAI-Plattformen.

In diesem Artikel werden zunächst die Cloud-basierten Plattformen zur Anwendungsintegration vorgestellt (Kapitel 2). Die „Sicherheitsempfehlungen für Cloud Computing Anbieter" des Bundesamtes für Sicherheit in der Informationstechnik (BSI, Kapitel 3) bilden schließlich die Grundlage für die Bewertung von sieben ausgewählten Plattformen (Kapitel 4).

2 CLOUD-BASIERTE INTEGRATIONSPLATTFORMEN

Cloud-basierte Integrationsplattformen[1] zählen zu den „Platforms as a Service" (PaaS) [Tietz et. al. (2011)] und sind mandantenfähige Systeme, in denen sich verschiedene Kunden eine Systeminstanz teilen. Sie erlauben die Entwicklung, Ausführung und Verwaltung von Integrationsprozessen und die Verbindung von On-Premise- und SaaS-Anwendungen [Pezzini und Lheureux (2011)]. Der funktionale Fokus der Plattformen ist die Integration auf Daten- und Funktionsebene. Die Integration auf Ebene der Geschäftsprozesse z. B. über BPM-Komponenten wird nur selten abgedeckt, die Integration auf Ebene der Benutzeroberflächen ist nicht Bestandteil der Plattformen. Die Funktionsbausteine der Plattformen unterscheiden sich jedoch nicht von denen klassischer EAI-Plattformen [Ring (2000)]:

- Prozessmanagement: Die Prozessmanagement-Funktionalität dient der Ausführung der Transformationsoperatoren.
- Transformation: Verschiedene Operatoren erlauben z. B. die Abbildung zwischen unterschiedlichen Datenschemata und Datenformaten.
- Konnektivität: Vorgefertigte Adapter ermöglichen die Anbindung von Cloud- oder On-Premise-Anwendungen. Die Kopplungsmechanismen erlauben die Verknüpfung der Anwendungen über Dateitransfers, asynchrone Nachrichten und synchrone Dienstaufrufe.
- Administration und Entwicklung: Administrationsfunktionen sind z. B. das Deployment und Monitoring der Integrationsprozesse. Schließlich verfügen alle Plattformen über Entwicklungswerkzeuge, z. B. für die grafische Modellierung von Integrationsprozessen.

Generell können zwei Plattformarchitekturen unterschieden werden. Im ersten Fall erfolgt die Integration zwischen den beteiligten Anwendungen in der Cloud. Daten von lokalen wie SaaS-Anwendungen werden gleichermaßen an die Cloud der Plattform übertragen und dort verarbeitet. In der Cloud werden nur Metadaten gespeichert, das sind insbesondere Prozessmodelle, Datenstrukturen und -abbildungen sowie Konfigurationsdaten für Anwendungsadapter (z. B. Benutzername und Passwort). In diesem Fall liegt die Verantwortung für die Betreuung der Integrationsinfrastruktur vollständig beim Anbieter. Als Alternative zur Verarbeitung der Daten in der Cloud kann die Datenintegration auch lokal erfolgen. Dabei wird in der lokalen Umgebung durch den Nutzer eine spezielle Laufzeitumgebung („Software-Agent") installiert. Die Daten von SaaS und lokalen Anwendungen werden an die lokale Laufzeitumgebung übermittelt und dort verarbeitet. Integrationsdaten werden in der Folge nicht in die Cloud des Plattformanbieters transferiert. Zwischen lokaler Laufzeit und Cloud werden lediglich Metadaten ausgetauscht, die in der Cloud gespeichert werden. Erfolgt die Datenintegration lokal, ist das Unternehmen selbst für die Integrationsinfrastruktur (inkl. Lastverteilung) verantwortlich.

[1] Von [Pezzini und Lheureux (2011)] als „Integration Platform as a Service" (IPaaS) bezeichnet.

Unabhängig vom Architekturtyp erfolgt die Administration (z. B. Benutzerverwaltung oder Monitoring) über eine webbasierte Oberfläche der Integrationsplattform. Der Entwurf der Integrationsprozesse erfolgt – je nach Plattform – ebenfalls über eine Weboberfläche oder über eine lokale Anwendung, die den Upload der Prozesse zur Plattform erlaubt.

3 BEDROHUNGEN UND SICHERHEITSANFORDERUNGEN IM CLOUD-COMPUTING

Cloud-Computing-Systeme sind grundsätzlich komplexe verteilte Systeme, weswegen sie prinzipiell den hierfür geltenden Bedrohungen ausgesetzt sind. Diese sind z. B. Sicherheitslücken im System des Anbieters wie die mangelhafte Benutzerauthentisierung oder die fehlende Überprüfung von Benutzereingaben auf schadhaften Code. Da die Kunden jedoch physische Ressourcen nutzen, auf die sie selbst keinen unmittelbaren Zugriff haben, ergeben sich eine Reihe spezifischer Bedrohungen [Vossen u. a. (2012), S. 175-178]:

- Unüberprüfbare Datenhaltung: Die Datenhaltung liegt in der Hoheit des Anbieters oder dessen Zulieferer und ist in der Regel nicht durch den Kunden überprüfbar (z. B. endgültiges Löschen von Daten).
- Mangelhafte Kontrollmöglichkeiten über Anbieter: Protokolle und Dokumentationen zur Datenverarbeitung befinden sich beim Anbieter, weswegen Kontrollen in der Regel nur eingeschränkt möglich sind.
- Vervielfältigung und Verteilung der Daten: Kunden haben keine Gewissheit, wie Anwendungen bzw. Daten geographisch verteilt sind.
- Nichtverfügbarkeit von Diensten: Cloud-Anbieter nutzen häufig selbst Dienste anderer Cloud-Anbieter. Durch das Ineinandergreifen zahlreicher Dienste bekommt die Stabilität der jeweiligen Schnittstellen eine gesteigerte Bedeutung. Änderungen an einer grundlegenden API eines Anbieters können z. B. dazu führen, dass Dienste eines anderen Anbieters nicht mehr funktionieren. Das Schutzziel der Verfügbarkeit von Diensten und Daten ist bezogen auf den einzelnen Anbieter somit besonders gefährdet[2].
- Gesteigerte Komplexität der IT-Landschaft: Aufgrund der starken Verteilung von Cloud-Diensten sind sie insgesamt komplexer als klassische verteilte Systeme. So sind IT-Infrastruktur und das Betriebspersonal häufig global – auch über unterschiedliche Firmen – verteilt.
- Gegenseitige Beeinflussung der Nutzer: Da sich verschiedene Nutzer eine Plattform teilen, ist die gegenseitige Beeinflussung nicht ausgeschlossen (z. B. Zugriff eines Nutzers auf Daten eines anderen Nutzers).

Zur Gewährleistung der Informationssicherheit ist eine Reihe von technischen und organisatorischen Sicherheitsmaßnahmen erforderlich. Informationen bzw. Daten sind zu schützende Güter für die insbesondere die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität (d. h. Vollständigkeit und Unversehrtheit) gelten [Federrath und Pfitzmann (2000)]. Die technischen Sicherheitsmaßnahmen betreffen sowohl die Infrastruktur (Netzwerk, Hosts, Anwendungen) als auch die Daten. Dazu zählen z. B. Verschlüsselungsmechanismen für die Übertragung von Daten und Autorisierungsverfahren für Benutzer. Komplementär dazu sind organisatorische Maßnahmen wie Mitarbeiterschulungen oder die Schlüsselverwaltung [Vossen u. a. (2012), S. 180 ff.].

Verarbeiten die Cloud-Computing-Systeme personenbezogene Daten, wie es etwa bei CRM-Systemen in der Regel der Fall ist, müssen zudem die Regelungen zum Datenschutz be-

[2] Unter Umständen kann die Verfügbarkeit jedoch durch die Verteilung auf mehrere Anbieter oder die Spezialisierung der Infrastruktur-Zulieferer auch steigen.

achtet werden. Die datenschutzrechtlichen Anforderungen sind in Deutschland insbesondere durch das Bundesdatenschutzgesetz (BDSG) geregelt. Werden von einem Unternehmen die Daten von Personen, die unter das BDSG fallen, durch einen Dritten verarbeitet, muss der Betroffene dazu im Vorfeld auf freiwilliger Basis einwilligen und der Dritte muss seinerseits das BDSG beachten (§ 4c Abs. 1 BDSG). Findet die Datenverarbeitung jedoch im Rahmen einer Auftragsdatenverarbeitung im Geltungsbereich des BDSG bzw. der EG-Datenschutzrichtlinie statt, ist keine Einwilligung der Betroffenen erforderlich, da Auftraggeber und Auftragnehmer als eine rechtliche Einheit betrachtet werden [Gola und Schomerus (2015), S. 299]. Cloud-Computing wird als Auftragsdatenverarbeitung eingestuft [Gola und Schomerus (2015)].

Die Auftragsdatenverarbeitung setzt allerdings voraus, dass die Daten innerhalb der EU oder in Ländern verarbeitet werden, deren Datenschutzniveau von der EU-Kommission als angemessen betrachtet wird (z. B. in der Schweiz). Mit den USA als Drittstaat wurde von der EU ursprünglich das „Safe-Harbor"-Abkommen beschlossen, mit dem sich Anbieter gegenüber dem Handelsministerium zur Einhaltung von „vergleichbaren" Datenschutzprinzipien wie in der EU verpflichten können. Dieses Abkommen wurde jedoch vom Europäischen Gerichtshof als ungültig erklärt [EuGH (2015)]. Als Alternative zu „Safe-Harbor" können die US-amerikanischen Unternehmen in der Theorie jedoch „Standardvertragsklauseln" der EU zustimmen [vgl. EU Kommission (2015)], wie dies z. B. der CRM-Anbieter Salesforce.com unmittelbar nach dem EuGH-Urteil tat. Aus den datenschutzrechtlichen Anforderungen ergeben sich eine Reihe von Maßnahmen für die Anbieter, etwa die Bestellung eines Datenschutzbeauftragten oder die Kontrolle des Zugriffs auf die personenbezogenen Daten (§ 9 BDSG, § 4f Abs. 1 Satz 1 BDSG).

Die Anforderungen an Informationssicherheit und Datenschutz im Cloud-Computing wurden von unterschiedlichen Organisationen in Form von Empfehlungen und Standards zusammengefasst. Die internationale „Cloud Security Alliance", in der einige Kundenorganisationen, Anbieter und Universitäten organisiert sind, bietet mit der „Cloud Controls Matrix" einen Überblick über verschiedene Empfehlungen und Standards [CSA (2014)]. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt in seinem Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter" [BSI (2012)] Vorschläge betreffend Informationssicherheit und Datenschutz. Die verschiedenen Anforderungsbereiche sowie ausgewählte Beispielanforderungen für Public-Cloud-Anbieter zeigt Tab. 1. Unterschieden wird zwischen den Anforderungskategorien Basis (B), hohe Vertraulichkeit für Daten mit hohem Schutzbedarf für Vertraulichkeit (C+) und hohe Verfügbarkeit (A+) für Dienstleistungen mit hohem Verfügbarkeitsbedarf. Das Schutzziel Integrität wird nicht durch die BSI-Anforderungen abgedeckt.

[3] Daneben wird der Datenschutz für nicht-öffentliche Stellen auch durch das Telemedien- und das Telekommunikationsgesetz geregelt.

ANFORDERUNGSBEREICH	BEISPIELANFORDERUNG (B = Basis, C+ = hohe Vertraulichkeit, A+ = hohe Verfügbarkeit)
Sicherheitsmanagement beim Anbieter	(B) Implementation eines anerkannten Informationssicherheits-Managementsystems (z. B. ISO 27001)
Sicherheitsarchitektur Rechenzentrums-Sicherheit	(B) Überwachung des Zutritts: Zutrittskontrollsystem, Videoüberwachungssysteme, Bewegungssensoren, Sicherheitspersonal, Alarmsysteme, etc.
Serversicherheit	(C+, A+) Einsatz zertifizierter Hypervisoren (Common Criteria mindestens EAL 4)
Netzsicherheit	(B) Verschlüsselte Kommunikation zwischen Cloud Computing-Anbieter und -Nutzer (z. B. TLS/SSL)
Anwendungs- und Plattformsicherheit	(B) Sichere Isolierung der Anwendungen (PaaS)
Datensicherheit	(B) Regelmäßige Datensicherungen, deren Rahmenbedingungen (z. B. Umfang, Speicherintervalle) nachvollziehbar sind
Schlüsselmanagement	(B) Best-Practices der Schlüsselverwaltung umsetzen
ID- und Rechtemanagement	(C+) Starke Authentisierung (z. B. Zwei-Faktor-Authentisierung) für Cloud-Kunden
Kontrollmöglichkeiten für Nutzer	(B) Kunden müssen die Möglichkeit haben, messbare Größen, wie im SLA vereinbart, zu überwachen
Monitoring und Security Incident Management	(B) 24/7 umfassende Überwachung der Cloud-Dienste sowie zeitnahe Reaktion bei Angriffen bzw. Vorfällen
Notfallmanagement	(B) Der Anbieter muss ein Notfallmanagement betreiben
Portabilität und Interoperabilität	(B) Exit-Vereinbarung mit zugesicherten Formaten unter Beibehalten aller logischen Relationen und ggf. Offenlegung der damit verbundenen Kosten (SaaS)
Sicherheitsprüfung und -nachweis	(C+, A+) Regelmäßige und unabhängige Sicherheitsrevisionen
Personalanforderungen	(B) Sensibilisierung der Mitarbeiter des Cloud Service Anbieters für Informationssicherheit und Datenschutz
Vertragsgestaltung Transparenz	(B) Offenlegung der Subunternehmer des Anbieters
Service Level Agreements	(B) Definierte Sicherheitsleistungen durch Security-SLA oder im SLA deutlich hervorgehoben
Datenschutz/Compliance	(B) Gewährleistung des Datenschutzes nach dt. Recht (B) Für den Cloud-Nutzer relevante gesetzliche Bestimmungen müssen durch den Anbieter eingehalten werden

Tab. 1: Anforderungsbereiche für Public-Cloud-Anbieter gemäß den Sicherheitsempfehlungen des BSI (Auszug aus [BSI (2012), S. 22 ff.])

Abgeleitet von den genannten Bedrohungen können die im vorherigen Abschnitt genannten Anforderungen des BSI präzisiert werden:

- Sicherheitsarchitektur insb. Netzsicherheit: Für die Integration von On-Premise-Anwendungen sind Maßnahmen zu treffen, die den Schutz der gesamten IT-Landschaft gewährleisten. Denkbar sind z. B. die verschlüsselte Kommunikation zwischen Plattform und On-Premise-Anwendungen sowie Proxy-Dienste und dedizierte Sicherheitszonen als Zwischenschicht zwischen On-Premise-IT und Plattform [BSI (2012), S. 32 f.].
- Sicherheitsarchitektur insb. Schlüsselmanagement: Kritische Daten müssen verschlüsselt werden. Hervorzuheben sind Passwörter, die in den Anwendungsadaptern hinterlegt sind, um auf die Anwendungsschnittstellen zuzugreifen. Ein Schlüsselmanagement muss sicherstellen, dass die verwendeten Schlüssel vertraulich, integer und authentisch erzeugt, gespeichert, ausgetauscht, genutzt und vernichtet werden [BSI (2012), S. 39 ff.].
- ID- und Rechtemanagement: Für die Mitarbeiter des Plattform-Anbieters aber auch für die Nutzer der Plattform auf Kundenseite (z. B. Entwickler, IT-Architekten) muss eine starke Authentisierung (z. B. Zwei-Faktor-Authentisierung) genutzt werden. Zudem muss ein rollenbasiertes Rechtemanagement-System den Zugriff auf Integrations- und Metadaten auf Anbieter- und Nutzerseite regeln und protokollieren [BSI (2012), S. 43 ff.].

4 BEWERTUNG CLOUD-BASIERTER INTEGRATIONSPLATTFORMEN

4.1 Vorgehen

Zur Bewertung ausgewählter Cloud-basierter Plattformen wurden die Kriterien des BSI genutzt, weil angenommen wird, dass diese in Deutschland häufig Anwendung finden. Allerdings wurden sie um das Kriterium der Integrität erweitert. Eine Internetsuche mit Google nach „Integration Platform as a Service", „IPaaS", „Integration Platform" und „Cloud Integration" ergab 23 Plattformen, welche die in Kapitel 2 erwähnten Funktionalitäten aufwiesen. Hiervon wurden Dell Boomi Atomsphere, IBM Cast Iron Live, Informatica Cloud, Jitterbit, MuleSoft Cloudhub, SAP HCI und Snaplogic ausgewählt, denen das Marktforschungsunternehmen Gartner [Pezzini u. a. (2015)] im „magischen Quadranten" eine subjektiv besondere „Vollständigkeit der Vision" (u. a. Marktverständnis, Geschäftsmodell, Innovation) und „Fähigkeit zur Umsetzung" (u. a. Produktqualität, Kundensupport) zugewiesen haben. Die „magischen Quadranten" der Firma Gartner werden von Unternehmen in der Praxis häufig zur Auswahl von Software herangezogen. Daher kann davon ausgegangen werden, dass die gut im Quadranten positionierten Plattformen häufig in die Auswahl eingeschlossen werden. Nachfolgend wurden Testversionen[4], Produktbeschreibungen, Dokumentationen und Videos ausgewertet. Interviews mit den Herstellern wären im Rahmen der weiteren Forschung wünschenswert (z. B. zu internen Prozessen der Anbieter).

4.2 Sicherheitsmanagement beim Anbieter

Die betrachteten Anbieter verfügen über unterschiedliche Systeme zum Management der Informationssicherheit. Verbreitet ist die ISO 27001 [ISO (2013)] ebenso wie die „Service Organisation Controls 2" (SOC 2). Bei SOC 2 handelt es sich um einen amerikanischen Standard aus der Wirtschaftsprüfung, der auch Anforderungen an die Informationssicherheit umfasst [AICPA (2014)]. Allerdings ist aufgrund der unzureichenden Angaben der Anbieter unklar, was der Geltungsbereich dieser Zertifikate ist (z. B. nur Rechenzentrum) und ob das Sicherheitsmanagement alle Mitarbeiter und Systeme des Anbieters umfasst. Einige Anbieter halten sich zudem an branchenspezifische Standards zur Verarbeitung von Krankenversicherten-

[4] Die Testversion war bei IBM Cast Iron Live nicht verfügbar.

und Patientendaten wie den „Health Insurance Portability and Accountability Act“ (HIPAA), den „Health Level Seven International Standard“ (HL7) oder den „Health Information Trust Alliance Standard“ (HiTrust) sowie zur Verarbeitung von Kreditkartendaten den „Payment Card Industry Data Security Standard“ (PCI DSS). Zwar verweisen einige Hersteller (z. B. Dell) ebenfalls auf Zertifizierungen (z. B. ISO 27001), allerdings gelten diese zum Teil nur für die Cloud-basierte IT-Infrastruktur (z. B. Amazon). Die Zertifikate sagen nichts über die Sicherheitsstandards für die Entwicklung und den Anwendungsbetrieb der Integrationsplattform aus, die sich auf der IT-Infrastruktur befindet.

4.3 Sicherheitsarchitektur

4.3.1 Rechenzentrums-Sicherheit, Serversicherheit und Netzsicherheit

Mit Ausnahme von IBM und SAP nutzen die Anbieter Cloud-basierte IT-Infrastrukturen von Amazon oder Rackspace. Sämtliche Infrastrukturen verfügen über ein Sicherheitsmanagement basierend auf ISO 27001. Der Zugriff auf die Weboberfläche der Plattform (z. B. zur Administration) erfolgt bei allen Anbietern über eine verschlüsselte HTTPS/TLS-Verbindung. Alle Anbieter mit Ausnahme von Informatica ermöglichen die Ausführung der Integrationsprozesse in der Cloud. Der Zugriff auf lokale Anwendungen beschränkt sich in der Regel auf eine „demilitarisierte Zone“ (vgl. z. B. [Dell (2015)]) oder eine „Virtual Private Cloud“ (vgl. z. B. [MuleSoft (2015)]). Die Datenübertragung zwischen lokaler Umgebung und Integrationsplattform erfolgt im ersten Fall über eine gesicherte HTTPS- oder SFTP-Verbindung und im zweiten Fall über einen IPsec oder TLS gesicherten VPN-Tunnel.

Dell, IBM, Informatica, Jitterbit und Snaplogic unterstützen die lokale Ausführung der Integrationsprozesse. In diesem Fall verschlüsselt die lokale Laufzeitumgebung die Datenübertragung zur Cloud-Plattform (z. B. TLS 1.0 und TLS 1.2, vgl. z. B. [Dell (2015)]). Der lokale Laufzeit-Agent und die Plattform tauschen lediglich Status- und Metadaten aus. Die Anwendungsadapter der Plattformen unterstützen vielfältige Sicherheitsstandards zur Kommunikation mit den integrierten Anwendungen (z. B. WS-Security, OAuth2). SAP HCI erlaubt zudem die Verschlüsselung auf Nachrichtenebene via PKCS#7 sowie die Verschlüsselung von Dateitransfers via SFTP und PGP.

4.3.2 Anwendungs- und Plattformsicherheit

Die Plattformen sind durchgängig mandantenfähig, allerdings machen die Anbieter fast keine Angaben dazu, wie Mandanten voneinander isoliert werden. Lediglich SAP verweist auf separate Datenschemata [SAP (2013), S. 11 ff.]. Dell und Jitterbit weisen zusätzlich darauf hin, dass bei der Entwicklung die OWASP-Top10-Risiken von Webanwendungen berücksichtigt werden[5] [OWASP (2013)]. Mit Ausnahme von MuleSoft und SAP bieten die Anbieter lokale Laufzeitumgebungen für die Integration von On-Premise-Systemen. Diese haben den Vorteil, dass Integrationsdaten nicht mit der Cloud des Plattformanbieters ausgetauscht werden, sondern lediglich zwischen On-Premise- und SaaS-Anwendungen. Die Plattform in der Cloud tauscht mit der lokalen Umgebung lediglich Metadaten über eine HTTPS-Verbindung aus.

[5] Dazu zählen z. B. das „Cross-Site-Scripting“ oder die „Code-Injection“.

