Hubert A. Jäger
Ralf O. G. Rieken *Hrsg.*

Manipulationssichere Cloud-Infrastrukturen

Nachhaltige Digitalisierung durch Sealed Cloud Security

Springer Vieweg

Manipulationssichere Cloud-Infrastrukturen

Hubert A. Jäger • Ralf O. G. Rieken
Hrsg.

Manipulationssichere Cloud-Infrastrukturen

Nachhaltige Digitalisierung durch Sealed Cloud Security

Springer Vieweg

Hrsg.
Hubert A. Jäger
Uniscon GmbH
München, Deutschland

Ralf O. G. Rieken
Uniscon GmbH
München, Deutschland

ISBN 978-3-658-31848-2 ISBN 978-3-658-31849-9 (eBook)
https://doi.org/10.1007/978-3-658-31849-9

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg
© Der/die Herausgeber bzw. der/die Autor(en), exklusiv lizenziert durch Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020
Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.
Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.
Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung: Sybille Thelen
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Geleitwort von Prof. Dr.-Ing. Axel H. Stepken

Vorsitzender des Vorstandes der TÜV SÜD Aktiengesellschaft

Die Digitalisierung wirtschaftlicher Ökosysteme führt zu wesentlich beschleunigter Interaktion zwischen Menschen, zwischen Menschen und Maschinen und zwischen Maschinen. Sie führt zu einer informationellen Integration ganzer Wertschöpfungsketten und gesteigertem Komfort im Alltag. Technisch wird diese Interaktion und Integration durch Cloud-Computing ermöglicht und getragen.

Diese Vernetzung und der damit verbundene Wandel bergen ungemein große Chancen, sowohl für jedes Individuum, als auch für die Gesellschaft als Ganzes. Gestern noch komplizierte und aufwändige Vorhaben sind heute bereits einfach umsetzbar und morgen schon für große Gesellschaftskreise nutzbar. Zum einen stärken die durch die Digitalisierung möglichen Effizienzsteigerungen die Wettbewerbsfähigkeit der Wirtschaft, zum anderen gibt die sehr viel einfachere Verarbeitung von Information einen breiten Raum für zahlreiche neue Geschäftsmodelle. Geschäftserfolg ohne Digitalisierung ist heute nahezu undenkbar.

Diesen formidablen Chancen stehen aber auch zunehmende, nicht zu unterschätzende Risiken entgegen:

- Big-Data-Analysen und künstliche Intelligenz liefern die Grundlage für wichtige Entscheidungen. Oft werden dabei statistische Zusammenhänge festgestellt, deren kausale Abhängigkeit jedoch zunächst unklar bleiben. Es gilt darauf zu achten, dass bei datenbasierten Entscheidungen statistische Korrelation nicht mit erwiesener Kausalität verwechselt werden.
- Die Verbreitung von Information erfolgt digital auf intendierte oder nicht-intendierte Weise so einfach und häufig, dass der Datenschutz für die Gewährleistung der Würde und Freiheit aller betroffenen Personen mehr und mehr an Bedeutung gewinnen wird.
- Für die so genannten „kritischen“ Infrastrukturen, also für die Versorgung der gesellschaftlich wichtigen Einrichtungen, entstehen durch die Digitalisierung zahlreiche neue Angriffsflächen. Die Funktion technischer Anlagen kann durch Angreifer sabotiert oder verändert werden, sodass Gefährdungen für Leib und Leben vieler Menschen

entstehen können. Die zunehmende Abhängigkeit der Systeme untereinander stellt eine zusätzliche Bedrohung dar.

- Eine der Begleiterscheinungen der Datenökonomie ist die zunehmende Bedeutung der Wahrung von Geschäftsgeheimnissen für den Erfolg und Bestand eines Unternehmens. Die Umsetzung der EU-„Trade Secret Directive" wird weitere Anstrengungen im Bereich der IT-Sicherheit in Unternehmen erfordern.
- Viele neue Geschäftsmodelle des „Internet of Things" (IoT) bedingen, dass für die Ermittlung von wichtigen Kenngrößen, den so genannten „Key Performance Indicators" (KPI), genügend Daten für eine statistisch stabile Auswertung vorhanden sind. Oft kann diese Datenmenge nur durch eine Datenauswertung über Unternehmensgrenzen hinweg gewonnen werden. Damit der Wettbewerb zwischen den Unternehmen durch etwaige Datenlecks bei deren Verarbeitung nicht unlauter verzerrt werden kann, ist eine ausreichende Anonymisierung der Daten im Sinne des für die Wirtschaftswelt notwendigen Vertrauens und des Kartellrechts erforderlich.

All diesen durch die Digitalisierung erhöhten Risiken, deren Liste sicher noch unvollständig ist, liegt das Problem der Cybersicherheit zu Grunde. Die Sicherheit der informationstechnischen Systeme, einschließlich und insbesondere der Cloud, wird zum Dreh- und Angelpunkt einer zuverlässigen, nachhaltigen und sicheren Wirtschaft.

Es ist den beiden Gründern der Uniscon GmbH, den Mitherausgebern und Hauptautoren dieses Werkes, den Herren Dr. Hubert Jäger und Dr. Ralf Rieken zu verdanken, dass die als „Sealed Cloud" bezeichnete Technologie erfolgreich entwickelt wurde. Mit ihrer Hilfe lassen sich die genannten Risiken auf ein für die Gesellschaft erträgliches Maß reduzieren.

Die Technischen Überwachungsvereine (TÜV) sehen es als ihre zentrale Aufgabe, die negativen Auswirkungen der technischen Entwicklungen auf das Leben der Menschen zu minimieren. Mit der Digitalisierung erweitert sich dieser Aufgabenbereich auf die informationstechnischen Systeme und bezieht sich dort insbesondere auf die Cybersicherheit.