Tab. 2: Bewertung ausgewählter Cloud-basierter Integrationsplattformen anhand der BSI-Anforderungsbereiche (Quelle: Eigene Darstellung)

Kriterium	Dell Boomi Atomsphere	IBM Cast Iron Live	Informatica Cloud	Jitterbit	MuleSoft Cloudhub	SAP HCI	Snaplogic
4.2 Sicherheitsmanagement beim Anbieter	k. A.	ISO 27001 (unklar, ob nur RZ)	ISO 27001, PCI DSS	HIPAA/HL7	SOC 2, PCI, HiTrust	ISO 27001:2013, Cobit, SOC 2, PCI, ISF	SOC 2
4.3 Sicherheitsarchitektur							
a. RZ-/Server-/Netzsicherheit	ISO 27001:2005, SCO 1 (Rackspace), 128-Bit-SSL für Weboberfläche/ On-Premise-Anbindung, Adapter mit versch. Standards (z. B. WS-Security)	ISO 27001 (eigene RZ), SSL für Weboberfläche/ Agenten, Adapter mit versch. Standards (WS-Security)	ISO 27001/2 (Amazon), 128-Bit-SSL für Weboberfläche/On-Premise-Anbindung, Adapter mit versch. Standards (z. B. WS-Security)	ISO 27001/2 (Amazon AWS), SSL für Weboberfläche/Agenten, Adapter mit versch. Standards (WS-Security)“	ISO 27001/2 (Amazon), 128-Bit-SSL für Weboberfläche, VPC für On-Premise-Anbindung, Adapter mit versch. Standards (z. B. OAuth2)	eigene Infrastruktur, D/ USA, ISO 27001, SSL für Weboberfläche/für Agents, Adapter mit versch. Standards z. B. PKCS#7), PGP für On-Premise	ISO 27001/2 (Amazon AWS), SSL für Weboberfläche/Agenten, Adapter mit versch. Standards (z. B. OAuth2)“
b. Anwendungs- u. Plattformsicherheit	mandantenfähig, OWASP, lokale Laufzeit vorhanden	mandentenfähig, lokale Laufzeit vorhanden	mandentenfähig, lokale Laufzeit vorhanden	mandentenfähig, OWASP, lokale Laufzeit vorhanden	mandentenfähig, lokale Laufzeit nur via separaten MuleESB	mandentenfähig, gem HANA-Plattform (z. B. Tenant-Isolierung)	Mandentenfähig, lokale Laufzeit vorhanden
c. Datensicherheit	k. A. zur Datensicherung/-löschung von Metadaten	k. A. zur Datensicherung/-löschung von Metadaten	k. A. zur Datensicherung/-löschung von Metadaten	k. A. zur Datensicherung/-löschung von Metadaten	k. A. zur Datensicherung von Metadaten, Message Queues können ebenfalls gespeichert werden	k. A. zur Datensicherung/-löschung von Metadaten	k. A. zur Datensicherung/-löschung von Metadaten
d. Schlüsselmanagement	Verschlüsselung von Passwörtern, Schlüsselmanagement	k. A.	k. A.	Verschlüsselung von API-Passwörtern, k. A. zum Schlüsselmanagement	Verschlüssung von Passwörtern, k. A. zum Schlüsselmanagement	Schlüsselmanagement	Verschlüsselung von API-Passwörtern, Schlüsselmanagement
4.4 ID- u. Rechtemanagement	einfache Authent., rollenbas. Rechtemanagement	einfache Authent./LDAP, rollenbas. Rechtemanagement	einfache Authent., rollenbas. Rechtemanagement	einfache Authent., rollenbas. Rechtemanagement	einfache Authent./ externes ID-Mgmt (Oauth), rollenbas. Rechtemanagement	einfache Authent./Single Sign-On via Kerberos möglich, Policies, rollenbas. Rechtemanagement	einfache Authent, Single Sign-On via SAML-2/ LDAP möglich, rollenbas. Rechtemanagement
4.5 Kontrollmöglichkeiten für Nutzer	trust.boomi.com (rudimentär)	k. A.	trust.informaticacloud.com (rudimentär)	trust.jitterbit.com (rudimentär)	trust.mulesoft.com (rudimentär)	gem. HANA-Plattform	elastic.snaplogic.com/sl/dashboard.html
4.6 Monitoring u. Security Incident Management	24/7 Monitoring/Incident-Mgmt, Logging	24/7 Monitoring/Incident-Mgmt, Logging	24/7 Monitoring/Incident-Mgmt, Logging	24/7 Monitoring/Incident-Mgmt, Logging	24/7 Monitoring/Incident-Mgmt, Logging	24/7 Monitoring/Incident-Mgmt, Logging	24/7 Monitoring/Incident-Mgmt, Logging
4.7 Notfallmanagement	k. A.	k. A.	k. A.	k. A.	k. A.	ISO 22301 (RZ)	k. A.
4.8 Portabilität u. Interoperabilität	rudimentärer Export von Mappings, Plattform API	im-/Export via CastIron Live Studio	Im-/Export via Power Center, Plattform API	Im-/Export via Jitterbit Studio	Im-/Export via Anypoint Studio, Plattform API	Im-/Export via Integration Designer u. Data Services	Im-/Export von Projekten, Platform API
4.9 Sicherheitsprüfung u. -nachweis	siehe 4.5	k. A.	siehe 4.5	siehe 4.5	siehe 4.5	gem. HANA-Plattform	siehe 4.5
4.10 Personalanforderungen	k. A.	k. A.	k. A.	definiert	k. A.	gem. HANA-Plattform	k. A.
4.11 Vertragsgestaltung							
a. Transparenz	rudimentär	rudimentär	rudimentär	umfassende Information	rudimentär	gem. HANA-Plattform	rudimentär
b. Service Level Agreements	k. A.	k. A.	k. A.	k. A.	k. A.	gem. HANA-Plattform	k. A.
4.12 Datenschutz u. Compliance	Sitz USA, Verarbeitung USA	Stammsitz USA, Verarbeitung in den USA /EU	Sitz USA, Verarbeitung USA /EU, SOC 1	Stammsitz USA, Verarbeitung in den USA /EU	Sitz USA, Verarbeitung USA /EU, SOC 1	Sitz EU, Verarbeitung USA/EU, 95/46/EG, SOC 1/3, ISO 9001	Verarbeitung in den USA (kein Safe-Harbor) oder EU
4.13 Integrität	keine zusätzl. Angaben	keine zusätzl. Angaben	keine zusätzl. Angaben	keine zusätzl. Angaben	keine zusätzl. Angaben	keine zusätzl. Angaben	keine zusätzl. Angaben

4.3.3 Datensicherheit

Die Plattformen verarbeiten zwar Integrationsdaten, speichern aber nur Metadaten. Detaillierte Angaben dazu, welchen Metadaten gespeichert werden, machen die Anbieter nicht. MuleSoft Cloudhub bietet optional Warteschlangen für Nachrichten an, die Integrationsdaten speichern. Detaillierte Angaben dazu, wie und wann die Daten gesichert werden, machen die Anbieter nicht. Bei der Nutzung der Infrastrukturen renommierter Anbieter wie Rackspace oder Amazon werden die Daten redundant gespeichert [Amazon (2014); Rackspace (2015)].

4.3.4 Schlüsselmanagement

Einzig SAP HCI erlaubt die Verschlüsselung der Daten auf der Plattform. Bei den anderen Anbietern beschränkt sich die Verschlüsselung auf die Anwendungspasswörter[6] (MuleSoft erlaubt zusätzlich die Verschlüsselung von Warteschlagen). Dell Boomi, SAP HCI und Snaplogic verwenden hierzu ein Public-Private-Key-Verfahren. Bei Dell Boomi wird bei der Erstellung eines Benutzerkontos ein Schlüsselpaar erzeugt und Anwendungspasswörter werden mit dem öffentlichen Schlüssel verschlüsselt. Allerdings wird das Schlüsselpaar einseitig beim Anbieter gespeichert, weswegen das Vorgehen letztlich nutzlos ist. Zur Laufzeit werden die Passwörter dann mit dem privaten Schlüssel entschlüsselt. IBM Cast Iron Live, Informatica Cloud, Jitterbit und Cloudhub machen keine Angaben dazu, wie Schlüssel verwaltet werden. Alle Anbieter machen keine Angaben zur Stärke der Verschlüsselung (z. B. RSA 2048 Bit).

4.4 ID- und Rechtemanagement

Alle Anbieter unterstützen standardmäßig nur die einfache Authentisierung mit Benutzername und Passwort. Eine Zwei-Faktor-Authentisierung wird von keinem Dienst angeboten. Allerdings unterstützen einige Anbieter z. B. die Authentisierung via Kerberos (SAP) oder die Einbindung eines externen Cloud-Dienstes zum ID-Management (z. B. OAuth-Protokoll via PingIdentity-Dienst). Alle Plattformen bieten ein rollenbasiertes Rechtemanagement, das z. B. regelt, welche Benutzer auf welche Integrationsprozesse zugreifen dürfen.

4.5 Kontrollmöglichkeiten für Nutzer

Die Anbieter machen keine Angaben dazu, welche Kontrollmöglichkeiten die Nutzer hinsichtlich des administrativen Zugriffs durch den Anbieter haben. Die Plattformen bieten rudimentäre Informationen zu Service-Parametern wie Verfügbarkeit (Ampelsysteme), Wartungsfenstern und Sicherheitsaktualisierungen an. Hierzu werden den Benutzern Statuswebsites bereitgestellt (z. B. trust.jitterbit.com). Die Parameter beziehen sich nur auf die Plattformen selbst, nicht jedoch auf die Internet-Verbindung zwischen Anbieter und Benutzer. Letztere ist nicht Gegenstand der Service-Level-Agreements der Anbieter und muss separat mit dem Internet-Service-Provider vereinbart werden.

4.6 Monitoring und Security-Incident-Management

Rund um die Uhr überwachen alle Anbieter die jeweilige Plattform und reagieren auf sicherheitskritische Vorfälle. Ebenfalls werden Anmeldungen und Änderungen von Benutzern und Administrationen protokolliert.

4.7 Notfallmanagement

Mit Ausnahme von SAP HCI, das über ein Notfallmanagement nach ISO 22301 verfügt, machen die Anbieter dazu keine Angaben.

[6] Informatica macht hierzu keine Angaben.

4.8 Portabilität und Interoperabilität

Die Plattformen nutzen häufig keine Webanwendungen sondern normale Windows/ Linux-Anwendungen (z. B. auf Basis von Eclipse) für den Entwurf der Integrationsprozesse. Diese können lokal gespeichert werden, befinden sich allerdings in proprietären Formaten. Bei Dell Boomi Atmosphere erfolgt auch der Entwurf im Web und ein Export der Integrationsprozesse aus der Plattform ist nicht möglich. Die einzige Ausnahme sind Datenabbildungen, die als einfache Excel-Dateien exportiert werden können. Einige Plattformen (z. B. Informatica Cloud, MuleSoft Cloudhub) bieten eine Plattform-API mit der alternativ zur Weboberfläche auf die Plattform zugegriffen werden kann.

4.9 Sicherheitsprüfung und -nachweis

Die Anbieter informieren Cloud-Nutzer in der Regel mittels der Statuswebsites (vgl. Kontrollmöglichkeiten für Nutzer) über sicherheitsrelevante Vorfälle und Penetrationstests.

4.10 Personalanforderungen

Lediglich Jitterbit macht Angaben zu Personalanforderungen [Jitterbit (2014)]. Allerdings umfassen auch die von manchen Anbietern umgesetzten Sicherheitsstandards bereits Sicherheitsanforderungen an das Personal (vgl. z. B. [ISO (2013)], Control A.7.2.2).

4.11 Vertragsgestaltung

4.11.1 Transparenz

Mit Ausnahme von Jitterbit und SAP HCI weisen die Anbieter nicht unmittelbar darauf hin, wo die Daten des Nutzers verarbeitet werden. Allerdings ergab die detailliertere Betrachtung, dass der Kunde zwischen verschiedenen Deployment-Lokationen für die Integrationsumgebung (Ausnahme: Dell Boomi) wählen kann (inkl. EU-Cloud). Ob dort oder an einem anderen Standort dann ebenfalls die Metadaten des Nutzers gespeichert werden, ist unklar. Subunternehmer werden nur rudimentär offengelegt (z. B. Amazon Web Services bei Jitterbit). Eingeschränkt informieren die Anbieter darüber, welche Informationen verarbeitet bzw. gespeichert werden.

4.11.2. Service-Level-Agreements (SLA)

Die Anbieter machen generell nur grundlegende Angaben zu SLA-Parametern („Boomi's goal is to achieve 99.99% Service Availability") und keine spezifischen sicherheitsrelevanten Angaben innerhalb der Service-Level-Agreements. Auch die Angaben zu Subunternehmern und deren Sicherheitsmaßnahmen sind rudimentär und beschränken sich meist nur auf deren Zertifizierungen („Amazon Web Services ist ISO 27001 zertifiziert").

4.12 Datenschutz und Compliance

Zum Zeitpunkt der Erstellung dieses Artikels ist unklar, wie die Anbieter mit Sitz in den USA auf die Außerkraftsetzung der „Safe-Harbor"-Liste reagieren. Drei US-Hersteller (Jitterbit, MuleSoft und Snaplogic) sind aber auch nicht auf der Liste aufgeführt, was aus europäischer Sicht kritisch einzustufen ist. Im Fall der Datenverarbeitung in der EU haben sich die Unternehmen an die EU-Datenschutzrichtlinie 95/46/EG zu halten (z. B. SAP weist auf deren Einhaltung explizit hin). Allerdings stellt sich auch hier die Frage, inwiefern US-Unternehmen Daten auf ihren EU-Servern an US-Behörden weitergeben. Von den betrachteten Unternehmen ist einzig SAP der Anbieter mit Stammsitz in der europäischen Jurisdiktion.

4.13 Integrität

Keiner der Anbieter macht hierzu weitergehende Angaben als die vorgenannten.

FAZIT

Die detaillierte Betrachtung der sieben ausgewählten Plattformen in Hinblick auf die Sicherheitsanforderungen des BSI ergab grundsätzlich, dass die öffentlich verfügbaren Informationen zu Informationssicherheit und Datenschutz der Anbieter unzureichend sind. Zwar werden technische Funktionalitäten im Detail beschrieben, Informationen zur Umsetzung der betrachteten Sicherheitsanforderungen sind insgesamt aber unvollständig. Folglich muss der Kunde einzeln im Dialog mit den Anbietern klären, inwiefern und wie Sicherheitsanforderungen erfüllt oder nicht erfüllt werden.

Aus unserer Betrachtung wurde z. B. nicht eindeutig ersichtlich, was der organisatorische und geographische Geltungsbereich der aufgeführten Zertifizierungen zum Sicherheitsmanagement-System überhaupt ist. Welche Daten effektiv beim Hersteller gespeichert werden und ob diese überhaupt verschlüsselt werden, geht ebenso aus den öffentlichen Angaben der Hersteller nicht hervor. Die meisten Anbieter verschlüsseln die kritischen Anwendungspasswörter der Anwendungsschnittstellen, machen aber keine Angaben zum Verfahren. Im Falle von Dell Boomi wird jedoch auf ein Publiy-Key-Konzept zur Verschlüsselung der Passwörter verwiesen, welches gänzlich unwirksam ist. Keiner der betrachten Anbieter nutzt beim Zugriff auf die Weboberfläche der Plattform eine starke Authentisierung (z. B. Zwei-Faktor-Authentisierung), wie diese beim E-Banking üblich ist. Welche Kontrollmöglichkeiten der Nutzer über die Prozesse des Anbieters hat, ist gleichsam intransparent und die über die Status-Websites bereitgestellten Informationen sind rudimentär.

Für den Fall, dass personenbezogene Daten verarbeitet werden sollen, ist zum jetzigen Zeitpunkt eindeutig von der Speicherung in der Cloud US-amerikanischer Anbieter abzuraten, weil unklar ist, welches Datenschutzniveau nach der Aussetzung der „Safe-Harbor"-Liste gewährleistet wird. Werden Dienste eines US-amerikanischen Anbieters genutzt, sollten die Daten allenfalls in einer lokalen Integrationsumgebung beim Kunden verarbeitet werden und es sollte überprüft werden, dass lediglich Metadaten in die Cloud übertragen werden. Als Alternative können die Dienste europäischer Unternehmen wie das dargestellte SAP HCI oder Elastic.io genutzt werden.

REFERENZEN

AICPA (2014): Service Organization Controls (SOC), http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/serviceorganization'smanagement.aspx, zuletzt aufgerufen am 23. Juli 2015.

Amazon (2014): Amazon S3 – Produktdetails, https://aws.amazon.com/de/s3/faqs, zuletzt aufgerufen am 23. Juli 2015.

Boillat, T. und Legner, C. (2014): Why Do Companies Migrate Towards Cloud Enterprise Systems? A Post-Implementation Perspective, in: IEEE 16th Conference on Business Informatics, 1, 2014, S. 102-109. doi: 10.1109/CBI.2014.46.

BSI (2012): Bundesamt für Sicherheit in der Informationstechnik, Eckpunktepapier, Sicherheitsempfehlungen für Cloud Computing Anbieter, Bonn, 2012.

CSA (2014): Cloud Controls Matrix, https://cloudsecurityalliance.org/research/ccm/#_downloads, zuletzt aufgerufen am 21. Juli 2015.

Dell (2015): Data Communication Security, http://help.boomi.com/atomsphere/GUID-A5BD775D-E710-44D7-9322-98D3F3532DBC.html, zuletzt aufgerufen am 23. Juli 2015.

EU Kommission (2015): Model Contracts for the transfer of personal data to third countries, http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm, zuletzt aufgerufen am 7. Oktober 2015.

EuGH (2015): PRESSEMITTEILUNG Nr. 117/15, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117de.pdf, zuletzt aufgerufen am 7. Oktober 2015.

Federrath, H. und Pfitzmann, A. (2000): Gliederung und Systematisierung von Schutzzielen in IT-Systemen, in: Datenschutz und Datensicherheit DuD, 24(12), 2000, S. 704-710.

Gola, P. und Schomerus, R. (2015): BDSG: Bundesdatenschutzgesetz – Kommentar, München, 2015.

ISO (2013): ISO/IEC 27001 – Information security management, International Organization for Standardization, 2013.

Jitterbit (2014): Jitterbit Harmony Security & Architecture Whitepaper, http://www.jitterbit.com/Files/Product/HarmonySecurityWhitepaper.pdf, zuletzt aufgerufen am 23. Juli 2015.

MuleSoft (2015): Virtual Private Network, https://developer.mulesoft.com/docs/display/current/Virtual+Private+Cloud, zuletzt aufgerufen am 23. Juli 2015.

OWASP (2013): OWASP Top 10 – 2013, https://www.owasp.org/images/4/42/OWASP_Top_10_2013_DE_Version_1_0.pdf, zuletzt aufgerufen am 23. Juli 2015.

Pezzini, M. und Lheureux, B. J. (2011): Integration platform as a service: moving integration to the cloud, in: Gartner, 2011, S. 1-9.

Pezzini, M., Natis, Y. V., Malinverno, P., et al (2015): Magic Quadrant for Enterprise Integration Platform as a Service, in: Gartner, 2015, S. 1-35.

Rackspace (2015): Cloud Block Storage: FAQs, http://www.rackspace.com/knowledge_center/product-faq/cloud-block-storage, zuletzt aufgerufen am 10. Oktober 2015.

Ring, K. (2000): EAI: Making the right Connections, in: Ovum Reports 1–9, Boston, 2000.

SAP (2013): SAP HANA Cloud Integration, https://help.sap.com/cloudintegration/SAP_HCI_Overview.pdf, zuletzt aufgerufen am 23. Juli 2015.

Tietz, V., Blichmann, G. und Hübsch, G. (2011): Cloud-Entwicklungsmethoden, in: Informatik-Spektrum, 34, 2011, S. 345-354. doi: 10.1007/s00287-011-0531-1

Vossen, G., Haselmann, T. und Hoeren, T. (2012): Cloud-Computing für Unternehmen: Technische, wirtschaftliche, rechtliche und organisatorische Aspekte, Heidelberg, 2012.

Fallstudie: Architekturgestützter Entwicklungsansatz für IT-Compliance-Management in Regierungsbehörden – Anforderungen, Lösungsansätze, Forschungsbedarf

Dr. Silvia Knittl

Das IT-Compliance-Management hat die Aufgabe sicherzustellen, dass die IT konform zu den jeweiligen Vorgaben ist. Unternehmensarchitekturmanagement (Enterprise-Architecture-Management, EAM) beschreibt und strukturiert komplexe IT-Systeme und zeigt deren Zusammenhang zu den geschäftlichen Aufgaben in einer Organisation. In diesem Beitrag wird untersucht, inwieweit die Methoden des EAM für das IT-Compliance-Management eingesetzt werden können. Die Grundlage dazu bildet ein konkreter Fall aus der Praxis in Regierungsverwaltungen, wo in einem Identitäts- und Access-Management-Projekt bereits erfolgreich EAM-basierte Ansätze eingesetzt wurden und sich die Frage ergab, ob mit den gleichen Methoden auch die Governance entwickelt werden könnte. Der Beitrag zeigt dazu abgeleitete Anforderungen, aus der Literatur identifizierte Lösungsbausteine und weist offene Fragen bzw. möglichen weiteren Forschungsbedarf aus.

Zusätzliche Schlüsselwörter: IT-Compliance-Management, EAM, TOGAF, SABSA

1 EINLEITUNG

Compliance ist ein Querschnittsthema und betrifft alle Bereiche innerhalb einer Organisation. Die Anforderungen an Compliance umfassen laut [TÜVRheinland (2011)]: „Alle Regeln, die von der Organisation und den dort tätigen Personen zu beachten sind, unabhängig davon, ob es sich um gesetzliche oder behördliche Compliance-Anforderungen handelt oder solche, deren verbindliche Anwendbarkeit die Organisation für sich selbst oder eine andere Organisation für seine Mitglieder festgelegt hat." Abbildung 1 zeigt einen Auszug verschiedener Regeltypen, die in einem Compliance-Management-System zu berücksichtigen sind.

In diesem Beitrag wird der Fokus auf das IT-Compliance-Management gelegt. Betrachtet wird dabei ein konkreter, aber anonymisierter Fall, von Regierungsbehörden. In diesem Fall ist die Aufgabenstellung in einem IT-Sicherheitsprojekt die Einführung von Identity- und Access-Management (IAM) und die Sicherstellung der dazugehörigen Steuerungs- und Führungsprozesse einschließlich der Schaffung der notwendigen rechtlichen Rahmenbedingungen für den Einsatz dieses IAM-Systems.

Dr. S. Knittl
access GmbH, Marktstraße 47-49, 64401 Groß-Bieberau

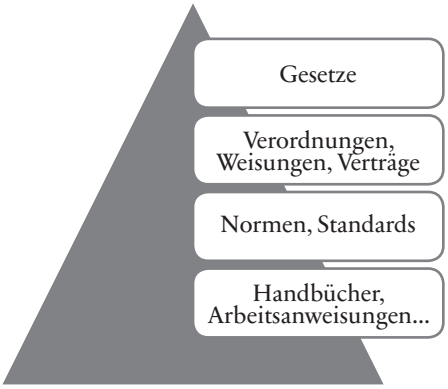


Abb. 1: Compliance: Pyramide verschiedener Regeltypen (Quelle: Eigene Darstellung)

Für das IAM wurde ein architekturgestützer Ansatz gewählt. Die Fragestellung ist nun, ob Steuerungs- und Führungsprozesse ebenfalls mittels eines architekturgestützen Ansatzes umgesetzt werden können. Betrachtet werden hierbei aus Gründen der Übersicht nicht alle möglichen Steuerungs- und Führungsprozesse, sondern das IT-Compliance-Management. Dazu wird zunächst die Fallstudie kurz beschrieben und bereits entdeckte Anforderungen aufgestellt. Im nachfolgenden Abschnitt werden mögliche Lösungsansätze dargestellt und offene Fragen bzw. weitere Forschungsfragestellungen aufgezeigt.

2 FALLBESCHREIBUNG: ARCHITEKTURGESTÜTZTES IT-COMPLIANCE MANAGEMENT IM BEHÖRDENUMFELD

In diesem Abschnitt wird der bisher gewählte Entwicklungsansatz für IT-Compliance-Management in einer Regierungsorganisation strukturiert dargestellt. Ausgangslage waren Steuerungs- und Führungsprozesse für IAM. Das IAM selbst wurde mittels eines architekturgestützten Verfahrens basierend auf TOGAF und SABSA entwickelt [Open Group (2011)]. TOGAF ist ein Architektur-Rahmenwerk und umfasst Methoden und Werkzeuge mit dessen Hilfe Unternehmensarchitekturen entwickelt werden können. SABSA ist ein Rahmenwerk zur Entwicklung risikogetriebener Unternehmenssicherheitsarchitekturen und wird aufgrund seines modularen Aufbaus oft in Teilen oder in Kombination mit anderen Sicherheits-Rahmenwerken eingesetzt (vgl. z. B. [Hoernes (2014)], [Taiwhenua (2014)], [Siedsma und Verboven (2015)]). SABSA wurde in TOGAF integriert [Open Group (2011)] und gliedert die Ergebnisartefakte eines Architekturentwicklungsprojektes in einer Matrix (siehe Abbildung 2). Für diese Matrix verwendet es in einer Dimension sechs einfache Fragepronomen und in der anderen den Grad der Vergegenständlichung von der Idee bis zur Umsetzung, der wiederum jeweils eine federführende Rolle zugeordnet ist.

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	Business Desicions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
Conceptual	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
Logical	Information Assets	Risk Management Poicies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
Physical	Data Assets	Risk Management Practices	Process Mechanism	Human Interface	ICT Infrastructure	Processing Schedule
Component	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
Service Management	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management

Abb. 2: SABSA-Matrix (Auszug aus [Open Group (2011)])

Die nachfolgende Beschreibung folgt nun in der Struktur dem SABSA-Modell und beschränkt sich aus Gründen der Übersicht auf dessen Dimensionen Organisation (Wer – „People“), Motivation (Warum), Prozessmodell (Wie) und Informationsmodell (Was – „Business Assets“) auf der Kontextebene.

2.1 Organisatorische Aspekte von IT-Compliance-Management und dessen Motivation

Die betrachteten Regierungsbehörden folgen der typischen Organisation einer Stab- bzw. Linienorganisation. Die Grundlage der Handlungen der verschiedenen Organisationseinheiten liegen als Auftrag vom Gesetzgeber im Rahmen einer Verfassung, Gesetz oder Regierungsbeschluss vor [Spektor 2005]. Zu den Aufgaben der Regierungsorganisationen gehört jedoch auch die Vorbereitung von Gesetzen. Die Prüfung von Regierungsorganisationen ist institutionalisiert durch dedizierte Kontrollorgane und ist etabliert im Bereich Datenschutz oder im Bereich der Finanzkontrolle, wie etwa auf Bundesebene der Bundesrechnungshof in Deutschland oder die Eidgenössische Finanzkontrolle in der Schweiz. Für diese beiden Prüfaufgaben, d. h. im Bereich Datenschutz und Finanzen, liegen dann auch entsprechende gesetzliche Grundlagen vor. Neben gesetzlichen Vorgaben werden im Bereich der Motivation weitere Regelungen vorausgesetzt. Zur Umsetzung von IAM in diesem Beispiel sind bewährte Methoden im Bereich der Unternehmenssicherheitsarchitektur als relevante Grundlagen identifiziert worden, wie etwa TOGAF, SABSA und Archimate [Hoernes (2014)].

IAM ist nun eine Disziplin, die alle Organisationseinheiten betrifft, die diese entsprechenden Dienste einsetzen. Das dafür umzusetzende IT-Compliance-Management-System muss nun die Rollen und Verantwortlichkeiten über eine dezentrale, verteilte Organisation hinweg konsistent festlegen. Die IT selbst ist in Regierungsorganisationen oft verteilt auf verschiedene interne und externe Organisationseinheiten. Die Komplexität der IT-Organisation, die von einem IT-Compliance-Management-System in solchen Behörden erfasst werden muss, ist u. a. in [Knittl und Wiedmer (2015)] dargestellt.

Als Anforderung ergibt sich somit im Bereich „People“ die Definition der relevanten Rollen und deren Verantwortlichkeiten. In der Abbildung 4 sind bereits drei der relevanten Rollen im Kontext Compliance dargestellt: die zuständige Rolle für den Erlass einer Vorgabe bzw. eines Gesetzes, diejenige für die Umsetzung und diejenige für die Prüfung der Konformität. Im Bereich der „Motivation“ besteht die Anforderung der Prüfung, ob die rechtlichen Grund-

lagen für deren jeweilige Aufgaben ausreichend sind und ob die weiteren methodischen Vorgaben, wie etwa die verwendeten Methoden SABSA, TOGAF oder Archimate prinzipiell für die Umsetzung geeignet sind.

2.2 Informationsmodell für IT-Compliance-Management

Die „Business-Assets", d. h. die relevanten Informationsobjekte im IT-Compliance-Management, sind in einem geeigneten Informationsmodell abzubilden. Wichtig ist hier zum einen, den eigentlichen Gegenstand von IT-Compliance, d. h. die IT selbst zu erfassen. Zum anderen sind auch die zu berücksichtigenden Vorgaben vollständig zu ermitteln und entsprechend abzubilden. Als Anforderung ergibt sich somit, dass das Informationsmodell mindestens enthält, welche Vorgaben auf welche Assets anzuwenden sind.

2.3 Prozesse für IT-Compliance-Management

Die eigentlichen Prozessaktivitäten im IT-Compliance-Management unterscheiden sich bei Behörden nicht von denjenigen anderer Organisationen und sind vereinfacht nach [FINSOZ e.V. (2014); [TÜVRheinland (2011)]:

2.3.1 Analyse und Erfassung relevanter Vorgaben

Zunächst müssen die für die Organisation relevanten Vorgaben ermittelt werden und in geeigneter Form erfasst werden. In der Abbildung 3 werden etwa auszugsweise Vorgaben dargestellt, die im Rahmen eines Identitäts- und Access-Management-Projekts im ersten Schritt als relevant identifiziert worden sind.

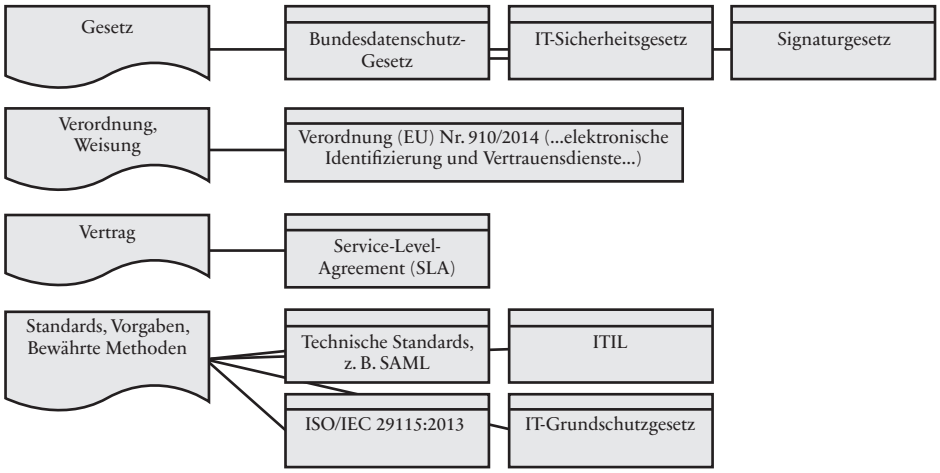


Abb. 3: Vorgaben: Auflistung für ein IAM-Projekt (Auszug) (Quelle: Eigene Darstellung)

2.3.2 Ableiten von Anforderungen

Im nächsten Schritt sind dann je Vorgabe, die aus der Vorgabe zu berücksichtigenden Anforderungen und entsprechende Kontrollmerkmale abzuleiten.

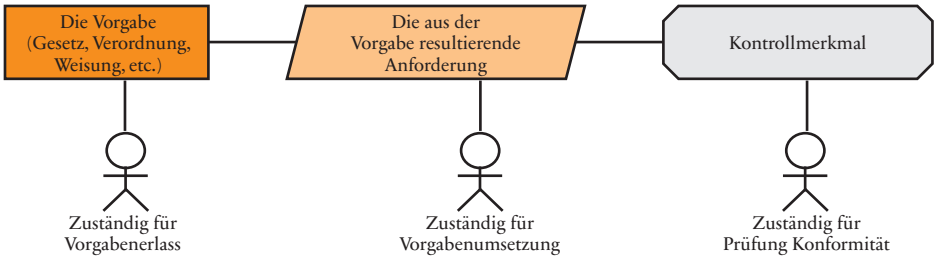


Abb. 4: ArchiMate-Notation: Vorgabe – Anforderung – Kontrollmerkmal (Quelle: Eigene Darstellung)

Die Abbildung 5 zeigt dazu auszugsweise Anforderungen aus dem Bundesdatenschutzgesetz visualisiert mit Hilfe der ArchiMate-Notation [OpenGroup (2013)]. Eine aus §4 resultierende Anforderung ist, dass die Zulässigkeit der Datenverarbeitung per Gesetz oder durch die Einwilligung des Nutzers erlaubt worden sein muss. Aus dieser Anforderung ergeben sich dann mögliche Kontrollpunkte, wie die Prüfung der rechtlichen Grundlage oder die der Nutzereinwilligung.

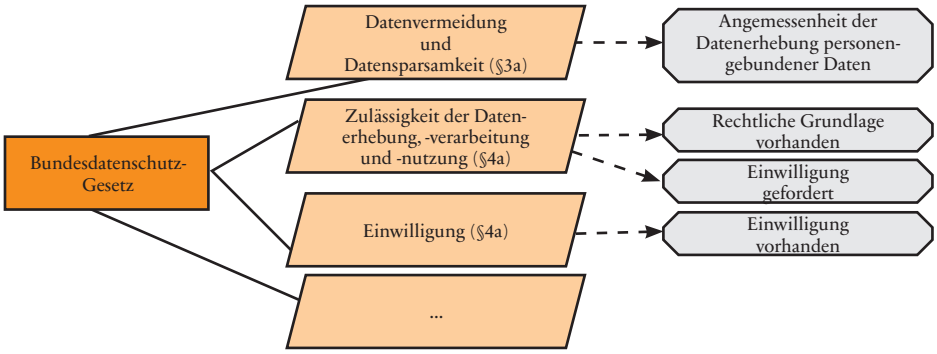


Abb. 5: Bundesdatenschutzgesetz – Auszug Anforderungen und Kontrollmerkmale in ArchiMate-Notation (Quelle: Eigene Darstellung)

2.3.3 Integrieren

In dieser Phase wird entschieden, welche der vorher ermittelten Anforderungen wie und zu welchem Grad umgesetzt werden. Dazu können Arbeitsabläufe so gestaltet werden, dass diese die Erfüllung der Compliance-Anforderungen erleichtern oder ermöglichen oder es können Kontrollmechanismen festgelegt werden, um etwaige Nichtkonformität erkennen zu können.

2.3.4 Prüfen

In der letzten Phase erfolgt eine gem. Prüfplan durchgeführte Prüfung der Konformität. Wichtig ist dabei auch das nachhaltige Dokumentieren und stufengerechte Kommunizieren der Ergebnisse. Diese erstellten Dokumente bilden dann auch die Grundlage für die Evaluation der Wirksamkeit des gesamten Compliance-Management-Systems.
Die Anforderung im Prozessbereich ist hier die geeignete Abbildung auf die betrachtete Organisation. Als Grundlage dazu müssen vorab die oben geforderten Rollen und Verantwortlichkeiten festgelegt worden sein.

3 LÖSUNGSANSÄTZE UND FORSCHUNGSBEDARF BEI ARCHITEKTURGESTÜTZTEN ANSÄTZEN IM BEREICH IT-COMPLIANCE-MANAGEMENT BEI BEHÖRDEN

Im vorherigen Teil wurden Anforderungen an IT-Compliance-Management basierend auf der betrachteten Fallstudie ermittelt. In diesem Abschnitt wird nun aufgezeigt, inwieweit und bei welchen Aspekten architekturgestützte Ansätze das IT-Compliance-Management in Regierungsbehörden unterstützen können und wo es weitere offene Fragen bzw. weiteren Bedarf an Forschung geben könnte.

3.1 Organisation und Motivation

Wie oben dargestellt, benötigen Verwaltungen als Grundlage für ihre Handlungen eine gültige Rechtsgrundlage. In der Schweiz etwa wurde in der Bundesinformatikverordnung die Grundlagen für eine IKT-Steuerung und -Führung gelegt. In den USA hat der Clinger-Cohen Act bereits 1996 eine formelle Grundlage dafür geschaffen, dass bewährte Praktiken im IT-Management auch für Behörden eingeführt werden können. Festgelegt wurde dazu die CIO-Position in jeder größeren Einheit und die Forderung nach der Erstellung von Unternehmensarchitekturen [Congress of United States of Amerika (1996)]. In weiteren Analysen wäre daher zu prüfen, ob die bestehenden rechtlichen Grundlagen ausreichend sind.

Eine notwendige Voraussetzung zur Umsetzung von Unternehmensarchitektur-Management und daher auch für ein architekturgestütztes Compliance-Management in Verwaltungsorganisationen ist laut [Obermeier (2014)] die Festlegung von Rollen und Verantwortlichkeiten unter der Berücksichtigung der spezifischen Rahmenbedingungen der öffentlichen Verwaltung. Hierzu sind weitere Analysen notwendig, welche spezifischen Rollen und Verantwortlichkeiten es in der jeweiligen Verwaltungsorganisation sind. Möglicherweise könnte der Multi-Level-Governance-Ansatz der OECD hier auch für IT-Compliance entsprechenden Input liefern [Rodrigo, Allio und Andres-Amo (2009)]. In [Schultis, Elsner und Lohmann (2014)] werden drei verschiedenen Kollobarationsmodelle für große, dezentrale Architekturprojekte vorgestellt. Weitere Fragestellungen könnten sich damit beschäftigen, ob und welche der dort ermittelten Herausforderungen in der Organisation von Architekturprojekten in großen, dezentralen Umgebungen von der Industrie- auf Verwaltungsumgebungen übertragbar sind.

3.2 Prozess

Es gibt bereits viele Ansätze im Bereich Compliance von Unternehmensarchitekturen, die sich damit beschäftigen, wie die Unternehmensarchitekturen selbst konform zu verschiedenen Vorgaben gestaltet werden können. In [Obermeier (2014)] werden etwa explizit Anforderungen für öffentliche Verwaltungen postuliert, wie etwa dass das EAM-Konzept die Prüfung von Prinzipien und Richtlinien erzwingen und dass es in bestehende Managementprozesse eingebettet werden muss. IT-Compliance-Management wäre so ein bestehender Managementprozess, es wird jedoch hierzu keine dedizierte Lösung entwickelt. In [Liimatainen, Heikkilä und Seppänen (2008)] werden Ansätze aufgestellt, wie in Behörden Entwicklungsprogramme konform zur Architektur gestaltet werden können, in [Knodel und Popescu (2007)] wird dargestellt, welche Mechanismen es gibt, um Architektur-Compliance festzustellen. Im Artikel von [Lohmann (2011)] werden Ansätze zur Compliance von Geschäftsprozessen dargelegt.

Nur wenige Ansätze beschäftigen sich jedoch damit, wie mittels architekturgestützer Verfahren das IT-Compliance-Managment selbst effektiv entwickelt sowie eingesetzt werden kann. In [Vicente (2011)] beschreibt der Autor in seinem Ansatz eine Referenzarchitektur für ein integriertes Governance-, Risiko- und Compliance-Management unter Verwendung der

Architekturentwicklungsmethode (ADM) von TOGAF und ArchiMate. Bei diesem Ansatz wären weitere Assessments notwendig, inwieweit diese in Verwaltungsorganisationen eingesetzt werden können. [Foorthuis, et al. (2009)] beschreiben, wie Organisationen (Business) und IT-Projekte auf Compliance überprüft werden können mit Hilfe von Unternehmensarchitektur. Sie beschreiben in ihrer Arbeit verschiedene Arten von Compliance-Checks, wie etwa für Korrektheit, Konsistenz oder Vollständigkeit. Der Beitrag von [Julisch et al. (2011)] verfolgt einen ähnlichen Ansatz mit Pattern-basierten Kontrollen. Bezogen auf obiges Funktionsmodell ist zu prüfen, wie diese Ansätze im IT-Compliance-Management bei Behörden verwendet werden können

3.3 Informationsmodell

Die obige Anforderung nach Erstellung von Informationsmodellen für IT-Assets in verteilten, dezentralen Umgebungen wurden u. a. in [Knittl (2012)] gezeigt. Dort wurde auch der Zusammenhang zwischen dem ITIL-basierten Konfigurationsmanagement und dem Unternehmensarchitekturmanagement dargelegt. Eine interorganisationale CMDB kann somit als Werkzeug eine Basis für organisationsübergreifendes Architekturmanagement bilden. Wie die ioCMDB für das IT-Compliance-Management verwendet werden könnte, wäre in weiteren Analysen zu prüfen. Der Ansatz von [Sillaber und Breu (2012)] zeigt auf, dass in einem Provider-Netzwerk die jeweiligen Compliance-Anforderungen über das gesamte Netzwerk entsprechend abgebildet werden müssen. Sie liefern hierzu ein Metamodell, dessen Verwendung in einer ioCMDB zu testen wäre. Prinzipiell ist die Unterstützung der Prozessaktivitäten durch architekturgestützte Verfahren möglich. Die Modellierungskonvention ArchiMate [OpenGroup (2013)] kann dazu verwendet werden, wie z. B. [Waltl, Schneider und Matthes (2014)] in ihrer Arbeit beschreiben. Dort zeigen die Autoren explizit die Machbarkeit der Modellierung von Compliance-Anforderungen mittels ArchiMate. ArchiMate wurde daher auch für die Darstellung der obigen Abbildungen verwendet. Jedoch setzt diese Aufgabe voraus, dass die entsprechenden Anforderungen einfach aus dem Gesetz bzw. der Vorgabe extrahiert werden können. Aktuelle Untersuchungen zeigen jedoch, dass die Komplexität der Gesetzestexte und deren Zerlegung selbst noch ein eigener Forschungsgegenstand sind [Waltl und Matthes (2015)]. Hierbei stellt sich die Frage, ob relevante Vorgaben und Gesetze, zumindest solche, die die IT betreffen, nicht von vornherein selbst mittels modellbasierter Verfahren entwickelt werden könnten, um deren Übertragbarkeit und damit Anwendbarkeit im Bereich der IT-Compliance zu erleichtern. Im Vorgehensmodell zur Erstellung von Gesetzen etwa dürfen bereits bei Bedarf kausale Modelle zur Illustration der Zusammenhänge von Ursachen und Problemen verwendet werden (vgl. z. B. [Bundesamt für Justiz (2014)]), der daraus entwickelte eigentliche Gesetzestext darf dann allerdings nur in natürlicher Sprache formuliert werden (z B. [Schweizerische Bundeskanzlei (2015)], [Bundeskanzleramt Österreich (2004)]) und soll möglichst knapp und einfach formuliert werden [Bundeskanzleramt Österreich (1990)]. Weiterer Forschungsbedarf wäre daher notwendig zur Untersuchung, inwieweit die Methoden der Rechtserzeugungsprozesse zumindest für die IT betreffende Gesetze auf architekturbasierte Verfahren umgestellt werden könnten, um deren Anwendbarkeit für die IT-Compliance zu vereinfachen.

4 ZUSAMMENFASSUNG

In diesem Artikel wurde anhand eines Fallbeispiels vorgestellt, welche Herausforderungen es beim Einsatz architekturgestützter Methoden im IT-Compliance-Management gibt. Die Ausgangslange war ein Projekt im Sicherheitsbereich im Verwaltungsumfeld in der Domäne Identitäts- und Access-Management (IAM). Dort wurden erfolgreich die Methoden des Architekturmanagements, wie etwa TOGAF, SABSA und ArchiMate, für dessen Entwicklung eingesetzt. Es ergab sich daher die Fragestellung, ob diese Methoden nicht ebenso erfolgreich zur Entwicklung von Steuerung und Führung von IAM, am Beispiel des IT-Compliance-Managements, verwendet werden können. Beleuchtet wurden daher die Anforderungen an ein architekturgestütztes IT-Compliance-Management anhand verschiedener Dimensionen und es wurde gezeigt, dass es in jeder der betrachteten Dimensionen bereits einzelne, teils isolierte Lösungsbausteine für eine Umsetzung gibt. Es sind nun jedoch weiteren Analysen oder Forschungsarbeiten notwendig, die prüfen, ob und inwieweit die hier identifizierten Ansätze für eine integrierte Lösung dienen können. Eine identifizierte Fragestellung ist es, ob die Methoden der Rechtserzeugungsprozesse selbst bereits mittels architekturbasierter Verfahren entwickelt werden könnten, damit die eigentliche Grundlage der IT-Compliance, nämlich Gesetze, unmittelbar, d. h. ohne nachträgliche Interpretation und Umsetzung in einer Unternehmensarchitektur angewendet werden können.

Methoden des Architekturmanagements für das IT-Compliance-Management zu verwenden, scheint nach obigen Analysen ein möglicher Weg zu sein. Die gewählte Fallstudie zeigt die Komplexität dieser Aufgabe in verschiedenen Bereichen: dezentrale Organisation, verteilte Verantwortlichkeiten, IT-Provider-Netzwerke, verschiedenartige, teils kontextabhängige zu berücksichtigende Vorgabetypen. Aus diesem Grund sollten zukünftig weitere Fallstudien zu diesem Thema durchgeführt werden. Dadurch können die hier aufgestellten Anforderungen auf deren Übertragbarkeit getestet und ggf. weitere neue Anforderungen ermittelt werden.

REFERENZEN

Bundesamt für Justiz (2014): Gesetzgebungsleitfaden – Module Gesetz, Verordnung und Parlamentarische Initiative, Bern, 2014.