Die Aufgaben der Überwachung von Technik können jedoch nur auf der Grundlage einer umfassenden Bildung und einem sehr ausgeprägten Know-How in den sich sehr schnell entwickelnden Feldern wahrgenommen werden. Daher können sich die Unternehmen der TÜV nicht nur auf periodische Inspektionen und Zertifizierungen beschränken, sondern müssen sowohl an der Analyse von Problemen als auch an der Entwicklung von ausreichend sicheren Lösungen aktiv beteiligt sein. Dies schließt auch eine kontinuierliche Überwachung von relevanten Systemen durch automatische Überwachungsagenten mit ein, wie es durch die Sealed Cloud beispielhaft umgesetzt wird. Seit der Gründung der TÜV vor über 150 Jahren entsprechen präventive Lösung von sicherheitsrelevanten Problemen der Tradition dieser Institutionen. Im Informationszeitalter steigt der Bedarf an technischer Überwachung dramatisch an, und entsprechend engagiert sich der TÜV verstärkt in den Bereichen Cybersicherheit und digitale Dienste. Daher ist es nur konsequent, die Aktivitäten der Uniscon GmbH in das Portfolio der TÜV SÜD Gruppe zu integrieren.

Das vorliegende Werk sei allen Lesern empfohlen, die in Wirtschaft, öffentlicher Verwaltung oder Forschung und Lehre Verantwortung für eine nachhaltige Gestaltung der informationstechnischen Systeme tragen.

München Axel Stepken
im April 2019

Vorwort

Die Digitalisierung ist ohne sicheres Cloud-Computing nicht denkbar. Für den modernen Menschen ist die Nutzung des Internets zur täglichen Selbstverständlichkeit geworden. Nicht nur verbindet er sich mit Hilfe von PCs, Tablets oder Smart Phones mit Mitmenschen und Webseiten, mit denen er Informationen austauscht, auch ist er gewohnt, dass Geräte, Maschinen, Kameras und Sensoren im Haushalt oder der Arbeitsumgebung jederzeit an das Internet angeschlossen sind. Diese interagieren automatisch miteinander und ermöglichen dadurch neue Funktionen und Dienstleistungen. Jedoch werden die Signale nur in seltenen Fällen direkt zwischen den Geräten und Maschinen ausgetauscht. In der Regel koordinieren zentrale Server den Fluss der Daten.

Diese zentralen Server werden „Cloud“ genannt, da der Nutzer nur „wolkig“ ungenau weiß, wo die Server stehen und was mit den Daten in diesen Servern genau passiert. Dieser mangelnden Transparenz ist der Nutzer nicht nur bezüglich der Cloud ausgesetzt. Er kann auch nicht unmittelbar erkennen, was die vielfältige Software seiner eigenen Geräte und der Sensoren in seiner Umgebung genau bewirkt. Der Cloud gegenüber aber ist das Unbehagen am größten. Je wichtiger die Vertraulichkeit der Daten ist, um so mehr sind die Nutzer auf Transparenz und nachvollziehbare Sicherheit der Daten angewiesen.

Bevor in die Struktur des Buches eingeführt wird, sei die Entstehungsgeschichte der manipulationssicheren Sealed Cloud aus der persönlichen Sicht der Herausgeber eingegangen: Der Grundstein für die Entwicklung der Sealed Cloud wurde im Herbst 2007 gelegt, als sich Arnold Monitzer, Hubert Jäger und Ralf Rieken nach mehreren Jahren in den USA und in den verschiedensten Positionen bei unterschiedlichen Unternehmen wieder in München zusammenfanden. Alle drei trieb das unternehmerische Interesse. Doch was sollte es werden? Der Aufbau eines neuen Geschäfts sollte systematisch erfolgen. Also stellte man eine Liste mit Anforderungen und grundlegenden Ideen zusammen:

1. Es sollte ein Softwareunternehmen werden, da hier die größten Möglichkeiten gesehen wurden. Außerdem gab es in diesem Umfeld die meisten Erfahrungen.
2. Als Geschäftsmodell wurde Software as a Service wegen der kontinuierlichen Einnahmen nach einem Mietmodell als attraktiv bewertet.

3. Die noch zu entwickelnde Lösung sollte einen großen Bedarf adressieren, für den Europa den Lead-Markt repräsentiert. Auf diese Weise sollte ein ausreichend großer Vorsprung erarbeitet werden, bis die üblicherweise wesentlich besser finanzierten US-Firmen den Markt entdecken und zu Wettbewerbern werden.
4. Da die Gründer nach vielen Stationen nicht mehr umziehen wollten, sollte das Angebot sehr gut mit den Kostenstrukturen eines deutschen Standorts vereinbar sein und nicht leicht in Billiglohnländer verschoben werden können.
5. Und damit das Unternehmen neben den geschäftlichen Themen auch inhaltlich anspruchsvolle Themen adressiert und somit Ingenieuren Spaß macht, sollten möglichst grundlegende Probleme gelöst werden müssen.

Nach Aufstellung dieser Liste begann ein langer Prozess des Suchens, des Analysierens, des Bewertens von vielen Ideen, die zwar interessant aber geschäftlich nicht attraktiv waren. Es kristallisierte sich jedoch generell das Thema „Vertrauen im Internet“ als Kernthema heraus – Vertrauen in privaten und geschäftlichen Beziehungen, Vertrauen bei der Nutzung von Dienstangeboten, Vertrauen bei Transaktionen, etc.

Vertrauen und Datenschutz spielen in der europäischen Kultur und Gesellschaft eine wesentlich größere Rolle als in den USA. Vertrauen ist auch schwer in Billiglohnländer zu verlagern. Für Angebote mit großer Vertrauenswürdigkeit kann eine höhere Zahlungsbereitschaft angenommen werden.