Bundeskanzleramt Österreich (1990): Handbuch der Rechtssetzungstechnik – Teil 1: Legistische Richtlinien, Wien, 1990.

Bundeskanzleramt Österreich (2004): Richtlinien für die Erarbeitung und die Gestaltung von Rechtstexten und Muster, http://www.bundeskanzleramt.at/DocView.axd?CobId=1649, zuletzt aufgerufen am 17. Oktober 2015.

Congress of United States of Amerika (1996): Information Technology Management Reform Act (Clinger-Cohen Act of 1996), http://www.gpo.gov/fdsys/pkg/PLAW-104publ106/pdf/PLAW-104publ106.pdf, zuletzt aufgerufen am 8. Juli 2015.

FINSOZ e.V. (2014): IT-Compliance-Guideline für die Sozialwirtschaft – Richtlinienpapier FINSOZ e.V., https://www.finsoz.de/sites/default/files/dokumente/IT-Compliance-Guideline_V1f.pdf, zuletzt aufgerufen am 24. November 2015.

Foorthuis, R., Hofman, F., Brinkkemper, S. und Bos, R. (2009): Assessing Business and IT Projecs on Compliance with Enterprise Architecture, http://ceur-ws.org/Vol-459/paper6.pdf, zuletzt aufgerufen am 24. November 2015.

Hoernes, P. (2014): Ein IAM Grossprojekt aus der Perspektive des Enterprise Architekten – Erfahrungen aus der Schweizer Bundesverwaltung, Vortrag i. Rahmen d. GI Arbeitskreises EAM, 2014.

Julisch, K., Suter, C., Woitalla, T. und Zimmermann, O. (2011): Compliance by Design – Bridging the Chasm between Auditors and IT Architects, in: Computers & Security, Volume 30, Ausgabe 6-7, 2011, S. 410-426.

Knittl, S. (2012): Werkzeugunterstützung für interorganisationales IT-Service-Management – ein Referenzmodell für die Erstellung einer ioCMDB, 2012.

Knittl, S. und Wiedmer H. U. (2015): Dienste und IT-Governance in der Bundesverwaltung – Bedarf, Nutzen und Potenzial, in: eGov Präsenz, 01, 2015, S. 50-51.

Knodel, J. und Popescu D. (2007): A Comparison of Static Architecture Compliance Checking Approaches, in: Conference on Software Architecture (WICSA ,07), Mumbai, 2007, S. 12.

Liimatainen, K., Heikkilä J. und Seppänen V. (2008): A Framework for Evaluation Compliance of Public Service Development Programs with Government Enterprise Architecture, in: The 2nd European Conference on Information Management and Evaluation (ECIME 2008), London, 2008, S. 269-276.

Lohmann, N. (2011): Compliance by design for artifact-centric business processes, in: 9th International Conference, BPM, Clermont-Ferrand, 2011, S. 99-115.

Obermeier, M. (2014): Enterprise Architecture Management in der öffentlichen Verwaltung: Design, Einführung und Evaluation, München, 2014.

Open Group (2011): TOGAF® and SABSA® Integration – How SABSA and TOGAF complement each other to create better architectures, http://www.vanharen.net/Player/eKnowledge/togaf-and-sabsa-integration.pdf, zuletzt aufgerufen am 24. November 2015.

Open Group (2013): ArchiMate® 2.1 Specification, https://www2.opengroup.org/ogsys/publications/viewDocument.html?publicationid=13363&documentid=12366, zuletzt aufgerufen am 7. Juli 2015.

Rodrigo, D., Allio, L. und Andres-Amo, P. (2009): Multi-Level Regulatory Governance: Policies, Institutions and Tools for Regulatory Quality and Policy Coherence, in: OECD Working Papers on Public Governance, Nr. 13, 2009.

Schultis, K., Elsner, C. und Lohmann, D. (2014): Architecture challenges for internal software ecosystems: a large-scale industry case study, in: Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering (FSE 2014), New York, 2014, S. 542-552.

Schweizerische Bundeskanzlei (2015): SCHREIBWEISUNGEN – Weisungen der Bundeskanzlei zur Schreibung und zu Formulierungen, Bern, 2015.

Siedsma, P. und Verboven, M. (2015): Practical Experiences of SABSA Domain Modelling at ING, in: 7. SABSA World Congress, Naas, 2015.

Sillaber, C. und Breu, R. (2012): Managing legal compliance through security requirements across service provider chains: A case study on the German Federal Data Protection Act, in: Informatik 2012: Proceedings der GI/GMDS-Jahrestagung, Gesellschaft für Informatik, 2012, S. 1306-1317.

Spektor, I. (2005): Die Organisation der öffentlichen Verwaltungen, http://www.organisation-oeffentliche-verwaltung.de, zuletzt aufgerufen am 3. August 2015.

Taiwhenua, T. (2014): All-of-Government Risk Assessment Process: Information Security, https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf, zuletzt aufgerufen am 17. Oktober 2015.

TÜV Rheinland (2011): TR CMS 101:2011 – Standard für Compliance Management Systeme, https://www.tuv.com/media/germany/60_systeme/csr_nachhaltigkeit_compliance/compliance/faktenblaetter/compliance_standard_tr.pdf, zuletzt aufgerufen am 24. November 2015.

Vicente, P. F. O.(2011): A Reference Architecture for Integrated Governance, Risk and Compliance, Lissabon, 2011.

Waltl, B. und Matthes, F. (2015): Comparison of Law Texts: An Analysis of German and Austrian Legislation regarding Linguistic and Structural Metrics, in: Internationales Rechtsinformatik Symposium (IRIS), Salzburg, 2015.

Waltl, B., Schneider, A. W., und Matthes, F. (2014): Deriving and Modelling Compliance Requirements from Legal Audits, in: EICAR: Trust and Transparentcy in IT Security, Frankfurt am Main, 2014.

Dokumentationsmanagement als Erfolgsfaktor eines effektiven Informationssicherheitsmanagements

Manuela Reiss

Ein integriertes Dokumentationsmanagement ist ein wichtiger Erfolgsfaktor für ein effektives Informationssicherheitsmanagement. Die Praxis sieht leider häufig anders aus. Unternehmen, die sich für die Einführung von Informationssicherheitsmanagement (ISMS) ggf. mit einer Zertifizierung entscheiden, befassen sich in der Regel zwar ausführlich damit, welche Dokumente zu erstellen sind. Der Dokumentenverwaltung und -lenkung wird jedoch kaum Aufmerksamkeit gewidmet. Mehrwert, Anpassbarkeit und Funktionstüchtigkeit der Dokumentation bei sich ständig ändernden Organisationsumgebungen sind aber nur mit einem geordneten und geplanten Umgang mit der Dokumentation zu erreichen. Notwendig ist daher ein Dokumentationsmanagement, das eine zentrale Steuerung der Dokumentation ermöglicht und dafür u. a. Vorgaben zur Strukturierung und Verwaltung der Dokumente definiert.
In der jüngsten Zeit werden von der International Organization for Standardization (ISO) Anforderungen an die Steuerung der Dokumentation durch das Management definiert. Entsprechend diesen Vorgaben definiert das Kapitel 7.5 der ISO 27001:2013 [ISO/IEC (2013)] umfassende Anforderungen an das Management der Dokumentation. Aber Standards, Frameworks oder Modelle zur Implementierung eines integrierten Dokumentationsmanagements fehlen nach wie vor und damit den Unternehmen hilfreiche Ansätze zur Implementierung und zur Pflege einer anforderungsgerechten und nachhaltigen Dokumentation. In der Konsequenz ist das Dokumentationsmanagement ein weithin unterschätzter Managementbereich. Und auch in der wissenschaftlichen Literatur finden sich nur wenige Ansätze, die sich umfänglich mit dem Themenbereich Dokumentationsmanagement beschäftigen. Der Beitrag erläutert die Dokumentationsanforderungen der ISO-Norm und stellt auf Basis dieser Anforderungen einen Ansatz zur Umsetzung vor, mit dem Ziel einen kontrollierten und einheitlichen Umgang mit der Vielzahl an Dokumenten, die in einem Managementsystem wie dem ISMS entstehen, zu gewährleisten.

Zusätzliche Schlüsselwörter: Dokumentationsmanagement, Informationssicherheitsmanagement, Dokumentation, Dokumentenmanagement, Compliance

1 PROBLEMLAGE: FEHLENDES MANAGEMENT BEI DER DOKUMENTATION UND FEHLENDE ANSÄTZE ZUR STANDARDISIERUNG

Das folgende Kapitel zeigt zunächst typische Problemfelder im Umgang mit der Dokumentation in der Praxis auf und stellt anschließend aktuelle Ansätze in der Literatur vor.

Manuela Reiss
Limeshain, Deutschland
www.dokuit.de

1.1 Problemfelder bei der Dokumentation

Dass ein Informationssicherheitsmanagement mehr erfordert als die Absicherung der IT-Systeme ist den meisten Unternehmen bewusst. Ausgehend von den Risiken für die Geschäftsprozesse müssen alle Organisationsbereiche in die Betrachtung von Informationssicherheit einbezogen werden. In der Praxis bedeutet das aber auch, dass die Dokumentation bereichsübergreifend zu steuern und zu verwalten ist.

Dem ungeachtet fehlt es in vielen Unternehmen an einer zentralen Steuerung und Überwachung der Dokumentationsaufgaben. Und die von den Normen definierten Anforderungen an Verfahren zur Lenkung von Dokumenten existieren nicht selten nur auf dem Papier. Die häufigsten Schwachstellen sind dabei

- eine fehlende „funktionierende" allgemein nutzbare Dokumentationsplattform,
- fehlende formale Vorgaben für die Dokumente,
- fehlende Regelungen für die Verwaltung und Speicherung von Dokumenten,
- nicht gelebte Prozesse zur Qualitätssicherung der Dokumentation,
- fehlende Regelungen für die Aktualisierung der Dokumentation,
- eine unzureichende Zuordnung von Verantwortlichkeiten.

Die genannten Mängel führen u. a. dazu, dass häufig nicht bekannt ist, ob erforderliche Dokumente bereits existieren bzw. dass vorhandene Dokumente nicht aktuell, nicht konsistent und nur mit Mühe auffindbar sind.

Erschwerend kommt hinzu, dass es keine Standards, Frameworks oder Modelle zur Implementierung eines integrierten Dokumentationsmanagementsystems gibt. Erst in der jüngsten Zeit werden in einigen ISO-Normen auch Anforderungen an die Steuerung der Dokumentation durch das Management definiert (siehe Kapitel 2). Dementsprechend sind auch hilfreiche Ansätze zur Implementierung und zur Pflege einer anforderungsgerechten und nachhaltigen Dokumentation in der Literatur kaum zu finden.

1.2 Aktuelle Lösungsansätze für ein Dokumentationsmanagement

Die Relevanz der Dokumentation, vor allem bei einer prozessorientierten Ausrichtung, wird zwar in der Literatur vielfach hervorgehoben. Bei Leonhard et al (2009) beispielsweise findet sich dazu folgende Aussage: „Die Dokumentation der Prozesse einer Organisation leistet einen unmittelbaren Beitrag zur Stabilität und zur Sicherheit der Prozesse sowie zur Fehlervermeidung und damit zur Gesamtwirtschaftlichkeit der Organisation." [Leonhard et al. (2009), S. 8] Wie eine solche Dokumentation effektiv und nachhaltig aufgebaut und gepflegt werden kann, wird hingegen nicht oder nur punktuell betrachtet. Dementsprechend ist auch der Begriff „Dokumentationsmanagement" bzw. „documentation management" in der Literatur nur vereinzelt und mit unterschiedlicher Definition zu finden.

Zu den Wenigen, die sich explizit mit dem Management der Dokumentation auseinandersetzen, gehört Andenmatten (2008). In seinem Praxishandbuch für Servicemanagement und IT-Governance beschreibt er die Anforderungen der ISO/IEC-Spezifikationen und definiert Anforderungen an ein Dokumentationsmanagement. So heißt es bei ihm „Dokumentation-Management stellt ein vollständiges und lückenloses Steuern und Regeln aller Dokumente und Daten zur Abwicklung des Geschäftes sicher. Dokumente und Daten sind den eingesetzten Systemen für die sachgerechte Abwicklung und Ordnung der Ablage zuzuweisen". [Andenmatten (2008), S. 47]

Ebenfalls aus Sicht der ISO 20000 fordern Disterer et al. (2010) die Handhabung und Lenkung aller Dokumente in einem übergeordneten Managementsystem festzulegen, einschließlich der Rollen, der Handhabung der Aufbewahrung (Aufbewahrungsort, Aufbewahrungsdauer, Archivierung), der Namensregeln sowie der Mechanismen zur Versionskontrolle [Disterer et al. (2010), S. 29-30].

Ausschließlich im Rahmen von Projektmanagement betrachtet Lent Dokumentationsmanagement und definiert es folgendermaßen: „Documentation describes the products, delivered by project, for service staff, operators and users. Documentation Management secures its correct, complete and recipient conform elaboration during the whole project course." [Lent (2013), S. 243]
Den wichtigsten Beitrag zu diesem Thema liefert Bald (2000) in seiner Arbeit Entwicklung eines generischen Systemansatzes für das Dokumentationsmanagement in Unternehmungen. Sein Ziel ist die Ableitung eines Systemansatzes für eine integrierte Dokumentation von Managementsystemen. Konkret beschreibt er ein integriertes Dokumentationsmodell für die Managementsysteme Qualitätsmanagement, Umweltschutz und Arbeitsschutz sowie weiterer Subsysteme. Im Gegensatz zu den bislang genannten Ansätzen, die fast ausschließlich dokumentenbezogene Komponenten betrachten und dabei Inhalt und Aufbau der Dokumente in den Vordergrund stellen, befasst sich Bald auch mit Fragen des Managements von Dokumentation. Bei ihm heißt es „Unter Dokumentationsmanagement wird […] die Summe aller Tätigkeiten und Funktionen verstanden, die im weiteren Sinne mit der Erstellung und Verwaltung (als Funktion des Dokumentenmanagements) […] von Dokumentationen der unterschiedlichsten Art in Verbindung stehen." [Bald (2000), S. 15]

2 ANFORDERUNGEN AN EINEN OPTIMIERTEN ANSATZ

Die vorgestellten Ansätze liefern allgemeingültige Aussagen zum Dokumentationsmanagement entsprechend ihrer jeweiligen Ansätze. Eine konkrete Hilfestellung zur Implementierung von Dokumentationsmanagement bietet nur Bald mit seinem Ansatz. Einschränkend fokussiert er sich dabei auf die folgenden Managementsysteme: Qualitäts- und Umweltschutzmanagement, Arbeitsschutz und ausgewählte Management-Sub-Systeme. Die genannten Systeme werden nicht exemplarisch betrachtet, sondern bilden die Säulen seines Modells, was den allgemeingültigen Nutzen seines Ansatzes begrenzt.
Unter der Prämisse moderner Unternehmensstrukturen mit integrierten Managementsystemen und umfassenden Anforderungen an das Management von Dokumentation ist aber gerade die Unterstützung eines integrierten Dokumentationsmanagementsystems, das das Informationssicherheitsmanagementsystem genauso unterstützt, wie das QM-System eine Hauptforderung an einen optimierten Ansatz. Welche weiteren Anforderungen sich ableiten und wie ein solcher Ansatz aussehen sollte, wird in Kapitel 3 vorgestellt.

Um sich einem eigenen Ansatz für ein ganzheitliches Dokumentationsmanagement zu nähern, ist ein Blick in die ISO/IEC Directives, Part 1, Consolidated ISO Supplement sinnvoll. Bei den ISO/IEC Directives, Part 1 [ISO/IEC (2014)] handelt es sich um einen Leitfaden für die Entwickler von Managementsystemstandards, der sicherstellen soll, dass zukünftig alle Normen einer gemeinsamen übergeordneten Struktur und einheitlichen Anforderungen entsprechen. Dementsprechend müssen alle neuen und überarbeiteten Normen den in den ISO/IEC Directives, Part 1 Anhang SL beschriebenen Anforderungen an die Struktur und die Kerninhalte entsprechen.
Die Struktur der beiden aktuellen ISMS-relevanten ISO-Normen 27000:2012 und 27000:2013 entspricht bereits den Vorgaben der ISO/IEC Directives, Part 1. Außerdem wenden sie den einheitlichen Basistext, die gemeinsamen Benennungen und die Basisdefinitionen für den Gebrauch in Managementsystemnormen an. Konkret werden in den ISO/IEC Directives, Part 1 in Kapitel Annex SL 7.5, Appendix 2 in Abschnitt 7.5 Documented information die folgenden Dokumentationsanforderungen definiert:

Generell: Von der Norm geforderte und als erforderlich befundene dokumentierte Informationen müssen vorhanden sein.
Erstellung und Verwaltung: Festlegungen für Dokumente hinsichtlich angemessener Kennzeichnungen und Formate sowie angemessener Eignungsprüfung und Genehmigung.
Steuerung dokumentierter Informationen: Steuerung dokumentierter Informationen

- zur Sicherstellung von Verfügbarkeit, Vertraulichkeit und Integrität
- sowie Implementierung geeigneter Maßnahmen für Änderungen (u. a. Versionskontrolle), Verteilung, Zugriff und Verwendung
- sowie Speicherung und Archivierung (Erhaltung der Lesbarkeit)
- sowie Löschung [ISO/IEC (2014), S. 132-133].

Neben der Anforderung zur Bereitstellung der notwendigen Dokumente leiten sich vor allem auch an das Management gerichtete Anforderungen ab, was durch die Zuordnung zum Managementrahmen der Norm verdeutlicht wird. Die Anforderungen schließen sowohl die Einrichtung eines Dokumentenmanagements zur Erstellung und Verwaltung der Dokumente als auch die Steuerung und Überwachung der Dokumentationsaufgaben ein. Konkret lassen sich die folgenden drei Aufgabenbereiche für das Dokumentationsmanagement ableiten:

- Bereitstellung von Richtlinien und Vorgabedokumenten,
- Festlegung von Struktur und Inhalt der Dokumentation,
- Steuerung der Dokumente während des gesamten Lebenszyklus.

3 AUFBAU EINES DOKUMENTATIONSMANAGEMENTSYSTEMS

Auf der Basis der Anforderungen aus den aktuellen ISO-Normen und langjähriger praktischer Erfahrungen wurde vom Autor ein Ansatz für ein prozessorientiertes Dokumentationsmanagementsystem entwickelt. Bevor dieses in Abschnitt 3.2 vorgestellt wird, werden zunächst die verwendeten Begriffe erläutert.

3.1 Begriffe und Abgrenzungen

Um Managementsysteme eindeutig, verständlich und konsistent darstellen und dokumentieren zu können, ist eine eindeutige Verwendung der Begriffe erforderlich. Dies gilt auch für das Dokumentationsmanagement. Da es jedoch weder in der Praxis, noch in der Literatur eine einheitliche Verwendung dokumentationsbezogener Begriffe gibt und auch die relevanten Normen und Standards in ihrer Terminologie nicht konsistent sind, ist im ersten Schritt eine Definition und Abgrenzung der hier verwendeten Begriffe erforderlich.
Im Mittelpunkt eines Dokumentationsmanagementsystems steht sicherlich der Begriff „Dokument". Eine gute Quelle für Dokumentationsbegriffe, die hier Eingang findet, stellt die ISO Norm 9000 dar. Diese definiert für den Bereich Qualitätsmanagement alle relevanten Begriffe, was auch den Begriff Dokumentation einschließt. Und hier heißt es: „Dokumente sind Informationen und ihr Trägermedium", wobei gemäß Anmerkung 1 das Trägermedium Papier, ein magnetisches, elektronisches oder optisches Speichermedium, eine Fotografie, ein Bezugsmuster oder eine Kombination daraus sein kann. Als Informationen wiederum bezeichnet die ISO 9000:2005 „Daten mit Bedeutung" [Europäisches Komitee für Normung (2005), S. 29]. Im weiteren Beitrag werden die beiden Begriffe Dokument und Informationen in diesem Sinne verwendet.
Weiterhin gilt es den Begriff „Dokumentation" zu betrachten. Sowohl umgangssprachlich aber auch in der Fachsprache wird eine Zusammenstellung von Dokumenten als Dokumentation bezeichnet, allerdings mit unterschiedlicher Ausprägung. In der Softwareentwicklung wird der Begriff Dokumentation beispielsweise häufig auf die Beschreibung von Softwareprodukten beschränkt, und der deutsche Duden definiert Dokumentation als eine „Zusammen-

stellung und Nutzbarmachung von Dokumenten und Materialien jeder Art." [Duden (2014), S. 29]
Festzustellen ist, dass bei den genannten Definitionen nicht explizit zwischen den Tätigkeiten und den Ergebnissen unterschieden wird. Diesen Aspekt berücksichtigen Leonhard et al. in ihrer Definition: „Dokumentation umfasst neben den hierzu erforderlichen Tätigkeiten auch die Dokumente selbst." [Leonhard et al. (2009), S. 179]
Dem folgend wird im vorliegenden Beitrag Dokumentation als „Zusammenstellung von Dokumenten und Materialien zu einem definierten Sachverhalt in beliebiger Art und auf jeglichen Medium" definiert. Hierbei schließt die Zusammenstellung sowohl die Tätigkeiten als auch die Ergebnisse der Dokumentationstätigkeiten mit dem Ziel ein, die Zustände von physischen Objekten, Prozessen, Planungen, Gedanken u. a. aktuell, vollständig, korrekt und nachvollziehbar abzubilden.

Deutlich schwieriger ist der Begriff „Dokumentationsmanagement" zu definieren. In der Literatur ist dieser Begriff nur vereinzelt und mit unterschiedlicher Definition zu finden, zumindest, wenn man die Definitionen außen vor lässt, die hierunter ausschließlich die operative Verwaltung von Dokumenten verstehen. Da eine ausführliche Ableitung der beiden Begriffe Dokumentationsmanagement und Dokumentenmanagement den Rahmen des Beitrags sprengen würde, sei an dieser Stelle lediglich auf die Publikationen von Leonhard et al. (2009), Andenmatten (2008), Disterer et al. (2010) und Bald (2000) verwiesen. Vom Autor wird der Begriff folgendermaßen definiert:
Dokumentationsmanagement ist die Summe aller Aktivitäten und Funktionen für die Steuerung und Verwaltung von dokumentierten Informationen, die gewährleistet, dass alle erforderlichen dokumentierten Informationen aktuell, vollständig und in ausreichender Qualität verfügbar sind.
Das Dokumentationsmanagement ist vom Dokumentenmanagement zu unterscheiden. Dokumentenmanagement beschreibt die meist datenbankgestützte Verwaltung von Dokumenten. Im Fokus stehen die operativen Aktivitäten im Rahmen des Dokumenten-Lifecycle. In Abgrenzung zum Dokumentationsmanagement werden hier übergeordnete Steuerungs- und Kontrollfunktionen durch das Management nicht betrachtet.
Zuletzt muss noch der Begriff der „Dokumentierten Informationen" betrachtet werden. Dieser wurde von der International Organization for Standardization mit den ISO-IEC Directives Part 1 zur Entwicklung von ISO-Normen eingeführt und wie folgt definiert:
„Documented information….
Information required to be controlled and maintained by an organization (3.01) and the medium on which it is contained
Note 1 to entry: Documented information can be in any format and media and from any source. Note 2 to entry: Documented information can refer to
- the management system (3.04) including related processes (3.12);
- information created in order for the organization to operate (documentation);
- vidence of results achieved (records)." [ISO_IEC Directives Part 1 (2014), S. 128]

Demnach umfassen die dokumentierten Informationen die aus Sicht der jeweiligen Managementnorm vom Unternehmen zu lenkenden und nachzuweisenden (aufrechtzuerhaltenden) Informationen einschließlich der eingesetzten Medien.