Wenn man vertrauenserzeugende Dienste anbieten möchte, dann stellt sich sofort die Frage nach dem Vertrauen der Nutzer in den Anbieter der Dienste: Warum sollten die Nutzer dem Anbieter vertrauen? Bei großen Unternehmen mit einer starken, bekannten Marke gibt es im Allgemeinen ein Vertrauen in die Marke und damit einhergehend ein entsprechendes Vertrauen in den Schutz von Daten und Anwendungen bei diesen Unternehmen. Diese Situation ist das Ergebnis eines oft sehr langen Prozesses. Ein neu gegründetes Unternehmen mit geringem Bekanntheitsgrad beginnt hier bei Null. Für die drei Gründer war klar, dass eine für den geschäftlichen Erfolg notwendige beschleunigte Vertrauensbildung nicht durch eine Marke sondern nur durch eine innovative technische Lösung erreicht werden kann, die einen besonders hohen Datenschutz durch rein technische Mittel und Maßnahmen gewährleistet. Eine rein technische Lösung bietet eine Reihe von Vorteilen bezüglich Schutz und Vertrauensbildung:

1. Technische Maßnahmen lassen sich durch unabhängige Experten überprüfen.
2. Technische Lösungen arbeiten bei korrekter Realisierung kontinuierlich und zuverlässig, während jede Abhängigkeit von menschlichen Akteuren immer wieder zu Risiken führt.
3. Technisch abgesicherte Infrastrukturen können manipulationssicher gestaltet werden, d. h. der Aufbau und die Inbetriebnahme der Rechenzentren sind so beschaffen, dass die Sicherheit nur durch ein arglistiges Zusammenwirken von mehren Personen aus unterschiedlichen Organisationen (engl. „cross-organizational malicious coalition“) verletzt werden könnte.

Ausgehend von diesen Überlegungen formulierten die Gründer eine wesentliche Grundregel zur Realisierung der Lösung:

> Die Eigentümer, Besitzer und Betreiber des Systems müssen jederzeit durch rein technische Mittel und Maßnahmen manipulationssicher von jeglichem Zugriff auf Daten und Anwendungen der Nutzer ausgeschlossen sein.

Die konsequente Befolgung dieser Regel bei der Entwicklung des Sicherheitssystems für die geplante Cloud-Lösung führte dann im Resultat zum Konzept der „Sealed Cloud“ bzw. des „Sealed Computing“ oder „Confidential Computing“.

Es stellte sich heraus, dass mit diesem Konzept der notwendige Durchbruch für die Sicherheit und den Datenschutz bei Big Data, künstlicher Intelligenz und digitaler Überwachung erreicht werden kann, der für die Entwicklung der Datenökonomie so wichtig ist. Neben der Anwendung der Technologie für Cloud-Computing bietet die Versiegelung viele weitere attraktive Einsatzbereiche, wie zum Beispiel das „Internet der Dinge“, auf die in diesem Buch ebenfalls eingegangen wird.

Im Teil I dieses Buches werden die Probleme fehlender Sicherheit und fehlenden Datenschutzes aus rechtlicher, ökonomischer und technischer Sicht analysiert und Anforderungen formuliert. Als Lösung für das Dilemma, dass man entweder auf Cloud-Computing verzichten, oder den Betreibern und ihren Zulieferern nahezu blind vertrauen muss, wird das Prinzip der „Sealed Cloud“ vorgestellt.

Teil II erörtert grundsätzliche Voraussetzungen und Optionen für Sicherheit, taucht tief in eine technische Analyse der Sicherheit im Cloud-Computing ein und zeigt die Charakteristika der Sealed Cloud quantitativ auf.

Teil III widmet sich ausgewählten Anwendungsbeispielen, die das Potential sicheren Cloud-Computings aufleuchten lassen.

Hinweis an den eiligen Leser:
Am Ende eines jeden thematischen Abschnitts steht in diesem Buch in einer grauen Box ein Fazit. Beschränkt sich der eilige Leser darauf, so erhält er doch einen Überblick zu den in diesem Buch behandelten Themen.

München,
im März 2019

Hubert Jäger und Ralf Rieken

Inhaltsverzeichnis

Über die Herausgeber

Dr. Hubert A. Jäger studierte Elektro- und Nachrichtentechnik an der Universität Stuttgart und der ETH Zürich sowie Ökonomie am INSEAD, Fontainebleau, und der Steinbeis-Hochschule Berlin. Er war in leitenden Funktionen der Produktentwicklung, des Innovations- und Produktmanagements sowie der Geschäftsentwicklung bei großen High-Tech-Unternehmen in Deutschland und den USA tätig, bevor er zusammen mit Ralf Rieken die Uniscon GmbH gründete. Er ist visionärer Unternehmer und leidenschaftlicher Ingenieur und in dieser Rolle Erfinder und Autor zahlreicher Patente.

Dr. Ralf O. G. Rieken studierte Informationstechnik und sammelte in der Netzinfrastruktur- und IT-Industrie umfassende Erfahrungen in Produktentwicklung und Geschäftsstrategie. Der Unternehmer hatte verschiedene verantwortliche Positionen bei großen IT- und Netzlieferanten inne und lebte viele Jahre in den USA, wo er bis Ende 2007 als CEO eine Softwarefirma im Silicon Valley leitete. Wieder in Deutschland, baute er gemeinsam mit Hubert Jäger die Uniscon GmbH zu einem technisch führenden und heute schnell wachsenden Unternehmen für hochsichere Cloud-Lösungen auf.