3.2 Komponenten des Systems

Aus den in Kapitel 2 beschriebenen Anforderungen lassen sich vier Bereiche ableiten, die im Rahmen eines Dokumentationsmanagementsystems zu betrachten sind:
- übergeordnete Vorgaben zur Steuerung der Dokumentation,
- Struktur und Inhalte der Dokumentation (die dokumentierten Inhalte),

- das Dokumentenmanagement zur Verwaltung der Dokumente im Dokumenten-Lifecycle,
- Systeme und Anwendungen für die Dokumentation.

Die folgende Abbildung zeigt die benannten Bereiche im Kontext des vom Autor entwickelten Dokumentenmanagementsystems.

Prozessorientiertes Dokumentationsmanagementsystem

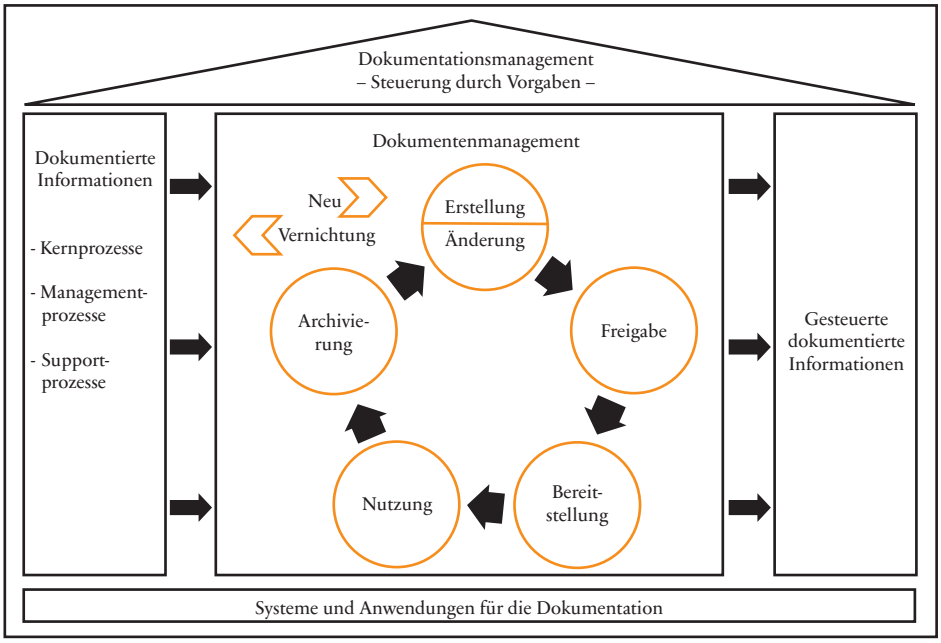


Abb. 1: Aufbau eines prozessorientierten Dokumentations-managementsystems [Reiss (2016), S. 302]

3.2.1 Dokumentationsmanagement – Steuerung durch Vorgaben

Die Steuerung der Dokumentation durch übergeordnete Vorgaben ist eine zentrale Aufgabe. Hierfür ist die in der Praxis häufig fehlende Dokumentationsrichtlinie ein wichtiges Instrument. Sie definiert auf welche Weise, in welcher Form und Tiefe und mit welcher Aktualität die Dokumentation zu pflegen ist. Außerdem macht die Dokumentationsrichtlinie Vorgaben zum Dokumentationsprozess und zu den Verantwortlichkeiten für das Dokumentationsmanagement. Die Erstellung und Durchsetzung einer Dokumentationsrichtlinie ist daher der erste und wichtigste Schritt zur Konsolidierung der Dokumentation und zur Implementierung eines Dokumentationsmanagements.

Sinnvollerweise wird die Dokumentationsrichtlinie (Management-Ebene) durch ein Dokumentationskonzept auf der operativen Ebene ergänzt, das Vorgaben für die Erstellung, Änderung und Speicherung von Dokumenten, d. h. für das Dokumentenmanagement definiert und diesem zuzuordnen ist.

3.2.2 Dokumentierte Informationen

Im Mittelpunkt steht hier die Frage: Was muss dokumentiert werden? Gerade bei einem Querschnittsthema wie dem Informationssicherheitsmanagement spielt diese Frage eine wichtige Rolle, da hiervon alle wesentlichen Prozesse des Unternehmens betroffen sind. Wichtig ist daher die Abbildung aller Dokumentationsbereiche und erforderlichen Dokumente in einer einheitlichen Struktur. Der Aufbau der Struktur schließt eine entsprechende Klassifizierung der Dokumente ein. Hilfreich ist hierfür eine Unterscheidung in Dokumentenklassen und Dokumententypen, wie in Abbildung 2 dargestellt. Zusätzlich müssen die erforderlichen Do-

kumente spezifiziert werden. Die konkreten Inhalte der Dokumente sind dann dezentral in den einzelnen Organisationsbereichen zu konkretisieren.

Dokumentenation für einen spezifischen Sachverhalt – ISMS-Dokumentation

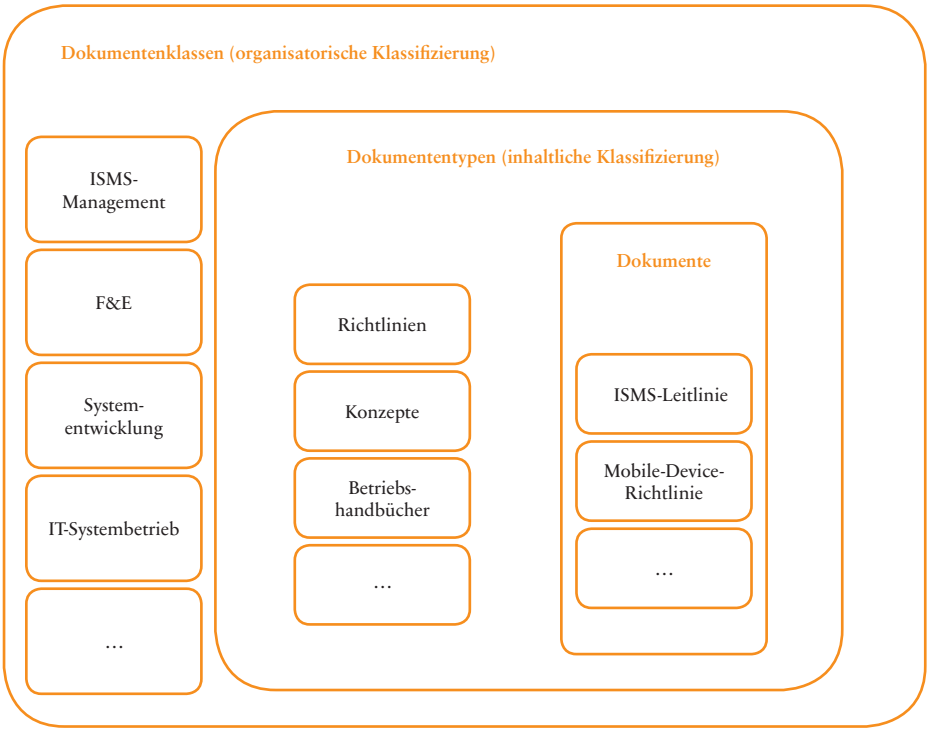


Abb. 2: Zusammenspiel von Dokumentklassen, Dokumententypen und Dokumente (Quelle: Eigene Darstellung)

Dokumentenklassen dienen der Unterscheidung von Dokumenten nach organisatorischen Kriterien. Im Bereich Informationssicherheitsmanagement sind das ISMS-Management, IT-Systembetrieb, Systementwicklung u. a. sinnvolle Klassen. Dokumentenklassen können in Unterklassen unterteilt werden. Für diese ist eine Unterscheidung nach inhaltlichen Kriterien sinnvoll. So kann beispielsweise die Dokumentenunterklasse IT-Systembetrieb in Systeme und operative Tätigkeiten unterteilt werden. Einer Dokumentenklasse können verschiedene Dokumententypen zugeordnet werden.
Ein Dokumententyp beschreibt eine Gruppe von Dokumenten mit gleichartigen Eigenschaften (Attribute). Die Zuordnung zu einem Dokumententyp definiert ein Dokument im Hinblick auf seinen Informationsinhalt, seine Anforderungen an die Dokumentenlenkung und die Darstellungsform. Die Einordnung kann generell oder sehr spezifisch erfolgen. Typische allgemeingültige Dokumententypen sind u. a. Richtliniendokumente, Prozessbeschreibungen, Installationshandbücher, Konzepte und Verträge. Die Klassifizierung kann bis zu einem konkreten Dokumententyp, z. B. Anwendungsbetriebshandbücher, verfeinert werden und ist dann durch einen gleichen inhaltlichen Aufbau gekennzeichnet.

3.2.3 Dokumentenmanagement

Eine wichtige Rolle innerhalb des Dokumentationsmanagementsystems spielt das eigentliche Dokumentenmanagement im Sinne der Erstellung und Verwaltung von Dokumenten auf Ba-

sis definierter Vorgaben. Jedes Dokument durchläuft von der ersten Arbeitsversion bis zu seiner endgültigen (finalen) Version die in Abbildung 1 dargestellten Phasen, einige davon auch mehrfach. Es ist demnach sicherzustellen, dass Dokumente während ihres gesamten Lebenszyklus gesteuert werden. Hierbei ist darauf zu achten, dass die Dokumente geordnet abgelegt werden, Änderungen kontrolliert erfolgen und zeitnah den betroffenen Personen kommuniziert werden.

- Erstellung und Freigabe: Der Lebenszyklus eines Dokuments beginnt mit dessen Erstellung. Die Notwendigkeit, Richtlinien und Vorgaben für das Erstellen und Freigeben von Dokumenten festzulegen, wurde bereits behandelt.
- Bereitstellung und Nutzung: Nachdem ein Dokument erstellt und gegebenenfalls freigegeben wurde, ist es in der vorher festgelegten Ablagestruktur für die Nutzung bereitzustellen. Diese Struktur muss sicherstellen, dass zu jedem Zeitpunkt allen Beteiligten bekannt ist, welchen Status ein Dokument aktuell hat und wo dieses abgelegt ist. Außerdem sollte die Ablage eine einfache Bereitstellung aller erforderlichen Dokumente unterstützen. Gleichzeitig müssen Berechtigungen sicherstellen, dass nur berechtigte Personen Zugriff auf die entsprechenden Dokumente erhalten.
- Dokumentenänderung: Die meisten Dokumente müssen entweder ab und zu geändert werden oder unterliegen regelmäßigen Überprüfungen. So fordern beispielsweise alle gängigen Standards im Rahmen des kontinuierlichen Verbesserungsprozesses auch eine Überprüfung und Überarbeitung der jeweiligen Dokumente. Wichtig ist, dass Änderungen standardisiert nach festen Vorgaben erfolgen. So muss zum einen sichergestellt werden, dass definierte Überprüfungszyklen auch nachvollziehbar eingehalten werden. Andererseits muss auch der Änderungsprozess selbst standardisiert erfolgen
- Archivierung: Die Archivierung von Dokumenten ist Voraussetzung für die Sicherstellung von Unveränderbarkeit, langfristiger Wiederauffindbarkeit, Wiedergabefähigkeit und jederzeitiger Verfügbarkeit eines Dokuments.

3.2.4 Systeme und Anwendungen für die Dokumentation

Mit steigendem Umfang und zunehmender Komplexität der Dokumentation steigt auch das Erfordernis nach einer zentralen IT-gestützten Datenhaltung und Tool-Unterstützung bei dem Dokumentenmanagement. Die entsprechenden Systeme und Anwendungen müssen die Dokumentationsaufgaben unterstützen und an den Vorgaben für das Dokumentationsmanagement ausgerichtet sein.

4 FAZIT

Für ein effektives Informationssicherheitsmanagement und nicht nur hierfür ist eine integrierte Betrachtung der verschiedenen Bereiche der Dokumentation und ein Dokumentationsmanagement mit Vorgaben und eingeführten Dokumentationsprozessen ein wichtiger Erfolgsfaktor. Ohne verbindliche Regelungen ergeben sich häufig individuell strukturierte Dokumentationsablagen, die die Verständlichkeit und Nachvollziehbarkeit der erarbeiteten Inhalte erheblich erschweren. Und übergeordnete Vorgaben sind Voraussetzung für die Durchsetzung einheitlicher Qualitätsstandards und für die Sicherstellung der Revisionssicherheit der Dokumentation.

Der vom Autor entwickelte Ansatz zum Aufbau eines Dokumentationsmanagementsystems erleichtert nicht nur die Identifizierung und Zuordnung der im Rahmen von Informationssicherheitsmanagement bzw. anderer Managementsysteme benötigten dokumentierten Informationen („Was muss dokumentiert werden“), sondern bietet auch Hilfestellung für die Steuerung („Wie muss dokumentiert werden“).

REFERENZEN

Andenmatten, M. (2008): ISO 20000: Praxishandbuch für Servicemanagement und IT-Governance, Düsseldorf, 2008.

Bald, J. (2000): Entwicklung eines generischen Systemansatzes für das Dokumentationsmanagement in Unternehmungen, Aachen, 2000.

Duden (2014): Duden - Die deutsche Rechtschreibung: Das umfassende Standardwerk auf der Grundlage der aktuellen amtlichen Regeln, Berlin, 2014.

Disterer, G., Kunert, O., Eibich-Meyer, I. (2010): Zertifizierung nach ISO 20000: Projekt- und Dokumentationsmanagement, Hannover, 2010.

Europäisches Komitee für Normung (2005): Qualitätsmanagementsysteme - Grundlagen und Begriffe (EN ISO 9000:2005), Brüssel, 2005.

ISO/IEC (2013): International Organization for Standardization: ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements, 2013.

ISO/IEC (2014): ISO/IEC Directives Part 1 and Consolidated ISO Supplement, 2014.

Lent, B. (2013): Cybernetic approach to project management, Berlin und New York, 2013.

Leonhard, K.-W., Naumann, P., Odin, A. (2009): Managementsysteme – Begriffe: Ihr Weg zu klarer Kommunikation, Berlin u. a., 2009.

Reiss, M. und Reiss, G. (2016): Praxisbuch IT-Dokumentation: Vom Betriebshandbuch bis zum Dokumentationsmanagement – die Dokumentation im Griff, München, 2016.

Technische Prüfung der Datenschutzerklärungen auf deutschen Hochschulwebseiten

Tim Wambach, Prof. Dr. Konstantin Knorr

Alle deutschen Hochschulen präsentieren sich im Internet über eine Webseite. Datenschutzaspekte spielen für Besucher dieser Seiten, wie zukünftige Studierende und Forschungspartner, eine immer wichtigere Rolle. Der vorliegende Beitrag untersucht die Existenz und den Inhalt der nach der deutschen Gesetzgebung verpflichtenden Datenschutzerklärungen (DSE). Ferner wird untersucht, ob sich die DSE mit den tatsächlichen Inhalten der Webseiten deckt. Die Methodik beinhaltet eine manuelle Überprüfung ausgewählter Webseiten und eine automatisierte Prüfung mittels eines modifizierten PyQt-Browsers mit dem Fokus auf der Erkennung von Trackern. Die Auswertung der Daten zeigt, dass viele DSE entweder fehlen, falsche Informationen beinhalten oder unvollständig sind. Der Artikel endet mit einer Diskussion der Ursachen und Empfehlungen zur Verbesserung der Missstände.

Zusätzliche Schlüsselwörter: Datenschutzerklärung, Hochschulen, Web-Tracking, Cookies, LDSG, BDSG, TMG

1 EINLEITUNG

Die Webseite ist das digitale Aushängeschild einer Hochschule. Studiengänge und Forschungsprojekte werden Interessenten darin präsentiert. Im Unterschied zu anderen Webseiten spielen dabei kommerzielle Interessen, zumindest bei den staatlichen Hochschulen, nur eine untergeordnete Rolle. Außerdem sind bei Hochschulen Mitarbeiter sehr frei bei der Gestaltung ihrer Webseiten und müssen häufig keinen zentralen Vorgaben entsprechen. Die Betreiber der Webseiten sind öffentliche Institutionen und keine Unternehmen. Datenschutzaspekte spielen bei Webseiten öffentlicher Betreiber eine immer wichtigere Rolle wie jüngst [Beltermann (2015a), Beltermann (2015b)] zeigten.

Selbstverständlich beinhaltet der Datenschutz an Hochschulen viele andere Fragestellungen [Witt (2004)], die allerdings interner Natur sind und nicht von externen Parteien untersucht werden können. Die Startseiten der Internetauftritte der Hochschulen sind frei zugänglich

Tim Wambach, M.Sc.
Universität Koblenz-Landau, Fakultät für Wirtschafts- und Verwaltungsinformatik, Projekt: Strukturwandel des Privaten, 56070 Koblenz, Deutschland,
https://www.uni-koblenz-landau.de/de/koblenz/fb4/iwvi/aggrimm/team-en/tim-wambach
E-Mail: wambach@uni-koblenz.de

Prof Dr. Konstantin Knorr
Hochschule Trier, Fachbereich Informatik, Am Schneidershof, Postfach 1826, 54208 Trier, Deutschland,
http://www.hochschule-trier.de/index.php?id=knorr
E-Mail: knorr@hochschule-trier.de

und vermitteln dem Besucher ein Bild davon, welchen Stellenwert der Datenschutz bei der Hochschule genießt.

Wir haben uns daher in diesem Artikel das Ziel gesetzt, die Datenschutzerklärungen der deutschen Hochschulen manuell und automatisiert zu prüfen. Es wird nachgewiesen, dass nicht nur Benutzer bei der Interpretation einer DSE überfordert sind, sondern auch Hochschulen nicht in der Lage sind, ihrer Verpflichtung in ausreichender Weise nachzukommen.
Der Artikel gliedert sich dazu in folgende Abschnitte: Eine Einführung zu Datenschutz an den Hochschulen, Datenschutzerklärungen für Hochschulwebseiten und Web-Tracking gibt Abschnitt 2. In Abschnitt 3 wird eine manuelle Auswertung der Datenschutzerklärungen der zehn Hochschulen mit den meisten Studierenden durchgeführt. Abschnitt 4 prüft darauf aufbauend automatisiert die DSE von Hochschulen mit mehr als 2.000 eingeschriebenen Studenten. Beide Abschnitte beschreiben die dazugehörige Methode und die erhobenen Daten. Den Abschluss bildet Abschnitt 5 mit einer Diskussion der erhobenen Daten und verwandter Arbeiten sowie einem Ausblick auf zukünftige Betätigungsfelder.

2 GRUNDLAGEN

2.1 Datenschutz an deutschen Hochschulen

Die deutsche Hochschullandschaft umfasst aktuell 426 Hochschulen, die sich in die Gruppen staatlich, private und konfessionelle Hochschulen unterteilen lässt. Die älteste deutsche Hochschule ist die Ruprecht-Karls-Universität Heidelberg aus dem Jahr 1386. In den letzten Jahren wurde eine große Zahl neuer Hochschulen gegründet. Die Studierendenzahlen schwanken von weniger als 20 bis zu fast 80.000 an der Fernuniversität Hagen. In allen deutschen Bundesländern und großen Städten sind Hochschulen ansässig [Drachentoeter (2015)].
Die Hochschulen unterliegen den deutschen Datenschutzgesetzen. Die Hochschulen sind in der Regel Körperschaften des öffentlichen Rechts und zugleich staatliche Einrichtungen. Sie können aber auch in anderer Rechtsform errichtet werden. Die größte Gruppe der staatlichen Hochschulen unterliegt in der Regel dem Landesdatenschutzgesetz (LDSG) des entsprechenden Bundeslandes. Für andere Hochschulen kann auch das Bundesdatenschutzgesetz (BDSG) gelten. Laut den LDSG und BDSG sind die Hochschulen verpflichtet, einen Datenschutzbeauftragten (DSB) zu benennen. Dieser kann entweder hochschulintern benannt werden, oft z. B. ein Mitarbeiter des Rechenzentrums oder aus der Verwaltung (Rechtsabteilung) oder Professor. Extern kann z. B. eine Kanzlei oder ein anderes Unternehmen im Auftrag der Hochschule diese Aufgabe übernehmen. Eine zentrale Herausforderung des Datenschutzes ist, dass er (1) juristische und (2) technische Aspekte beinhaltet.
Die Hochschulen müssen per Datenschutzgesetz einen Datenschutzbeauftragen benennen. Der DSB übt eine komplexe und äußerst anspruchsvolle Tätigkeit aus, die technische, juristische und verwaltungsorganisatorische Fähigkeiten verlangt. Leider treten aufgrund der komplexen und sich häufig verändernden Hochschul-IT-Infrastruktur immer wieder „Datenpannen“ auf [Knoke (2015)].
Bei vielen Hochschulen ist ein Trend zu beobachten, den Datenschutz an Externe zu vergeben oder die Kompetenzen zu bündeln. Die Hochschulen in Baden-Württemberg unterhalten z. B. mit ZENDAS (Zentrale Datenschutzstelle der baden-württembergischen Universitäten) eine eigene Zentrale für den Datenschutz. In anderen Bundesländern gibt es regelmäßige Treffen der Hochschuldatenschützer, z. B. organisiert durch den Landesdatenschutzbeauftragen.
[Witt (2004)] gibt ein Überblick typischer Probleme beim Hochschuldatenschutz. [ZENDAS (2015)] liefert per wöchentlichem Newsletter aktuelle Informationen zum Hochschuldatenschutz.