Über die Autoren

Lamya Abdullah Lamya Abdullah schloss 2008 an der University of Jordan, Jordanien, mit einem Bachelor in Computer Science ab. Ihren Master erwarb sie 2012 mit der Vertiefung im Bereich Computer- und Netzsicherheit an der selben Hochschule. Nach sechs Jahren Berufstätigkeit als Software-Entwicklerin nahm sie erneut Studien an der Birmingham City University im Vereinigten Königreich auf und sammelte Erfahrungen als Assistentin in der Lehre. Im Rahmen des Europäischen Marie Skłodowska-Curie Forschungs- und Trainingsnetzwerks „Privacy & Usability“ stieß sie zum Team der Uniscon GmbH und verfolgte dort in den Jahren 2016 bis 2019 mit Arbeiten an den Produkten iDGARD und Sealed Freeze ihr Doktorstudium, das sie nun an der Friedrich-Alexander-Universität in Erlangen und Nürnberg zum Thema Privatheit und Vertrauenswürdigkeit im Cloud-Computing vervollständigt.

Sibi Antony Sibi Antony graduierte 2006 an der Kerala University, Indien in Computer Science. Erste Erfahrungen mit hochverfügbaren und fehlertoleranten Kommunikationssystemen sammelte er an den Hewlett-Packard OpenCall Communications Laboratories, Bangalore, Indien. Zum Master-Studium der Informatik wechselte er an die Technische Universität München. Er erwarb seinen Mastertitel 2013 mit Vertiefungen zu „Distributed Systems“ und „Machine Learning“. Seitdem arbeitet er als Senior Software Developer bei der Uniscon GmbH und leistete entscheidende Beiträge zum Entwurf und der Entwicklung von iDGARD, Sealed Freeze und Sealed Platform.

Ansgar Dirkmann Ansgar Dirkmann studierte Physik an den Universitäten Freiburg i. Br. und Toulouse, Frankreich. Er vertiefte im Bereich Biophysik und graduierte als Dipl. Phys. im Jahr 1986. Seinen MBA erwarb er 1991 am Europäischen Institut für Unternehmenführung (INSEAD) in Fontainebleau, Frankreich. Dirkmann bekleidete verschiedene leitende Positionen im Vertrieb und Produktmarketing bei der Siemens AG und der Nokia-Siemens Networks GmbH & Co. KG. Sein fachlicher Hintergrund liegt in den Bereichen Telekommunikation und Smart Grids. Dirkmann wechselte 2013 als Vertriebsleiter zur Uniscon GmbH und verhilft dem jungen Unternehmen zu seinem starken Wachstum des Geschäfts bis heute.

Edmund Ernst Nach dem Studium der Elektrotechnik, Nachrichtentechnik und Kybernetik an der TU München und einem kurzen Ausflug in die Psychoakustik fokussierte sich Edmund Ernst auf die Entwicklung hochperformanter Mikroprozessor- und Speichersysteme bei der Siemens AG. Im Laufe der Jahre verbreiterte er seine Expertise auf Themen wie ASICs, FPGAs, DSPs, Koppelfelder, Taktsysteme, embedded SW, EMC sowie Design mechanischer Komponenten. Nach zahlreichen Stationen im Bereich Entwicklung, Projekt- und Produktmanagement war er zuletzt bis zu seinem Ausscheiden bei der Siemens AG im Jahre 2011 verantwortlich für die weltweite Entwicklung der elektronischen und mechanischen Komponenten der Kommunikationsysteme und -endgeräte für Unternehmenskunden. Danach wechselte er zur Uniscon GmbH und ist dort verantwortlich für das Design, den Aufbau, den operativen Betrieb und die Datensicherheit der Uniscon-Systeme sowie der von Uniscon an Kunden gelieferten Customer Premise Solution Systeme.

Jaro Fietz Jaro Fietz studierte Informatik an der Technischen Universität München und erwarb seinen Mastertitel 2020. Im Rahmen seiner Masterarbeit spezifizierte er das Sealed Trust Anchor Network und führte die entsprechende Sicherheitsanalyse durch. Seit 2014 arbeitet Herr Fietz bei Uniscon, insbesondere in den Bereichen der Entwicklung, Konzipierung und IT-Sicherheit.

Lars Iclodean Lars Iclodean studierte Mathematik an der Technischen Universität München. Er vertiefte sich in Numerischer Mathematik und graduierte 2015 mit einem Algorithmus über Attraktoren in dynamischen Systemen (Dipl.-Math. Univ.). Iclodean baute bei der Uniscon GmbH die Qualitätssicherung des SaaS-Angebotes iDGARD systematisch auf und betreut seit Jahren an der Telefon-Hotline die wichtigsten Kunden (VIP-Support). Heute verantwortet er den gesamten Kundenservice der Uniscon GmbH.

Dr. Hubert A. Jäger Hubert Jäger ist Experte für Invention, Innovation und Cloud-Sicherheit. Er war Geschäftsführer, Mitgründer und CTO der Uniscon GmbH. Zuvor bekleidete er leitende Funktionen bei der Siemens Enterprise Communications GmbH & Co. KG, der Optisphere Inc. und der Siemens AG. Als Student war er bereits für den Halbleiterpionier Siliconix Inc. in Santa Clara, Kalifornien, mitten im Silicon Valley tätig. Er studierte Elektrotechnik an der Universität Stuttgart (Dipl.-Ing.) und Nachrichtentechnik an der Eidgenössischen Technischen Hochschule, ETH-Zürich (Dipl.-Ing. NDS und Dr. sc. techn.) sowie Ökonomie und Business Administration am INSEAD, Fontainebleau, sowie an der Steinbeis Hochschule Berlin (BA). Erfahrungen sammelte Jäger im Halbleiterumfeld, der Hochfrequenz- und Antennentechnik, der faseroptischen Nachrichtenübertragung, insbesondere im Bereich Ultra-High-Speed Übertragungsnetzen (Wellenlängenmultiplex), der Standardisierung von WLAN-Multi-Hop-Netzen (IEEE 802.11s), dem „Disruptiven“ Innovationsmanagement (Innovation Board Office), des Managements der Softwareentwicklung an global verteilten Standorten und der Unternehmensgründung & -entwicklung. Er ist Autor zahlreicher Patente zu Erfindungen aus

unterschiedlichen Bereichen der IT und Telekommunikation, insbesondere zur Cloud-Sicherheit.

Daniel Kammerer Daniel Kammerer studierte Betriebswirtschaft (Dipl.-Betriebswirt) mit Schwerpunkt Marketing an der Technischen Hochschule Nürnberg Georg Simon Ohm – University of Applied Sciences. Während seines beruflichen Engagements im Bereich Marketing war er u. a. als Dozent für Marketing & Kommunikation sowie als Head of Marketing tätig und ist heute Spezialist für Online Performance Marketing.

Christos Karatzas Christos Karatzas studierte „Computer Science" an der Universität von Piraeus, Griechenland bis 2001 und erhielt den Master-Titel in „Information Systems" von der „Athens Economic University" (AUEB) 2003. Er arbeitete mehr als 16 Jahre als Software-Entwickler in verschiedenen Unternehmen der Bank-, Telekommunikations-, Spiele-, Sicherheits- und Medizintechnikbranche. Er vertiefte sich u. a. in den Bereichen der Architektur und Implementierung von verteilten Enterprise-Systemen und integrierten Lösungsarchitekturen. Seit 2017 ist er maßgeblich mit der Gestaltung der Architektur der Sealed-Platform beschäftigt.

Jaymin Modi Jaymin Modi studierte Elekto- und Nachrichtentechnik am Nirma Institute of Technology, Ahmedabad, Indien und graduierte dort 2005 mit dem „Bachelor of Engineering in Electronics and Communication". Für das Masterstudium wechselte er an die Fachhochschule Rosenheim, an der er 2008 mit dem „Master of Engineering in Elektro- und Informationstechnik" abschloss. Modi arbeitete für die GebeCom GmbH, München als Software-Ingenieur an einem Videotelefoniesystem basierend auf den IP-Telefonen der Reihe „OpenStage" der Siemens AG. Im Jahr 2010 begann er seine Tätigkeit als Software- und Systemingenieur bei der Uniscon GmbH, ebenfalls in München. Er trug entscheidend zum Entwurf und der Entwicklung der Systemarchitektur sowie der Anwendung iDGARD und der Sealed Cloud-Infrastruktur bei.

Arnold Monitzer Arnold Monitzer studierte Nachrichtentechnik an der Technischen Universität in Wien (Dipl.-Ing.). Er war bei der Siemens AG u. a. verantwortlich für das Systemdesign eines photonischen Crossconnects und „Managed Optical Distribution Frames" (MODIF), Performance-Analysen für medizintechnisch genutzte Rechenzentren in den U.S.A., sowie Projektleitung im Bereich Internettelefonie. Er ist einer der drei Mitgründer der Uniscon GmbH und verantwortet dort die Bereiche Fehleranalyse und Qualitätssicherung in der Softwareentwicklung.

Dau Khiem Nguyen Dau Khiem Nguyen (Dipl.-Ing Univ. und Dipl.-Inf. Univ.) studierte Lebensmitteltechnologie an der Technischen Universität Hanoi und Informatik an der Technischen Universität München. Er ist seit 2009 in der Softwareentwicklung der Uniscon GmbH tätig und leistete entscheidende Beiträge zur Business Logic und Sicherheitsarchitektur des Sealed-Cloud-Dienstes „iDGARD".

Dr.-Ing. habil. Ralf O. G. Rieken ist Mitbegründer und COO der Uniscon GmbH. Vor Uniscon war er viele Jahre in leitenden Positionen in der Netzinfrastruktur- und in der

IT-Industrie tätig in den Bereichen Softwareentwicklung, Technologie- und Geschäftsstrategie. Der Unternehmer lebte außerdem viele Jahre in den USA, wo er nach Positionen als Leiter Softwareentwicklung und Geschäftsstrategie bei einer Tochter der Siemens AG an der Ostküste dann in das Silicon Valley umsiedelte und dort bis Ende 2007 als CEO eine Softwarefirma leitete, die Softwareplattformen für Rechenzentren entwickelte. Nach seiner Rückkehr nach München übernahm er bei Fujitsu die Verantwortung für eine IT-Infrastruktur Consulting Organisation. Die aus den USA mitgebrachte Idee des Cloud-Computing war einer der Treiber für die Gründung der Uniscon GmbH, die er dann gemeinsam mit Hubert Jäger zu einem technisch führenden und heute schnell wachsenden Unternehmen für hochsichere Cloud-Lösungen entwickelt hat.

Claudia Seidl Claudia Seidl arbeitete nach ihrem Studium der Philosophie, Geschichte und Soziologie an der Alma Mater Wien als Innenpolitik-Redakteurin in der Austria Presse Agentur eG. Sie verantwortete mehrere Fachmagazine und Bücher. Von 2000 bis 2008 gründete und leitete sie das dreisprachige Kundenmagazin Compás von Volkswagen de Mexico AG. 2010 wechselte sie zur Uniscon GmbH. Sie baute dort die Content-Abteilung auf und leitete diese bis 2020.

Franz Stark Franz Stark arbeitete nach seiner Ausbildung zum Nachrichtentechniker von 1968 bis 2007 bei der Siemens AG in München, zuerst als Prüfsoftware-Entwickler, dann in der Qualitätssicherung und später als Projektleiter Entwicklung von Telekommunikationssystemen und Endgeräten. 2007 bis 2009 wechselte er als Leiter der Fertigungstechnologie in den Telekommunikations-Fertigungsbetrieb der Siemens AG nach Leipzig, wo er auch zusätzlich für die Qualitätssicherung der Fertigung verantwortlich war. 2010 wechselte er zur Uniscon GmbH mit Sitz in München mit dem Tätigkeitsschwerpunkt Hardware-Selektion und -Support.