2.2 Datenschutzerklärung für Hochschulwebseiten

Eine DSE ist laut Telemediengesetz (TMG) für alle Hochschulwebseiten verpflichtend. Nach § 13 TMG muss der Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über etwaige Weitergaben von Daten an Staaten außerhalb der EU unterrichten. Nach § 15 Abs. 3 TMG darf der Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Dienstanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen.
Der Aufbau und die Zuständigkeit für die Erstellung und Pflege der DSE sind bei den Hochschulen sehr unterschiedlich geregelt. Bei der Erstellung sind typischerweise Parteien wie das Rechenzentrum, Web-Redakteure, der Datenschutzbeauftragte und der Kanzler bzw. die Rechtsabteilung involviert. Oft wird die DSE als Teil des Impressums publiziert. Für die Struktur und den Aufbau der DSE gibt es keine klaren Vorgaben. Neben den rechtlich bindenden Vorgaben gibt es Aspekte, die z. B. von der OECD [OECD (2015)] empfohlen werden.

2.3 Web-Tracking

Web-Tracking im Internet hat in den vergangenen Jahren einen deutlichen Zuwachs erfahren. [Schneider et al. (2014)] analysieren den Einsatz von Web-Tracking Verfahren quantitativ. Damit Benutzer verlässlich zwischen verschiedenen Webangeboten verfolgt werden können, ist aus technischer Sicht die Einbindung eines externen Objekts, wie eines Scripts, Tracking-Pixel, Web-Bugs oder ähnliches notwendig. Durch Aufruf einer Webseite, die eine solche Einbindung vorgenommen hat (Embedder), wird eine Übermittlung an einen Tracking- oder Werbedienst (Tracker) bewirkt. Das Interesse des Webseitenbetreibers für den Einsatz von Web-Trackern kann betriebswirtschaftlich, z. B. zur Verbesserung der Marketingstrategie, begründet sein. Zudem stehen umfangreiche Analysetools kostenfrei zur Verfügung (Google Analytics). Für den Benutzer bringt eine solche unbemerkte Zusammenführung von Daten, die aus Webaktivitäten entstanden sind, jedoch nicht nur Vorteile.
In [Schneider et al. (2014)] wird gezeigt, dass Doubleclick und Adition die häufigsten Tracker sind, die auf deutschen Webseiten gesichtet wurden (Google Analytics wurde in dieser Arbeit nicht betrachtet). In [W3Tech (2015)] zeigt sich, dass ca. 50 % der Webseiten (weltweit) durch Google Analytics analysiert werden. Trackingmethoden dieser Art können allerdings vom Benutzer bemerkt werden. Es existieren bereits diverse Browsererweiterungen zum Selbstdatenschutz, z. B. Ghostery [Ghostery (2015)], die aber eine automatisierte Auswertung in ihren AGBs untersagen. Neben diesen technischen Maßnahmen werden Besucher durch Gesetze wie Landes-, Bundesdatenschutz- oder Telemediengesetz geschützt, sofern das Webangebot unter deutsches Recht fällt. Besonders zu erwähnen sind die „Impressumspflicht“ (§ 5 TMG) und Angaben zum Umgang mit personenbezogenen Daten (§ 13 TMG) in einer sog. DSE.

Aktuell ist es mit Standard-Browsern und deren Browsererweiterungen nur schwer möglich, Werbe- oder Trackingverfahren auf Webseiten verlässlich zu detektieren und zu messen. Dies ist nicht zuletzt der Vielfalt der Trackingmethoden geschuldet, die in [Mayer und John (2012)] näher beschrieben werden. Viele Cross-Domain-Tracking-Verfahren bewirken jedoch eine Verbindung vom Browser zum Trackinganbieter. Allein ein solcher Verbindungsaufbau ist bereits mit der Übergabe der IP-Adresse zu einer bestimmten Uhrzeit verbunden. Darüber hinaus wird durch die Verwendung von Cookies eine Zuordnung über mehrere Anfragen hinweg erleichtert. Zusätzliche Verbindungen, die nicht dem angeforderten Webauftritt angehören, werden im Folgenden als externe Verbindungen bezeichnet. Wird vom Benutzer bspw. eine Webseite angefordert, die Google Analytics zur Erhebung und Auswertung von Besucherstatistiken verwendet, baut der Browser im Hintergrund eine Verbindung zum Webserver von Google Analytics auf.

3 AUSWERTUNG DER DATENSCHUTZERKLÄRUNGEN DER ZEHN GRÖSSTEN HOCHSCHULEN

Im Juli 2015 wurden die Webseiten der zehn deutschen Hochschulen mit den meisten Studierenden (nach Angaben in [Drachentoeter (2015)]) untersucht. Zunächst wurde nach der DSE auf der Hauptseite gesucht. Falls diese gefunden wurde, wurde deren Inhalt geprüft und nach folgenden Kriterien aus den Kategorien (1) BASIS, (2) INHALT und (3) OECD bewertet. Tabelle 1 gibt eine Übersicht der Ergebnisse der Untersuchung.

	Basis				Inhalt				OECD			
Hochschule	Anzahl Wörter in DSE	Version	DSE vorhanden	Verweise auf Gesetze	HTTP-Logs	Web Tracker	Social Media	Werbung	Zweckbestimmung	Sicherung	Mitspracherecht	Ansprechpartner
Fernuniversität in Hagen	382	26.08.2014	IMP	LDSG	Ja	PIWIK	K.A.	K.A.	Ja	Nein	Nein	Ja-1
Ludwig-Maximilians-Universität München	2293	K.A.	Ja	LDSG, TMG	Ja	PIWIK	Facebook, Twitter	K.A.	Ja	Nein	Nein	Ja-2
Universität zu Köln	893	K.A.	Ja	K.A.	Ja	K.A.	Facebook, Google, Twitter, Youtube	Adition	Ja	Nein	Nein	Ja-1
Johann Wolfgang Goethe-Universität Frankfurt am Main		K.A.	FEHLT	K.A.	K.A.	K.A.	K.A.	K.A.	K.A.	K.A.	K.A.	K.A.
Ruhr-Universität Bochum	138	22.07.2015	IMP	K.A.	K.A.	PIWIK	Facebook	K.A.	Ja	Nein	Nein	Ja-1
Westfälische Wilhelms-Universität (Münster)	0	K.A.	FEHLT	K.A.	K.A.	K.A.	K.A.	K.A.	K.A.	K.A.	K.A.	K.A.
RWTH Aachen	424	14.05.2014	Ja	LDSG, TMG	Ja	K.A.	K.A.	K.A.	Ja	Nein	Ja	Ja-2
Universität Duisburg-Essen		07.04.2015	FEHLT	TMG	Ja	K.A.	Facebook, Twitter, Google+	K.A.	Ja	Nein	Nein	Ja-1
Universität Hamburg	614	K.A.	Ja	K.A.	K.A.	Google Analytics	Facebook	K.A.	Nein	Nein	Ja	Ja-2
Friedrich-Alexander-Universität Erlangen-Nürnberg		K.A.	IMP	K.A.	K.A.	K.A.	K.A.	K.A.	Nein	Nein	Nein	Ja-1

Tab. 1: Ergebnisse der manuellen Prüfung der DSE der größten deutschen Hochschulwebseiten (K.A. = „Keine Angaben“) (Quelle: Eigene Darstellung)

Die Kategorie BASIS umfasst:

- Die Spalte „Anzahl Wörter in DSE“ gibt an, wie viele Wörter die DSE enthält. Natürlich hängt die Länge der DSE von der Komplexität der spezifischen Hochschulinfrastruktur ab. Trotzdem gibt die Wortanzahl einen groben Anhaltspunkt, welche Bedeutung der Datenschutz auf der Webseite genießt.
- Version: Ist die DSE mit einem Datum oder einer Versionsnummer versehen? Das Fehlen einer Version erschwert es, bei wiederholten Besuchen Änderungen an der DSE zu erkennen.
- DSE vorhanden: Existiert eine separate DSE (=> „Ja“), ist sie Teil des Impressums (=>„IMP“) oder war sie nicht auffindbar („FEHLT“)? Laut einem aktuellen Urteil des OLG Hamburg sollte die DSE separat vom Impressum gehalten werden [Overbeck (2014)].
- Verweise auf Gesetze: Wird in der DSE auf einschlägige Gesetze wie das jeweilige LDSG, BDSG oder TMG verwiesen? Damit wird einem Besucher verdeutlicht, auf welcher Rechtsgrundlage die DSE steht.

Die Kategorie INHALT klärt, ob die DSE die technischen Aspekte HTTP-Logs, Web-Tracker, Social Media und Werbung adressiert und benennt ggf. die verwendeten Technologien.
Innerhalb der Kategorie OECD werden die folgenden Aspekte untersucht, die aus den OECD-Grundsätzen [OECD (2015)] abgeleitet sind:

- Zweckbestimmung: Wird der Grund für die Erhebung von personenbezogenen (PBZ) Daten angegeben?
- Sicherung: Werden Sicherheitsvorkehrungen genannt, mit denen die PBZ-Daten geschützt sind?
- Mitspracherecht: Wird der Benutzer auf die ihm nach BDSG zustehenden Rechte wie Auskunftsrecht und Löschrecht hingewiesen?
- Ansprechpartner: Wird ein Ansprechpartner für Datenschutzfragen genannt? Mögliche Antworten: „Nein", „Ja-1": Allgemeine Kontaktdaten, „Ja-2": Datenschutzspezifische Kontaktdaten

Nur vier von zehn Hochschulen haben eine separate DSE, drei haben gar keine, bei drei Hochschulen ist die DSE ins Impressum integriert. Die Länge schwankt zwischen 138 (Bochum) und 2.293 Wörtern (München). Nur bei vier von zehn ist die verwendete Version erkennbar. Vier von zehn Seiten nennen die rechtlichen Grundlagen. Fünf von zehn Seiten protokollieren die HTTP-Zugriffe. PIWIK (3) und Google Analytics (1) sind die erwähnten Tracker. Facebook (5) und Twitter (3) sind die am häufigsten erwähnten Social-Media-Seiten. Die Uni Köln nutzt als einzige Werbung (Adition).

Den Zweck der eigenen Datenerhebung nennen die meisten Seiten (=> statistische Auswertung, Abwehr/Erkennung von Angriffen). Die Verwendung von Werbung oder Social Media wird i.d.R. nicht begründet. Keine Seite nennt getroffene Sicherheitsvorkehrungen. Das Mitspracherecht wird nur bei zwei Seiten erwähnt. Drei Seiten haben spezifische Ansprechpartner für den Datenschutz, fünf allgemeine, zwei gar keinen.

4 AUTOMATISIERTE TRACKERERKENNUNG AUF HOCHSCHULWEBSEITEN

4.1 Methodik

4.1.1 Technische Grundlagen

Die Erhebung externer Verbindungen wäre z. B. durch Überwachung der Netzwerkkommunikation mittels tcpdump oder Wireshark möglich. Diese Methode hätte allerdings den Nachteil, dass unklar ist, an welcher Stelle die Webseite vollständig geladen wurde und die Überwachung beendet werden kann. Ebenfalls sind fehlerhafte Ergebnisse aufgrund der Aktivitäten anderer Anwendungen (im Hintergrund) nicht ausgeschlossen. Wir haben daher einen Browser so modifiziert, dass die erstellten externen Verbindungen nach dem Aufruf einer Webseite ausgelesen werden können. Die Python-Bibliothek PyQt [PyQt (2015)] beinhaltet einen Browser, der zur Verarbeitung gängiger aktueller Techniken (HTML, XHTML, CSS, JavaScript, HTML canvas, AJAX) in der Lage ist. Zur Analyse wurde das Framework durch die Einbindung einer eigenen QNetworkAccessManager-Klasse abgeleitet und so modifiziert, dass jede Verbindung durch den Browser protokolliert wird und anschließend ausgewertet werden kann. Die durchgeführten Änderungen werden in Listing 1 genauer dargestellt.

```
class NetworkAccessManager(QNetworkAccessManager):
  requests = []
  [...]
  def createRequest(self, operation, request, data):
    self.requests.append([ request.url().encodedHost(),
                           request.url().encodedPath()])

    return QNetworkAccessManager.createRequest(self,
                                               operation,
                                               request,
                                               data)
  def getRequests(self):
      return self.requests
```

Listing 1: Modifikation der QNetworkAccessManager-Klasse (Quelle: Eigene Darstellung)

Sobald alle Bestandteile der untersuchten Webseite vollständig geladen sind, ist der Analysevorgang abgeschlossen und gibt das Ergebnis aus, nämlich eine Auflistung sämtlicher HTTP-Anfragen (getRequests). Zur näheren Verdeutlichung ein Beispiel: Durch Abruf der Webseite http://www.uni-hamburg.de wurden am Tag der Erhebung, neben den Verbindungen zum Webserver der Universität selbst, auch Verbindungen zu serveby.flashtalking.com, t4ft.de, google-analytics.com und imagesrv.adition.com registriert. Vom Framework wird der HTTP User-Agent „User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/534.34 (KHTML, like Gecko) python Safari/534.34“ verwendet, ein durchaus typischer Eintrag, der auf aktuellen Windows-Plattformen Verwendung findet.

Die Überprüfung von Webseiten auf solche externen Verbindungen soll im Folgenden auf eine Testmenge angewendet werden, von der ein gewisses Maß an Sorgfalt im Umgang mit dieser Thematik erwartet wird. Dabei handelt es sich um Webauftritte von deutschen Hochschulen, die gemäß [Drachentoeter (2015)] mehr als 2.000 eingeschriebene Studierende (Stand: Juli 2015) aufweisen. Dies trifft auf 207 Einrichtungen zu. Bei dieser Analyseform wird lediglich die Hauptseite ausgewertet, d. h. es werden Verbindungen ausgewertet, die durch Aufrufen der Startseite erzeugt werden. Die Unterseiten bleiben von der Analyse unberührt. Automatische Weiterleitungen werden ausgeführt und berücksichtigt. Tag der Erhebung ist der 19.7.2015.

4.1.2 Überprüfung der Datenschutzerklärung

Nachdem nun eine Technik zur Erkennung von externen Verbindungen umgesetzt wurde, stellen wir die Frage, ob diese innerhalb der DSE berücksichtigt werden. Insbesondere beim Einsatz von Tracking-Verfahren muss dem Benutzer eine Widerspruchsmöglichkeit eingeräumt werden (§ 15 Abs. 3 TMG). Hierfür ist es notwendig, das Impressum bzw. die DSE des Webauftritts zu suchen.

Die Suche wird auf den Hauptseiten der Hochschuleinrichtungen durchgeführt. Im ersten Schritt wird auf der Hauptseite nach Links zu „Impressum“, „Datenschutz“, und „Privacy“ gesucht. Sofern eine solche Verlinkung gefunden werden kann, handelt es sich dabei um das gesuchte Dokument. Falls nur ein Link zum Impressum gefunden wird, wird anschließend in diesem nach Erwähnungen oder einer Verlinkung zu „Datenschutz“ oder „Privacy“ gesucht.

Werden im Impressum selbst Aussagen zum Datenschutz getroffen, sind Impressum und DSE zusammengefasst.
Auf diese Weise findet eine automatische Überprüfung statt, ob Impressum und DSE vorhanden sind. In den Fällen, in denen diese Dokumente nicht auffindbar waren, wurde anschließend eine manuelle Suche durchgeführt und die Daten ergänzt. Hierbei zeigten sich für einen Besucher möglicherweise unerwartet beiläufige Erwähnungen zum Datenschutz in sog. „Disclaimern", in denen ebenfalls Aussagen zum Urheberrecht der Inhalte getroffen wurden. Ebenfalls zeigten sich Fälle, bei denen Impressum und DSE nicht direkt auf der Hauptseite gefunden werden konnten, sondern eine Suche benötigten, bspw. http://www.unibw.de/.
Zur Auswertung von DSE muss der derzeitige IST-Zustand eines Webauftritts bestimmt und anschließend mit dem SOLL-Zustand aus der DSE verglichen werden. Nachdem nun eine Technik zur Bestimmung von externen Verbindungen entwickelt und eine Auflistung der Datenschutzerklärungen der Hochschulwebseiten zur Verfügung steht, kann nun ein automatischer Abgleich erfolgen. Hierfür muss zunächst festgelegt werden, nach welchen Begriffen innerhalb der DSE gesucht werden soll. Aus den beobachteten externen Verbindungen wurden die häufigsten mit einem Bezug zum Web-Tracking ausgewählt und genauer auf ihre Nennung in der DSE überprüft (vgl. Tabelle 2).
Zur automatisierten Analyse werden, sofern eine Verbindung zu einem dieser Dienste registriert wurde, Impressum und DSE nach einer Erwähnung des Dienstnamens selbst und dem Namen des Unternehmens durchsucht. Wird bspw. eine Verbindung zu google-analytics.com auf der Hauptseite detektiert, wird in den erwähnten Dokumenten sowohl nach „Google Analytics", als auch nach „Google" gesucht. Findet eine Erwähnung statt, wurde diese Weitergabe bei Erstellung der DSE bedacht. Andernfalls handelt es sich aufgrund der fehlenden Widerspruchsbelehrung (§ 15 Abs. 3 TMG) um eine nicht vollständige DSE, vgl. Tabelle 4.

4.2 Ergebnisse

4.2.1 Ergebnisse der Untersuchung von externen Verbindungen

In diesem Abschnitt werden die Ergebnisse der Untersuchung nach externen Verbindungen zusammengefasst. Die meisten Einbindungen standen in Verbindung zu Google, weshalb dieser ein eigener Abschnitt gewidmet ist (vgl. Abschnitt 4.2.2).
In 105 von 207 Fällen wurden keine externen Verbindungen registriert. In Tabelle 2 sind die Serveradressen von Ressourcen zu sehen, die in den verbleibenden 102 Fällen am häufigsten innerhalb der Hochschulwebseiten eingebunden wurden (fett markiert) sowie die Anzahl der Hochschulen, die eine solche Einbindung unternommen haben.

HOSTNAME	ANZAHL	GOOGLE-SERVICE	Bemerkungen
google-analytics.com	29	Ja	
ajax.googleapis.com	14	Ja	
fonts.googleapis.com	11	Ja	
www.googleadservices.com	10	Ja	
www.google.com	9	Ja	
code.jquery.com	8	Nein	JS-Bibliothek
imagesrv.adition.com	8	Nein	Werbeanbieter
doubleclick.net	7	Nein	Trackingdienst
s.ytimg.com	6	Ja	YouTube Vorschaubilder
www.youtube.com	6	Ja	
googletagmanager.com	4	Ja	
googleapis.com	3	Ja	
maps.google.com, translate.google.com , ssl.google-analytics.com, translate.google.com, translate.googleapis.com	2	Ja	
google.de, googletagservices.com, oauth.googleusercontent.com, tcp.googlesyndication.com	1	Ja	

Tab. 2: Top 10 (fett markiert) der am häufigsten registrierten externen Verbindungen & Google-Services (Quelle: Eigene Darstellung)

4.2.2 Externe Verbindungen zu Google

In den Analysen zeigte sich, dass 61 der 207 Hochschulwebseiten eine Verbindung zu einem Google-Service bewirkten. Hierbei wurde der Google-Service anhand der Zeichenkette „google“ im Hostnamen bestimmt. Services, die ebenfalls direkt oder indirekt Google angehören, wurden in diesem Fall nicht berücksichtigt, so z. B. „doubleclick.com“, das im Jahre 2007 von Google übernommen wurde. Der Grund hierfür ist, dass nicht in allen Fällen eine vollständige Erfassung geschäftlicher Beziehungen zwischen verschiedenen Tracking-Unternehmen möglich ist und deshalb zunächst nur die offensichtlichen Verbindungen betrachtet werden. In Tabelle 2 sind die zusätzlichen Google-Services aufgeführt und in Abbildung 1 ist der daraus resultierende Graph dargestellt.

4.2.3 Verwendung von Google Analytics

Die Testmenge wurde auf Einbindungen von google-analytics.com überprüft. Eine solche Einbindung fand in 29 Fällen statt. Google Analytics erlaubt eine Anonymisierung der Benutzer durchzuführen. In [Google (2015)] ist beschrieben, wie das letzte Oktett der IP-Adresse auf den Servern von Google entfernt wird – bei IPv6-Adressen die letzten 80 Bit. Ob diese Funktion genutzt wird, ist im Quelltext der Webseite oder über den ‚aip‘-Parameter der HTTP-Anfrage erkennbar. Die Kürzung wird jedoch erst nach der vollständigen Übertragung von Google selbst durchgeführt. Eine Übersicht der ‚aip‘-Verwendung bei den Hochschulen ist in Tabelle 3 einsehbar.

HOCHSCHULE	AIP
Macromedia Hochschule für Medien und Kommunikation	Ja
Hochschule für nachhaltige Entwicklung Eberswalde	Nein
Steinbeis-Hochschule Berlin	Ja
SRH Hochschule Heidelberg	Nein
Hochschule für Wirtschaft und Umwelt Nürtingen-Geislingen	Nein
AKAD Bildungsgesellschaft (Stuttgart)	Nein
Universität Hohenheim (Stuttgart)	Ja
Hochschule für angewandtes Management (Erding)	Ja
Hochschule für angewandte Wissenschaften Coburg	Ja
Universität Bayreuth	Ja
Diploma Hochschule (Bad Sooden-Allendorf)	Ja
Wilhelm Büchner Hochschule (Pfungstadt)	Ja
Europäische Fernhochschule Hamburg	Ja
HFH Hamburger Fern-Hochschule	Ja
Universität Hamburg	Ja
Private Fachhochschule Göttingen	Ja
HAWK Hochschule Hildesheim/Holzminden/Göttingen	Nein
Leuphana Universität Lüneburg	Ja
Hochschule Hamm-Lippstadt	Nein
Rheinische Fachhochschule Köln	Nein
FOM Hochschule (Essen)	Ja
Fachhochschule Kaiserslautern	Ja
Universität Koblenz-Landau	Ja
Hochschule Mittweida	Ja
Hochschule für Technik, Wirtschaft und Kultur Leipzig	Nein
Hochschule Anhalt (Bernburg, Dessau und Köthen)	Ja
Fachhochschule Nordhausen	Ja
Fachhochschule Schmalkalden	Ja
Ernst-Abbe-Fachhochschule Jena	Ja

Tab. 3: Nutzung von Google-Analytics auf Hochschulwebseiten (Quelle: Eigene Darstellung)

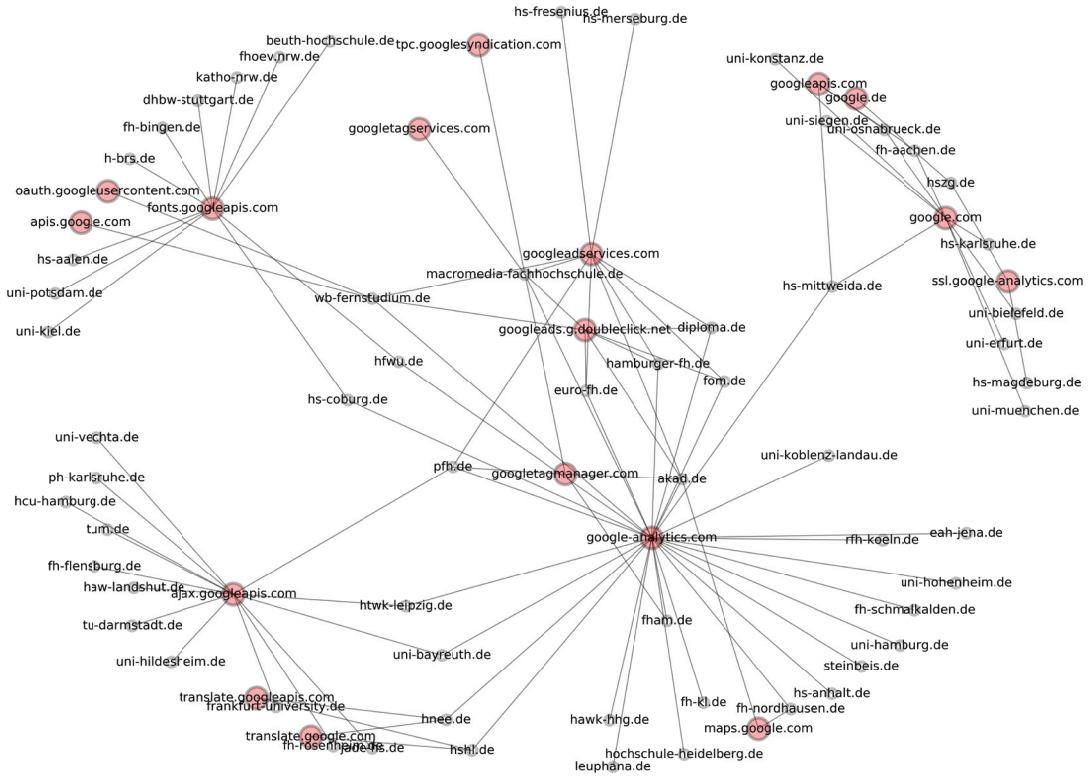


Abb. 1: Verbindungen von Hochschulwebseiten zu Google-Services (Quelle: Eigene Darstellung)

4.2.4 Ergebnisse der Untersuchung von Impressum und Datenschutzerklärung

In 20 der 207 Fälle waren keine expliziten Angaben zum Datenschutz auffindbar. In 137 Fällen wurde die DSE mit dem Impressum zusammengefasst bzw. war unter der gleichen Adresse abrufbar.

In 40 Fällen wurden Verbindungen zu den vier Anbietern (1) Google Analytics, (2) Doubleclick, (3) Adition oder (4) Facebook auf der Hauptseite detektiert. In 30 dieser Fälle wurden diese zumindest in Impressum oder DSE erwähnt. In den zehn verbleibenden Fällen war die DSE nachweislich unvollständig. Das Ergebnis dieser Analyse ist in Tabelle 4 einsehbar, wobei aus Gründen der Übersichtlichkeit die Negativ-Fälle gelistet sind. Es wurden zunächst nur diese vier Anbieter geprüft, da bei diesen klarer Bezug zu Tracking, Werbung und/oder Social Media erkennbar ist. Weitere Einbindungen wie z. B. „code.jquery.com“ wurden nicht weiter verfolgt.

Obwohl in vielen Datenschutzerklärungen explizit Facebook erwähnt wurde, konnte nur auf zwei Hauptseiten (http://diploma.de, https://www.akad.de) eine Verbindung zu Facebook gefunden werden. Dies ist möglicherweise der fehlenden Analyse der Unterseiten geschuldet; weitere Gründe werden in Abschnitt 5 behandelt.

HOCHSCHULE	google-analytics	doubleclick	adition	facebook
Universität der Künste Berlin			N	
Technische Universität Berlin			N	
Hochschule Karlsruhe Technik und Wirtschaft			N	
Hochschule Fresenius (Idstein)		N		
Universität Hamburg	J		N	
Rheinische Friedrich-Wilhelms-Universität Bonn			N	
Rheinische Fachhochschule Köln	N			
Universität Siegen			N	
Universität Koblenz-Landau	J		N	
Hochschule Magdeburg-Stendal	N			

Tab. 4: Ergebnis der automatischen Überprüfung von Datenschutzerklärungen.
„J": Erwähnung des Trackers in der Datenschutzerklärung,
„N": keine Erwähnung,
„Leeres Feld": keine externe Verbindung registriert.
(Quelle: Eigene Darstellung)

5 DISKUSSION UND AUSBLICK

5.1 Diskussion

Die Auswertung der manuellen Prüfung zeigt, dass drei der deutschen Hochschulen mit den meisten Studierenden gar keine DSE aufweisen und nur vier eine separate DSE besitzen. Die im TMG geforderten Punkte sind in den vorhandenen DSE weitgehend berücksichtigt. Sinnvolle Erweiterung wie z. B. eine Erwähnung der getroffenen Sicherheitsvorkehrungen oder des Mitspracherechts finden keine oder nur selten Erwähnung. Auffällig ist auch der starke Einsatz von Trackern, Social Media und vereinzelt auch Werbung. Leider wird dies in der DSE i.d.R. nicht begründet.

Die automatisierten Auswertungen zeigen, wie stark auf den 207 Hochschulwebseiten in Deutschland die Einbindung von externen Ressourcen genutzt wird. In ~50 % der Fälle fand eine Einbindung einer externen Ressource statt und 30 % der Hochschulen nutzen einen Dienst von Google. 14 % der deutschen Hochschulwebseiten nutzen zur Analyse Google Analytics, wobei in acht Fällen auf die Anonymisierungsoption zum Schutz der Besucher verzichtet wurde. Auf 20 Hochschulwebseiten (~10 %) war keine DSE auffindbar und es konnte nachgewiesen werden, dass diese in mindestens zehn Fällen (~5 %) unvollständig war.

In mindestens 30 Fällen (~15 %) besteht aus diesem Grund ein akuter Handlungsbedarf, eine klare DSE zu erarbeiten oder bestehende Fehler auszubessern. Ebenfalls ist bedenklich, dass auf fast jeder dritten Hochschulwebseite eine Übermittlung der IP-Adresse an Google stattfindet. Hier sollte dringend geprüft werden, ob Einbindungen von Google APIs, Karten, Übersetzungs- oder sonstigen Diensten tatsächlich notwendig sind.

Die Verwendung von Werbediensten, wie Adition, ist auf Webauftritten, insbesondere bei staatlich finanzierten Hochschulen, nur schwer nachvollziehbar und sollte von den Betreibern überdacht werden. Wie Tabelle 4 zeigt, wird der Einsatz von Adition deutlich häufiger verschwiegen als der von Facebook, was u. a. an der stärkeren „Sichtbarkeit" von Facebook liegen kann. Offensichtlich bewerten viele Hochschulen den monetären Anreiz beim Einsatz von Adition höher als den Datenschutz. Die Auswertung zeigte darüber hinaus, dass auf keiner Hauptseite eine Einbindung von Facebook vorgenommen wurde, ohne dies innerhalb der DSE zu erwähnen, obwohl in ca. 40 % der Hochschulwebseiten (Impressum, DSE) eine Aussage zu Facebook enthalten ist. Ein möglicher Grund hierfür könnte das starke Medieninteresse sein, das bei

anderen Trackingdiensten weniger präsent ist. Insbesondere in [ULD (2015a), ULD (2015b)] zeigt sich, wie intensiv das Thema Facebook von Aufsichtsbehörden verfolgt wird. So ist einerseits möglich, dass Facebook vorsichtshalber in die DSE aufgenommen wurde, oder dass die Einbettungen im Laufe der Zeit entfernt wurden.
Die manuelle Analyse einer DSE erlaubt eine deutlich tiefere inhaltliche Prüfung, z. B. die Prüfung der OECD-Kriterien in Tabelle 1, einer kleinen Anzahl von Seiten und ergänzt daher die automatisierte Untersuchung einer großen Zahl von Seiten. Beim Vergleich der Ergebnisse zeigt sich, dass viele Datenschutzerklärungen externe Verbindungen nur unvollständig auflisten oder externe Inhalte ankündigen, die auf den von uns untersuchten Seiten nicht verwendet wurden. Dass Analysewerkzeuge nicht immer auf der Hauptseite eingesetzt werden, zeigte sich z. B. bei http://www.uni-giessen.de/, bei der PIWIK erst auf einer der Unterseiten aktiv wird.
Die Ursachen der identifizierten Missstände sehen wir in folgenden Punkten: (1) der sich durch Gerichtsurteile ständig ändernde rechtliche Rahmen für die DSE, (2) Komplexität und Dynamik der Hochschul-IT, (3) oft unklare Zuständigkeit bei der Erstellung und Pflege der DSE. In allen Fällen könnte eine Hochschul-Muster-DSE helfen (vgl. Abschnitt 5.3). Ein weiteres Problem ist der Umfang des Webauftritts einer Hochschule, der häufig mehrere tausend Seiten umfasst. Die DSE soll möglichst für viele dieser Seiten gelten, was leicht zu einer Über- bzw. Unterdeckung führt.

5.2 Verwandte Arbeiten

In [Wambach (2015)] werden über ein Sandbox-Verfahren detailliertere Untersuchungen von Trackingverfahren auf Webseiten durchgeführt. In [Beltermann (2015a)] ist eine Untersuchung von 35 Behördenwebseiten zu finden, wovon neun Tracking-Verfahren einsetzen, ohne eine Widerspruchsmöglichkeit zu bieten. In [Beltermann (2015b)] können diesbezüglich vereinzelte Stellungnahmen der Behörden betrachtet werden. Dabei wurde insbesondere das Fehlen einer Widerspruchsmöglichkeit innerhalb der DSE gemäß § 15 Abs. 3 TMG von den Webseiten-Betreibern des Bundesverwaltungsgerichtes bestätigt.
Die Platform for Privacy Preferences (P3P) [P3P (2015)] bietet eine formelle Sprache, mit der spezifiziert werden kann, welche Daten von einem Webserver gespeichert werden, wozu diese Daten verwendet werden und wie lange sie gespeichert werden. Dies würde eine automatisierte Auswertung der DSE erheblich vereinfachen. Leider wird P3P kaum eingesetzt, da es von vielen potentiellen Nutzern als zu kompliziert angesehen wird und viele gängige Browser P3P nicht unterstützen.
Die strukturierte Analyse von DSE ist in letzter Zeit auch bei medizinischen Android-Apps durchgeführt worden [Sunyaev et al. (2014), Knorr et al. (2015)].

5.3 Zukünftige Arbeiten

Der letzte Abschnitt dieses Beitrags widmet sich zukünftigen Arbeiten, die die vorliegende Arbeit ergänzen und erweitern. Die vorgestellte Methodik kann z. B. um folgende Aspekte erweitert werden: (1) Berücksichtigung weiterer Technologien wie z. B. Cookies, (2) Untersuchung von anderen Klassen von Webseiten wie z. B. Seiten der öffentlichen Verwaltung, (3) zusätzliche Untersuchung von Unterseiten. Unterseiten können z. B. über sog. Spider wie Scrapy (scrapy.org) in einem ersten Schritt erfasst und dann mittels unseres modifizierten Browsers untersucht werden.
Die Hochschulen könnten stark von einer Hochschul-Muster-DSE profitieren, in der die häufigsten Anwendungen und Inhalte technisch und juristisch aufbereitet enthalten sind. Dieses Muster müsste dann nur noch auf die Hochschulspezifika angepasst bzw. erweitert werden.
Da in dieser Arbeit nur die technische Sichtweise dargestellt wird, wäre auch eine juristische Interpretation notwendig. So ist z. B. offen, ob Verbindungen zu Diensten wie code.jquery.com in der DSE benannt werden müssen.

DANK

Die Arbeit von Tim Wambach wurde durch die VolkswagenStiftung im Projekt „Strukturwandel des Privaten“ gefördert.

REFERENZEN

Beltermann, E. (2015a): Benutzerverfolgung durch staatliche Websites, https://netzpolitik.org/2015/benutzerverfolgung-durch-staatliche-websites/, zuletzt aufgerufen am 29. Juli 2015.

Beltermann, E. (2015b): Benutzerverfolgung durch staatliche Websites: Die Antworten, https://netzpolitik.org/2015/benutzerverfolgung-durch-staatliche-websites-die-antworten/, zuletzt aufgerufen am 29. Juli 2015.

Drachentoeter (2015): Liste der Hochschulen in Deutschland, https://de.wikipedia.org/wiki/Liste_der_Hochschulen_in_Deutschland, zuletzt aufgerufen am 20. Mai 2015.

Ghostery (2015): Add-ons, https://addons.mozilla.org/de/firefox/addon/ghostery/, zuletzt aufgerufen am 19. Juli 2015.

Google (2015): IP Anonymization in Google Analytics, https://support.google.com/analytics/answer/2763052?hl=en, zuletzt aufgerufen am 30. Juli 2015.

Knoke, F. (2015): Datenschützer an Unis: „Wir sind zahnlose Papiertiger", http://www.spiegel.de/unispiegel/studium/datenschuetzer-an-unis-wir-sind-zahnlose-papiertiger-a-585232.html, zuletzt aufgerufen am 19. Juli 2015.

Knorr, K., Aspinall, D. und Wolters, M. (2015): On the Privacy, Security and Safety of Blood Pressure and Diabetes Apps, in: Proc. of IFIP SEC 2015 International Conference on ICT Systems Security and Privacy Protection, May 26-28, Hamburg, 2015, S. 571-584.

Mayer, R. J. und John, C. M. (2012): Third-Party Web Tracking: Policy and Technology, in: Proceedings of the 2012 IEEE Symposium on Security and Privacy, 2012, S.12.

OECD (2015): OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, zuletzt aufgerufen am 6. August 2015.

Overbeck, A. (2014): Trenn oder Zahl!, in: DFN-Infobrief, 04, 2014, S. 5-7.

P3P (2015): Platform for Privacy Preferences (P3P) Project, Enabling smarter Privacy Tools for the Web, http://www.w3.org/P3P/, zuletzt aufgerufen am 1. August 2015.

PyQt (2015): PyQt Whitepaper, http://www.riverbankcomputing.com/static/Docs/PyQt4/pyqt-whitepaper-a4.pdf, zuletzt aufgerufen am 7. Juli 2015

Schneider, M., Enzmann, M. und Stopczynski, M. (2014): Web-Tracking-Report 2014, Darmstadt, 2014.

Sunyaev, A., Dehling, T., Taylor, P.L. und Mandl, K.D. (2014): Availability and quality of mobile health app privacy policies, in: Journal of the American Medical Informatics Association, 2014, S. 28-33.

ULD (2015a): Unabhängiges Landeszentrum für Datenschutz, https://www.datenschutzzentrum.de/facebook/, zuletzt aufgerufen am 27. Juli 2015

ULD (2015b): Unabhängiges Landeszentrum für Datenschutz, https://www.datenschutz-hamburg.de/ihr-recht-auf-datenschutz/internet/facebook.html, zuletzt aufgerufen am 25. Juli 2015

Wambach, T. (2015): Dynamische Trackererkennung im Web durch Sandbox-Verfahren, in: Tagungsband der DACH Security Konferenz 2015.

W3Tech (2015): Web Technology Surveys: Usage of traffic analysis tools for websites, http://w3techs.com/technologies/overview/traffic_analysis/all, zuletzt aufgerufen am 3. August 2015.

Witt, B.C. (2004): Datenschutz an Hochschulen, Ein Praxishandbuch für Deutschland am Beispiel der Universitäten Baden-Württembergs, Ulm, 2004.

ZENDAS (2015): Newsletter Verwaltung, https://www.zendas.de/zendas/newsletter_verwaltung/, zuletzt aufgerufen am 19. Juli 2015.

Analysis of preprocessing and rendering light field videos

Christian Petry

Since light field cameras became available on the consumer market, its versatile functions are more and more known to computer vision communities and photographers. After all, refocusing an image after it was taken is one of the features most wished for in photography. The possibility of refocusing a video after being taken extends this feature to an additional dimension, enabling direct user interaction in videos, which could result in a new form of entertainment and user experience.

This work presents different approaches of preprocessing and rendering light field videos made with a Lytro Illum, a plenoptic camera using microlenses. We compare three differently preprocessed light field videos and reveal the main issues for rendering on consumer hardware. Our results show, that one of the biggest obstacles lies in the transfer of data from light field video files to the main memory of the system. Therefore, the demosaiced and color corrected representation that balances preprocessing and resulting video file size is fastest in rendering light field video files. Rendering a short light field video directly from the main memory allows interaction like refocusing in real time and points out the need for future research on new codecs for light field videos based on non-raw light field images.

Additional Key Words: Light fields, videos, preprocessing, rendering performance

1 INTRODUCTION

An image taken by a conventional camera captures light heading towards a camera on a 2D plane. A light field camera is able to additionally collect spatial and angular light information. This enables applications like refocusing and view perspective shifting [Adelson and Wang (1992), Ng (2006)]. With a robust eye tracking, it could be even possible to adjust focus by simply looking at different areas in the scene. The possibility of view perspective shifting also enables surface reconstruction [Tao et al. (2013)].

The company Raytrix was the first to build and market commercially available plenoptic cameras [Zhang (2010)]. Their main use cases focus on microscopy, the manufacturing and automotive industry. Lytro Inc., founded by Ren Ng in 2006, is a company selling light field cameras on the consumer market. Lytro Inc. has brought out two versions of hand held cameras, which can capture light fields and display them on a desktop pc, as well as on the web [Lytro (2015)]. With the Lytro desktop application the user can not only change conventional settings like color correction, sharpening and denoising, but is also able to refocus, extract depth maps or slightly shift view perspective.

C. Petry
University of Applied Sciences Würzburg-Schweinfurt,
Würzburg, Deutschland,
http://www.fhws.de

Sequential light fields, or light field videos, aren't yet manageable by Lytro's cameras and software. The German company Raytrix however, built and marketed light field video cameras specially made for industrial use cases. Their prices though are unaffordable for end-users in the consumer market [Raytrix (2013)]. Even these cameras can only handle 7 frames per second at a resolution of only 10 megapixel [Raytrix (2015)]. In the year 2012 Raytrix presented a light field video camera at the "GPU Technology Conference" (GTC) [Perwass (2012)]. However, on a scientific point of view, the topic of light field videos with a single microlens camera is still quite unexplored.

In this work we analyze different approaches of preprocessing and rendering light field videos made with the Lytro Illum, a consumer light field video camera. As the Lytro Illum can only take one picture at a time, we analyze the possibilities on stop motion videos. We execute three sequential calculation steps when decoding a Lytro light field image. The first step is the extraction of raw light field images from files created by the camera. Second is demosaicing as well as color correcting the raw image and third is the rearrangement of the microlens image as a stitched image representation, similar to that of a 2D image array. With our framework, these three steps can either be executed beforehand or calculated on demand when rendering the video. After preprocessing it is possible to either save the light fields as consecutive images or as a compressed video on hard drive. In our evaluation, we analyze possibilities, restrictions and performance issues of rendering interactive light field videos based on these different preprocessing steps.

The paper is organized as follows: Section 2 reviews relevant work and the light field concept. In Section 3 we describe the three consecutive preprocessing steps, which we then use in Section 4 to oppose different approaches on rendering interactive light field videos. Finally, Section 5 then adds a conclusion of our results and further thoughts on light field videos.

2 RELATED WORK

The light field, as it was first introduced by A. Gershun in his paper, is defined by a plenoptic function in a static context [Gershun et al. (1939), Adelson and Bergen (1991)]. In light field videos though, the 4D function of a light field reclaims time as an additional parameter from the original plenoptic function. Since the year 1996, a free archive of light fields has been created at Stanford with a Multi-Camera array, a Lego Mindstorms gantry and a light field microscope, and was updated ever since [Levoy and Hanrahan (1996b)].
Several light field video systems have been developed based on camera arrays arranged on a rectangular plane [Chan et al. (2005); Wilburn et al. (2005)]. A hemispherical arranged camera system has been presented by [Akin et al. (2013)]. B. Smith described a stabilization technique for shaky light field videos [Smith et al. (2009)]. All these systems though, use several conventional cameras to capture the scene from different directions and do not include the possibilities of microlenses.

Recently, a light field video captured by a microlens camera, led to a 5-D depth velocity digital filter to enhance moving objects in light field videos [Edussooriya et al. (2015)].

3 DECODING AND DISPLAYING A LYTRO LIGHT FIELD

The Lytro Illum from Lytro Inc. is a camera, that uses microlenses to capture a light field (see figure 1). In total the CMOS sensor is able to capture about 40 megapixels (also called "Megarays") with a main lens that enables 8x optical zoom and 30-250mm equivalent focal length [Lytro (2015)]. In between the main camera lens and the photo sensor is an array of very small lenses. Each lens captures a tiny fraction of the scene viewed by the camera. Due to the main lens in front of the microlens array, the scene is viewed with the same field of view by each microlens. Each raw light field image taken with the Lytro Illum has a resolution of $7728 \cdot 5368$ pixels. With each pixel encoded in 10 bits and several additional meta information, the light fieldfile created by the camera needs approximately 53 MB disk space.

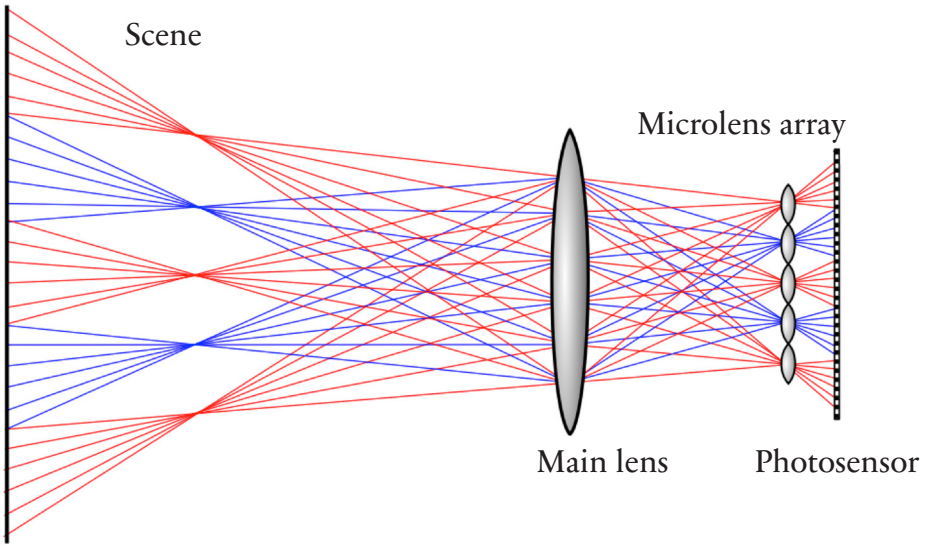


Fig. 1: Capturing a light field with a microlens array and a main lens. Each microlens records a small view of the scene (Source: Own Source)

In this section, three steps of preprocessing a light field are described. These steps are calculated sequentially and can be distributed as follows:

(1) Extracting the raw light field from the container file.
(2) Demosaicing and color correction.
(3) Decoding the microlens array to a convenient representation for rendering.