Wilhelm Würmseer Wilhelm Würmseer studierte von 2005 bis 2012 Sprach- und Literaturwissenschaften an der Ludwig Maximilian Universität München. Seit 2017 ist er Teil der Unternehmenskommunikation der Münchner TÜV SÜD-Tochter Uniscon GmbH. Nebenbei ist er als Blogger und freier Autor tätig.

Danksagung

Die Herausgeber und Autoren dieses Buches wollen sich bedanken: Als erstes gebührt der Dank den betroffenen Familien, ohne deren Rücksicht und Unterstützung ein solches Buch gar nicht entstehen kann. Als zweites gilt der Dank den Ratgebern und „Business Angels“ der Uniscon GmbH. Die Entwicklung und Markteinführung der Sealed-Cloud-Technologie sowie die Gewinnung der Erkenntnisse, die dieses Buch maßgeblich prägen, wäre nicht möglich gewesen ohne das unternehmerische Gespür, den Mut und das in die Gründer gesetzte Vertrauen dieser Personen. Dieser Personenkreis unterstützte die Uniscon GmbH kontinuierlich mit signifikantem Kapital und inhaltlich wichtigen Ratschlägen und vor allem in wichtigen Momenten der Unternehmensentwicklung mit visionären Ermutigungen. Namentlich danken wir den Herren Dr. Siegfried Bocionek, Klaus-Ulrich Bösner, Ansgar Dirkmann, Christoph Eibl, Edmund Ernst, Stephan Hauber, Thorsten Heins, Prof. Dr. Rolf Hofstetter, Herbert Kauffmann, Adolf Leonhardt, Dr. Gustav Mühlschlegel, Dr. Hans-Christian Perle, Lothar Pauly, Prof. Dr. Julius Reiter, Stefan Schulte, Hendrik Schulze und Christoph Spöri. Als dritte Personengruppe, der wir zu Dank verpflichtet sind, sind die Mitarbeiter der Uniscon GmbH zu erwähnen. Die meisten in diesem Buch vermittelten Erkenntnisse wurden während der Zeit des Aufbaus der Uniscon GmbH in der gemeinsamen Arbeit an der Gestaltung einer Möglichkeit für hochsicheres Cloud-Computing gewonnen. Dies wäre ohne das hervorragende Engagement der Mitarbeiter nicht gelungen, und viele der Mitarbeiter sind auch gleichzeitig Autoren dieses Werkes. Schließlich denken wir sehr gerne an die gemeinsame Arbeit mit Kunden sowie akademischen und industriellen Partnern und sagen ebenfalls ganz herzlichen Dank!

Teil I

Einführung in das Sealed Cloud-Computing

Herkömmlich gestaltete zentrale Server-Infrastrukturen werden von Personal der Rechenzentren und Software-Administratoren betreut, denen seitens der Anwender ein hohes Maß an Vertrauen entgegen gebracht wird. Dies geschieht nicht in erster Linie, weil diese an sich besonders vertrauenswürdig wären, sondern weil bei konventionellen Systemen keine Möglichkeit besteht, die privilegierten Zugriffsmöglichkeiten dieses Personenkreises technisch auszuschließen. Es musste bislang einfach den Administratoren vertraut werden.

Durch sorgfältig umgesetzte Rollen- und Berechtigungskonzepte kann zwar die Wahrscheinlichkeit unbefugter Zugriffe und möglicher Missbrauch der Daten durch Insider auf personenbezogene oder anderweitig sensible Daten reduziert werden, jedoch nicht auf ein Maß, das einem hohen oder sehr hohen Schutzbedarf von Verarbeitungsvorgängen entspräche.

In diesem Teil werden die damit verbundenen Herausforderungen im Cloud-Computing diskutiert und das Konzept der Sealed Cloud als Lösung dieser Thematik vorgestellt.

Herausforderung Datenschutz und Datensicherheit in der Cloud

1

Hubert A. Jäger, Ralf O. G. Rieken und Edmund Ernst

Zusammenfassung

Der Begriff „Verschlüsselung“ wird klassisch fast synonym zum Begriff „Sicherheit“ gebraucht. Welche Sicherheitslücken offen bleiben, selbst wenn man Verschlüsselung nach allen Regeln der Kunst anwendet, und welche Herausforderung es bedeutet, diese zu schließen, wird in diesem ersten Kapitel behandelt. Zunächst wird die Verteilung der Rollen, der Verantwortung und der Haftung beim Cloud-Computing betrachtet. In diesem Zusammenhang spielt die Zertifizierung von Cloud-Diensten eine entscheidende Rolle. Anschließend werden die Angriffsmöglichkeiten, die Herausforderung des Datenschutzes und der Datensicherheit mit dem Fokus auf das spezielle Problem der Insider-Attacken und dem damit verbundenen Vertrauensdilemma besprochen. Daraus ergeben sich schließlich die Anforderungen an sicheres Cloud-Computing, die am Ende dieses Kapitels formuliert werden.

1.1 Cloud-Computing als Datenverarbeitung im Auftrag

Beim Cloud-Computing werden Teile oder die gesamte Datenverarbeitung nicht auf den Endgeräten des Nutzers, sondern in einer zentralen Recheninfrastruktur ausgeführt. Der Nutzer erteilt dem Cloud-Anbieter den Auftrag für diese Verarbeitungsvorgänge. In diesem Abschnitt wird betrachtet, wer in diesem Konstrukt welche Rolle einnimmt und

H. A. Jäger (✉) · R. O. G. Rieken (✉) · E. Ernst
Uniscon GmbH, München, Deutschland
E-Mail: hubert.a.jaeger@web.de; ralf@rieken.de

© Der/die Herausgeber bzw. der/die Autor(en), exklusiv lizenziert durch Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

H. A. Jäger, R. O. G. Rieken (Hrsg.), *Manipulationssichere Cloud-Infrastrukturen*,
https://doi.org/10.1007/978-3-658-31849-9_1

die Verantwortung für welche Schutzziele trägt, und wie dies im Datenschutz und weiteren Gesetzen abgebildet ist.