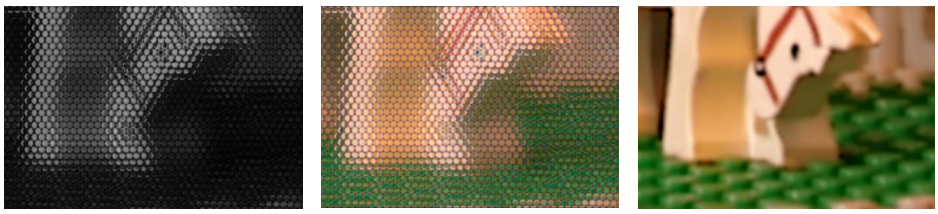
Each of these steps are coded in our software framework and their results can either be preprocessed and saved as image sequences (videos) to a hard drive, or calculated on demand by the GPU inside our glsl shader, when rendering the video frame by frame. The rendered result is always the same, independent of the amount of preprocessing steps. In the end, the result can be displayed as a video, which focus can be interactively manipulated by the viewer. Our software is available in our repository at https://bitbucket.org/cpetry/lfp-reader.

3.1 Extracting the raw light field

After a light field was taken, the Lytro Illum creates a file of type *.lfp, containing different several kinds of information, such as the light field, camera parameters and calibration details. Lytro support employees themselves are directing towards the Light Field Toolbox by Donald

Danserau [Dansereau (2012)] because "...at this point, there doesn't exist a published documentation on the file format". Other approaches to decode the container are outdated or not open source and do not work with the newer version of the Lytro Illum. Still, they are good enough to get a small impression on how Lytro saves light field images [Kucera (2015); Patel (2012)]. For our evaluation though, we created a new framework for decoding light fields.

As mentioned in the meta information inside the *.lfp file format, the raw light field is encoded in a 10 bit per pixel single channel image. Saving this raw image in a PNG lossless format, reduced from 10 to 8 bit per pixel, results in the first step of our decoding process (see figure 2(a)). Reducing the bits per pixel is necessary for displaying the whole color range on a standard computer monitor. As seen in the cropped and zoomed figures 2(a) and 2(b), the light field image is made of a great number of microlenses. In the raw representation, it is still possible to adapt color correction, gamma values and other post processing steps done in conventional photography when rendering from this stage on. It is essential to keep this in a lossless image format because of consequential errors regarding further decoding steps. This results in a grayscale image with 8 bits per pixel.



(a) Extracted raw light field

(b) Demosaiced and color corrected

(c) A completely decoded light field

Fig. 2. Zoomed representation of light field images, showing the first two steps of decoding a light field (Source: Own Source)

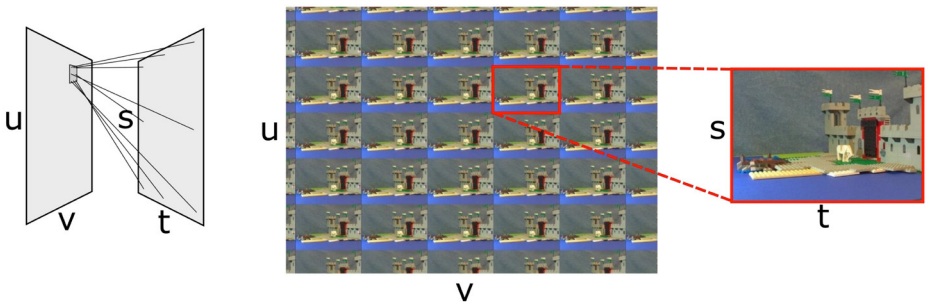


Fig. 3: UVST representation of a light field. One coordinate on the uv plane represents one image on the st plane. Here the uv plane is cropped. This representation is derived from [Levoy and Hanrahan (1996a)]

3.2 Demosaicing and color correction

In the second stage, the raw image has to be demosaiced. Inside the meta information are details about the Bayer color filtering of the raw format [Bayer (1976)]. The current Lytro Illum files are filtered with a "grbg"-filter. That means, that the colors are aligned in blocks of 4 pixels. The upper left and lower right pixel is green, the upper right is blue and the lower left represents a red color value. From these values it is possible to reconstruct coloring while maintaining image resolution, which is called demosaicing. Lytro does not publish any infor-

mation on their demosaicing algorithm of the Lytro desktop application. Therefore, we chose for our analysis a bilinear bayer interpolation. Other interpolation methods could enhance visual quality, but comes with a much higher computational cost [Malvar et al. (2004)].

After demosaicing the image has to be color corrected. Information about white balance, color correction matrix and gamma values are extracted from the meta file sections of the light field file. The demosaiced and color corrected image, as seen in figure 2(b) defines the second step of our decoding process. This file now consists of 24 bits per pixel with 3 color channels.

3.3 Decoding the microlens array for display

The next step is a conversion from microlenses to a 2d image array. The main purpose for this representation is the fast linear interpolation done by the graphics card [Woo et al. (1999)]. This enhances visual quality by smoothing pixel borders in small resolution images. For constructing the convenient representation $\Psi(u, v, s, t)$, (see the cropped image in center of figure 3) [Levoy and Hanrahan (1996a)], several additional information have to be recovered. The microlens center offset position in pixels, the clockwise rotation of the microlenses in degrees, and the lens and the pixel pitch of the microlens-array in meters. The algorithm for decoding the 2D sensor image to a 4D light field is further described by [Dansereau et al. (2013)]. By using this algorithm, the resolution of the light field image increases, because of reusing pixels at the border of each microlens. The resulting image is hereafter called UVST representation, which has $15 \cdot 5$ sub-images of $625 \cdot 433$ pixels each. Every sub-image shows a different view of the same scene. As a summary, the result of each preprocessing step is shown in the table below:

Preprocessing stage	Image size	Bpp	Size per light field
Raw grayscale	$7728 \cdot 5368$	8 bit	40.30 MB
Demosaiced & color corrected	$7728 \cdot 5368$	24 bit	120.90 MB
UVST representation	$9375 \cdot 6495$	24 bit	174.21 MB

Table 1: Summary of preprocessing steps and their characteristics

In our approach, we used the UVST representation as the basis for rendering light fields. All the images on the st plane are displayed as off-axis (sheared) perspective views of the scene (see center image of figure 3) [Levoy and Hanrahan (1996a)]. One pixel (x, y) at a specific coordinate (u, v) is then defined by

$$(x, y)=(s, t)+(u, v)\cdot s_{st}$$

with s_{st} as the size of the st plane, which equals to that of a sub-image with $625 \cdot 433$ pixels each.

3.4 Rendering the light field

Displaying a focused image of the light field, is then achieved by interpolating different shear warped (u, v) sub-images. Each neighboring sub-image inside a given radius of a given (u, v) coordinate gets slightly translated and added to the final image. Depending on the translation different parts of the scene are focused. Higher translation in direction of the center sub-image results in an image focused on objects further away from the initial focal length. A translation away from the center, produces an image focusing objects closer to the camera. The higher

[1] Bpp: bits per pixel.
[2] Sizes are stated as uncompressed images.
[3] The resolution grows due to the algorithm that reuses a one pixel border of each lens [Dansereau et al. 2013].

the chosen radius of sub-images used for this, the blurrier the image gets in parts not focused on. This idea was taken from the aperture viewer of the Stanford light field archive [Vaish and Adams (2008)].

After all preprocessing steps, a focused image of a Lytro Illum in its original state has a resolution of $625 \cdot 433$. This at first seems to be a startlingly low resolution, but can be increased by using super resolution algorithms [Bishop and Favaro (2012)]. This technique can render an image to three or four times the original size. For this work though, we evaluate videos in their original resolution, to not add optional factors influencing performance.

An overview of the here described steps, their amount of preprocessing and left over rendering workload, is visually compared in figure 4.

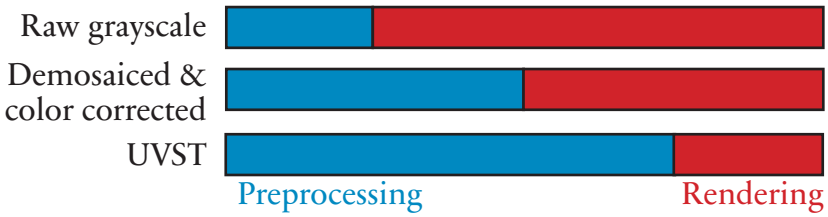


Fig. 4: Amount of preprocessed (blue) and left over rendering workload (red) for each representation described above. This visualization does not represent correct workload dimensions and only shows an overview for better understanding of further analysis (Source: Own Source)

4 FRAMEWORK ANALYSIS AND EXPERIMENTAL RESULTS

In order to render a video on consumer hardware, the frames have to be copied consecutively into the graphic cards memory. One straight forward solution is a pipeline that starts with decoding a frame from a video file stored on a hard drive and copying the result to the main memory. Afterwards the image gets forwarded to the graphic cards memory, where it is then further processed for rendering the interactive video.

For our test purposes, we shot a light field sequence of 116 frames with a Lytro Illum, resulting in a short stop motion video. The duration and thus the frame rate of the video, is determined by the processing speed of the whole system and the preprocessing stage the video is in. In this section, we determine bottlenecks of the processing pipeline to derive future possible enhancements. First we compare the preprocessing steps described above when rendering a video file directly from the hard drive. In the second step we analyze playing back a video completely copied onto the main memory. To get direct rendering workload of the graphics card, the third part analyzes pure rendering performance directly from the memory of the graphics card without any data transfer.

4.1 Comparison on rendering a video file

Playing back video files with a resolution of $1920 \cdot 1080$ (Full HD, 1080p) and even $4096 \cdot 2160$ (4K) does not pose a problem for current hardware. Additionally encoding a video file with H.264 (also called MPEG-4 AVC) or H.265 (also called HEVC) reduces the size of the resulting video file but comes with additional decoding calculations [ITU-T (2014a); ITU-T (2014b)]. These codecs though, do not work with a full resolution Lytro Illum light field. As stated in the re-

commendations, the maximum resolution for H.264 is 4096 · 2304 and for H.265 is 8192 · 4320 pixels. A lossy compression would furthermore change neighboring pixel values, which would result in incorrect colors, when demosaicing frames from the raw grayscale representation. To reduce the size of light field videos anyway, we use HuffYUV, one of the fastest and best performing lossless codecs for decoding and encoding videos [Lab (2007); Hashemian (1995)].

Preprocessing stage	Video file size	FPS	Processed MB/s
Raw grayscale	4.48 GB	4.0 – 4.3	~170 MB/s
Demosaiced & color corrected	6.11 GB	4.3 – 4.6	~242 MB/s
UVST representation	7.41 GB	3.5 – 3.8	~248 MB/s

Table 2: Performance comparison rendering HuffYUV encoded video files of a 116 frames stop motion video

The compressed size, rendering frame rate and processed MB/s are displayed in table 2. Notice that the raw video file does not have the approximate 1/3 file size of the demosaiced file. This is due to the HuffYUV compression algorithm. The video file was played back by a Intel Core i5-4460 CPU @ 3.20Ghz with an ATI Radeon 5850. The file was read from an up to date Solid State Disk resulting in 248 MB/s as maximum processed data achieved. To copy frames as fast as possible asynchronous Pixel Buffer Objects were used.

The fastest representation is the demosaiced & color corrected version of the video. One cause of this result is the lower frame size in comparison to the UVST representation. Approximately only 68 % of pixels of the UVST representation have to be copied. The raw grayscale approach in comparison has much more decoding and texture lookups left to do but still outperforms the UVST representation, due to much less data needed copying.

4.2 Comparison on rendering a preloaded video on the main memory

One of the main bottlenecks of rendering the video, derived from the results of table 2, is the transfer of data from the hard drive to the main memory. To be independent of the hard drive reading speed, the light field video can be rendered directly from the main memory. By reading the complete image sequence into the main memory before starting to render the video, both, video decoding and hard drive speed restrictions, can be avoided. However, this approach is only possible for short sequences or systems with a very high amount of main memory. The stop motion video (116 frames) we used, needs a system with more than 16 GB memory to be able to render it completely, depending on the representation.

Preprocessing stage	RAM usage	FPS	Processed MB/s
Raw grayscale	17.39 GB	8 – 9	~1424.25 MB/s
Demosaiced & color corrected	17.39 GB	15 – 16	~2531.98 MB/s
UVST representation	26.31 GB	20 – 21	~4877.87 MB/s

Table 3: Performance comparison of rendering sequential images residing on the main memory.

Frame rates and actual memory usage are shown in table 3. Now that the restriction of hard drive reading speed is avoided, the UVST representation can be rendered nearly fluently with about 20 FPS. It outperforms in terms of processed MB/s every other representation, but needs the most space on the main memory. The memory needed for all frames is by far higher than in the previous performance comparison. Each image needs now four color channels (RGBA)

and is uncompressed. Saving every frame on RAM as a four color channel image, increases the rendering performance by more than 300% in comparison to saving it as a three color channel image (Demosaiced & color corrected with only RGB: 4-5 frames). This significant difference is the cause of using optimal pixel formats of graphics cards [Nvidia (2007)].

4.3 Comparison on rendering one frame consecutively

When rendering the light field, the amount of preprocessing has a big impact on the frames per second shown on the screen. The more work has been done in advance, the less calculations the GPU has to do for each rendering cycle. Here, we compare rendering only one frame over and over, to get the maximum average rendering frame rate without any data transfer whatsoever. The results are shown in table 4.

Preprocessing stage	Image size	FPS
Raw grayscale	7728 · 5368	8 – 9
Demosaiced & color corrected	7728 · 5368	25 – 26
UVST representation	9375 · 6495	60 – 63

Table 4: Frames per second repeatedly rendering one single light field image

This shows the performance of changing focus of an image on a single light field. Computing a focused image from the raw representation needs too many calculations to be rendered fluently on current hardware. The frame rate remains between 8 and 9 frames per second. The demosaiced & color corrected representation can be rendered in realtime (above 24 FPS). Although the light field image is the largest in the UVST representation, the frame rate achieved clearly dominates. With rendering at 60 FPS a very fast and fluent user interaction can be achieved, which behaves similar to refocusing a scene with a camera before taking a photo. At this frame rate it is possible to reconsider super resolution or other additional visual improvements.

5 CONCLUSION

We presented a framework, which can render interactive light field videos on basis of different preprocessing steps on current standard consumer hardware. In every representation the video can be refocused directly by user input. The representation with the least preprocessing shown here, addressed as raw grayscale, enables additional interactions, such as color correction, adjusting gamma values or blurring and sharpening. These interactions can be compared to post processing of raw images taken with a conventional camera.

The frame rate though, when playing back a light field video file, is not high enough on current consumer hardware to realize an application for real time usage. Neither of the here presented preprocessing steps achieved more than 5 frames per second while rendering. The best performance achieved is that of a demosaiced & color corrected representation with about 4.5 frames per second. Derived from further analysis, one of the main tasks is a fast transfer of frames from a file on the hard drive to the memory of the graphics card.

When rendering directly from main memory, less decoding steps significantly improve rendering performance. The representation just before the final rendering, here called UVST representation, is the fastest and also the biggest in terms of file size, but can be used for near real time (over 20 FPS) interactive rendering when stored completely on the main memory. This requires either huge amount of memory or more advanced and adapted encoding and decoding algorithms.

As light field cameras are still quite new, resolution and the size of microlenses can still vary with newer technologies. A possible coding algorithm, therefore should be independent of several of these parameters. In consideration of previously developed codecs, one solution could be a new encoding algorithm applied to an UVST representation. This would maximize rendering performance and minimize artifacts as well as the file size of the video. Encoding a demosaiced & color corrected representation with an adapted rendering algorithm could pose a worthy alternative, which by nature has less pixel than the UVST representation and thus uses less bits per image.

REFERENCES

Adelson, E. H. and Bergen, J. R. (1991): The plenoptic function and the elements of early vision, in: Landy, M. S. and Movshon, J. A. (Eds.) Computational models of visual processing, Cambridge, MA: MIT Press, 1991, P. 3-20.

Adelson, E. H. and Wang, J. Y. A. (1992): Single lens stereo with a plenoptic camera, in: IEEE transactions on pattern analysis and machine intelligence 14, 2, 1992, P. 99-106.

Akin, A., Cogal, O., Seyid, K., Afshari, H., Schmid, A., and Leblebici, Y. (2013): Hemispherical multiple camera system for high resolution omni-directional light field imaging, in: Emerging and Selected Topics in Circuits and Systems, IEEE Journal on 3, 2, 2013, P. 137-144.

Bayer, B. (1976): US Patent 3,971,065, Color imaging array, http://www.google.de/patents/US3971065, accessed July 6th, 2015.

Bishop, T. E. and Favaro, P. (2012): The light field camera: Extended depth of field, aliasing, and superresolution, in: Pattern Analysis and Machine Intelligence, IEEE Transactions on 34, 5, 2012, P. 972-986.

Chan, S.-C., Ng, K.-T., Gan, Z.-F., Chan, K.-L., and Shum, H.-Y. (2005): The plenoptic video, in: Circuits and Systems for Video Technology, IEEE Transactions on 15, 12, 2005, P. 1650-1659.

Dansereau, D. (2012): Light field toolbox v0.4, http://www.mathworks.com/matlabcentral/fileexchange/49683-light-field-toolbox-v0-4, accessed July 6th, 2015.

Dansereau, D., Pizarro, O., and Williams, S. (2013): Decoding, calibration and rectification for lenselet-based plenoptic cameras, in: Computer Vision and Pattern Recognition (CVPR), 2013, P. 1027-1034.

Edussooriya, C., Dansereau, D., Bruton, L., and Agathoklis, P. (2015): Five-dimensional depth-velocity filtering for enhancing moving objects in light field videos, in: Signal Processing, IEEE Transactions on 63, 8, 2015, P. 2151-2163.

Gershun, A., Moon, P. H., and Timoshenko, G. (1939): The light field, Massachusetts Institute of Technology, 1939.

Hashemian, R. (1995): Memory efficient and high-speed search huffman coding, in: IEEE Transactions on Communications, 43, 10, 1995, P. 2576-2581.

ITU-T. H.264 (2014a): Advanced video coding for generic audiovisual services, https://www.itu.int/rec/T-REC-H.264-201402-I/en, accessed July 6th, 2015.

ITU-T. H.265 (2014b): High efficiency video coding, https://www.itu.int/rec/T-REC-H.265-201504-P/en, accessed July 6th, 2015.

Kucera, J. (2015): Lytro meltdown, http://optics.miloush.net/lytro/, accessed July 6th, 2015.

Lab, C. M. G. (2007): Lossless video codecs comparison '2007, http://compression.ru/video/codec_comparison/pdf/msu_lossless_codecs_comparison_2007_eng.pdf,accessed July 6th, 2015.

Levoy, M. and Hanrahan, P. (1996a): Light field rendering, in: SIGGRAPH '96, Proceedings of the 23rd annual conference on Computer graphics and interactive techniques, New York, 1996, P. 31-42.

Levoy, M. and Hanrahan, P. (1996b): The (old) stanford light field archive, http://graphics.stanford.edu/software/lightpack/lifs.html, accessed July 6th, 2015.

Lytro, I. (2015): Lytro Illum, https://www.lytro.com/illum/, accessed July 6th, 2015.

Malvar, H. S., He, L.-W., and Cutler, R. (2004): High-quality linear interpolation for demosaicing of bayerpatterned color images, in: International Conference of Acoustic, Speech and Signal Processing, Institute of Electrical and Electronics Engineers, Inc, 2004, P. 5-8.

Ng, R. (2006): Digital light field photography. Ph.D. thesis, stanford university.

Nvidia (2007): Fast texture downloads and readbacks using pixel buffer objects in OpenGL, http://http.download.nvidia.com/developer/Papers/2005/Fast_Texture_Transfers/Fast_Texture_Transfers.pdf, accessed July 6th, 2015.

Patel, N. (2012): lfptools, https://github.com/nrpatel/lfptools, accessed July 6th, 2015.

Perwass, C. (2012): Live 3d-video with a lightfield camera, http://on-demand.gputechconf.com/gtc/2012/presentations/S0335-Live-3D-Video-with-a-Lightfield-Camera.pdf, accessed July 6th, 2015.

Raytrix. (2013): 3d light field camera technology, b2b reseller price list, http://www.raytrix.de/tl_files/downloads/products.pdf, accessed July 17th, 2015.

Raytrix. (2015): R42 SERIES, http://www.raytrix.de/produkte/#r42series, accessed July 17th, 2015.

Smith, B., Zhang, L., Jin, H., and Agarwala, A. (2009): Light field video stabilization, in: IEEE 12th International Conference on Computer Vision (ICCV), 2009, P. 341-348.

Tao, M. W., Hadap, S., Malik, J., and Ramamoorthi, R. (2013): Depth from combining defocus and correspondence using light-field cameras, in: IEEE International Conference on Computer Vision (ICCV), 2013, P. 673-680.

Vaish, V. and Adams, A. (2008): The (new) stanford light field archive, http://lightfield.stanford.edu/lfs.html, accessed July 6th, 2015.

Wilburn, B., Joshi, N., Vaish, V., Talvala, E.-V., Antunez, E., Barth, A., Adams, A., Horowitz, M., and Levoy, M. (2005): High performance imaging using large camera arrays, in: ACM Trans. Graph. 24, 3, 2005, P. 765-776.

Woo, M., Neider, J., Davis, T., Shreiner, D., et al. (1999): Open GL programming guide, Boston, 1999.

Zhang, M. P. (2010): The First Plenoptic Camera on the Market, http://petapixel.com/2010/09/23/the-first-plenoptic-camera-on-the-market/, accessed July 6th, 2015.

IMPRESSUM

Herausgeber und V. i. S. d. P.
Prof. Dr. Robert Grebner
Hochschule für angewandte Wissenschaften
Würzburg-Schweinfurt

Münzstraße 12
97070 Würzburg
Telefon +49 931 3511-6002
Fax +49 931 3511-6044

Ignaz-Schön-Straße 11
97421 Schweinfurt
Telefon +49 9721 940-602
Fax +49 9721 940-620

Ansprechpartner
Vizepräsident Prof. Dr. Jürgen Hartmann
Prof. Dr. Karsten Huffstadt
Birgit Weigand
scj@fhws.de

Aus Gründen der besseren Lesbarkeit wurde auf die zusätzliche Formulierung der weiblichen Form verzichtet. Wir möchten deshalb darauf hinweisen, dass die ausschließliche Verwendung der männlichen Form explizit als geschlechtsunabhängig verstanden werden soll.

ISSN 2196-6095

Bibliografische Information der Deutschen Bibliothek:
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über *http://dnb.ddb.de* abrufbar.