1.1.1 Beteiligte und Schutzziele

Neben den Nutzern und dem Anbieter der Cloud sind noch eine Reihe weiterer Personenkreise an einer Datenverarbeitung in der Cloud beteiligt. Sofern die verarbeiteten Daten einen Bezug zu natürlichen Personen aufweisen, sind diese persönlich betroffen, also so genannte „betroffene Personen“. In Abb. 1.1 sind neben einem Nutzer und dem Betreiber bzw. Anbieter der Cloud auch die persönlich Betroffenen, ein an sich unbeteiligter Dritter, sowie für den betrieblichen und wirtschaftlichen Kontext ein industrieller Wettbewerber skizziert. Außerdem kann der Betreiber und Anbieter des Cloud-Dienstes eine auch Konformitätsberwertungs- oder Zertifizierungsstelle genannte Institution beauftragen, die ihrerseits unabhängige Prüfer beauftragt, den Dienst sowie die Anlagen und Prozesse, derer er sich zur Bereitstellung des Dienstes bedient, zu auditieren.[1] Diese Prüfer werden dann den Dienst sicherheitstechnisch untersuchen, die Dokumentation sowie die organisatorische und technische Implementierung prüfen, sowie der Zertifizierungsstelle die Ergebnisse vorlegen, die dann abhängig vom Ergebnis ggf. ein Zertifikat ausstellt.

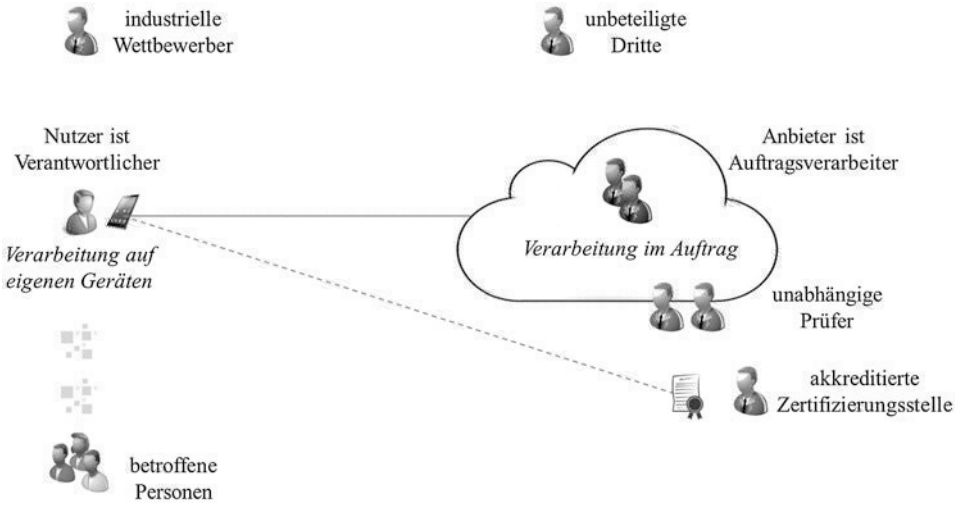

Abb. 1.1 Die Beteiligten beim Cloud-Computing

[1] Die umgekehrte Reihenfolge, dass etwa der Betreiber und Anbieter des Cloud-Dienstes einen unabhängigen Prüfer beauftragt, der seine Ergebnisse dann der Konformitätsberwertungs- bzw. Zertifizierungsstelle vorlegt, ist entsprechend einer Entscheidung der Deutschen Akkreditierungsstelle (DAkkS) nicht zulässig [1].

Welche Rollen die Beteiligten jeweils einnehmen, wird schon deutlich, wenn man sich die angelsächsischen Begriffe für die Beteiligten vor Augen führt:

- Der Cloud-Nutzer ist Verantwortlicher → „controller“
- Der Cloud-Betreiber ist Auftragsverarbeiter → „processor“
- Die betroffenen Personen sind → „data subjects“
- Die datenschutzrechtlich unbeteiligten Dritten sind die → „third parties“
- Die Wettbewerber, vor denen Betriebs- und Geschäftsgeheimnisse geschützt bleiben sollen, sind die → „competitors“
- Die unabhängigen Prüfer sind → „auditors“
- Die akkreditierte Zertifizierungsstelle bzw. Konformitätsbwertungsstelle ist der → „accredited certification body“

Der Cloud-Nutzer verarbeitet Daten teilweise auf den eigenen Geräten und teilweise in der Cloud. Diese nutzt er als ein weiteres Mittel zur Erledigung seiner Datenverarbeitungstätigkeiten.[2] Er erteilt hierfür dem Cloud-Betreiber einen Auftrag zur Datenverarbeitung. Die Daten, die er verarbeitet, können entweder auf die Betroffenen bezogene Daten – so genannte personenbezogene oder personenbeziehbare Daten – oder Betriebs- oder Geschäftsgeheimnisse sein. Die Daten können gleichzeitig sowohl personenbezogen als auch von Geheimhaltungsinteresse für einen Betrieb sein. Außerdem ist der Cloud-Nutzer ggf. ein Berufs- oder Amtsgeheimnisträger. In diesem Fall können die persönlichen Daten über den Personenbezug hinaus außerdem Berufs- oder Amtsgeheimnisse sein. Die Verantwortung des Cloud-Nutzers kann sich also auf drei verschiedene Hauptschutzziele beziehen:

- Datenschutz
- Berufs- oder Amtsgeheimnisschutz
- Betriebs- oder Geschäftsgeheimnisschutz

Der Datenschutz bezieht sich, wie in Kap. 3 bei der Abgrenzung des Begriffes Datenschutz von der Datensicherheit detailliert erläutert ist, auf den Schutz der von den personenbezogenen Daten betroffenen Personen. Wie in Abb. 1.2 angedeutet, bezieht sich der Datenschutz also nicht, wie der Name vermuten lassen könnte, auf den Schutz der Daten, sondern auf den Schutz der Persönlichkeitsrechte, d. h. letztlich auf den Schutz der Würde und der Freiheit der Betroffenen. Da die Würde unantastbar und die Freiheit unveräußerlich sind, sind auch personenbezogene Daten unveräußerlich.

[2] Ob hierfür eine weitere gesetzliche Grundlage nachgewiesen werden muss, ist umstritten. Diese datenschutzrechtliche Debatte ist für Deutschland mit der EU-Datenschutzgrundverordnung (DSGVO) neu aufgeflackert. Bisher (vor dem Inkrafttreten der DSGVO) wurde von einem gesetzlich speziell eingeräumten Privileg gesprochen, wenn der Cloud-Nutzer in ein Auftragsdatenverarbeitungsverhältnis eintrat und hierfür keine weitere gesetzliche Grundlage nachgewiesen werden musste.

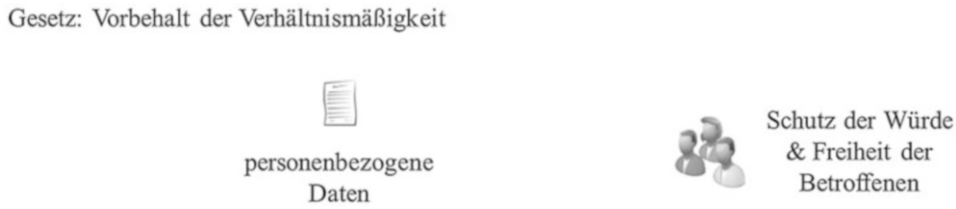

Abb. 1.2 Die Schutzziele des Datenschutzes sind die Würde und die Freiheit der Betroffenen

Das heißt, wenn eine Person heute ein Nutzungsrecht einräumt – gegebenenfalls gegen Zahlung – so kann sie dieses Recht morgen ohne Weiteres wieder zurückziehen. Es findet kein Eigentumsübergang im klassischen Sinn statt [2]. Mit personenbezogenen Daten kann in diesem Sinne nicht gehandelt werden. Dies mag vielleicht zunächst hochtrabend klingen, wird aber schnell plausibel, wenn man die in Zukunft zu befürchtenden Konsequenzen bei fehlendem Datenschutz – wie Konformitätsdruck, Manipulation, Gängelung und Zwang – bedenkt. Dies ist der Hintergrund für den ständig wachsenden Stellenwert des Datenschutzes. Der Datenschutz darf aber auch nicht den freien Verkehr von Daten behindern, daher sind alle vom Datenschutz vorgeschriebenen Maßnahmen stets „risikoangemessen" zu wählen, d. h. es muss bezogen auf die Schutzziele der Würde und Freiheit die Verhältnismäßigkeit gewahrt werden.

Personenbezogene Daten können jedoch zusätzlich noch Berufs- oder Amtsgeheimnisse sein, etwa gemäß § 203 des deutschen Strafgesetzbuches. Dort ist ein Katalog von Berufen angegeben, wie z. B. Ärzte, Apotheker, Rechtsanwälte, Wirtschaftsprüfer, Steuerberater, Versicherungsangestellte, Lebensberater, Datenschutzbeauftragte, etc., auf deren Vertrauensverhältnis zu den Patienten, Mandanten, Bürgern, etc. das Gesetz als Schutzziel abhebt. Das Gesetz bezieht sich auch auf Beamte und Angestellte des öffentlichen Dienstes, die mit Amtsgeheimnissen zu tun haben. In Abb. 1.3 ist angedeutet, dass für solche Daten nach herrschender Meinung [3] ein absolutes Offenbarungsverbot besteht, d. h. das Gesetz stellt unter Strafe, wenn andere als zur Kenntnis der Geheimnisse befugte Personen technisch in der Lage wären, Kenntnis von den Geheimnissen zu erlangen. Es kommt also nicht darauf an, ob jemand unbefugt Kenntnis von Geheimnissen erlangt, sondern lediglich, ob er aufgrund der technischen Gegebenheiten theoretisch oder praktisch Kenntnis

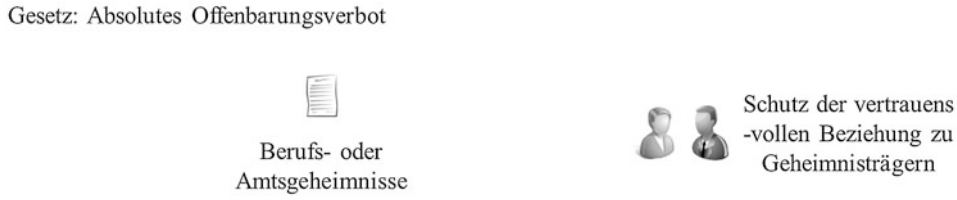

Abb. 1.3 Das Schutzziel des Geheimnisschutzes ist die vertrauensvolle Beziehung zu einem Berufs- oder Amtsgeheimnisträger. Eine Offenbarung liegt bereits ohne Versuch oder Vollzug, sondern bereits bei einer praktischen Möglichkeit zur Kenntnisnahme durch Unbefugte vor