O'REILLY®

PROJEKT EUREKA

bei Investments Unlimited

Helen Beal, Bill Bensing,
Jason Cox, Michael Edenzon,
Tapabrata Pal, Caleb Queern,
John Rzeszotarski, Andres Vega,
John Willis

Deutsche Übersetzung
von Jørgen W. Lang

Der Roman

über DevOps, Sicherheit,
Audit, Compliance und
Erfolg im digitalen Zeitalter

Lob für »Projekt Eureka«

»Dieses Buch erklärt auf hervorragende Weise, wie gute DevOps-Praktiken dazu beitragen können, dass Ihre Software sicher, geschützt und auditierbar ist. Ich habe eine Menge aus diesem Buch gelernt, was längst nicht bei allen DevOps-Büchern der Fall ist, die ich in den letzten Jahren gelesen habe. Dieses Buch ist ein Muss für alle CISOs und Führungskräfte, die die Sicherheit und Compliance in ihren Unternehmen verbessern wollen.«

– Ross Clanton, Chief Architect und Managing Director, American Airlines

»*Projekt Eureka* baut auf Jahre der DevSecOps-Literatur auf und verankert diese Prinzipien in regulierten Einheiten wie Finanzdienstleistungen. Diese technologische Fabel wird Sie fesseln mit nachvollziehbaren Geschichten, Gesprächen und Praxiswissen, das Sie in Ihrer eigenen Firma und Ihrem Team selbst umsetzen können.«

– Dr. Branden R. Williams, VP IAM Strategy, Ping Identity

»Endlich gibt es ein Buch, das für alle geeignet ist, die im Unternehmen Sicherheits-, Audit- und Compliance-Anforderungen erfüllen müssen. Sie können diesen praktischen Leitfaden sofort umsetzen. Dabei schätze ich besonders, dass alle für den Erfolg notwendigen Funktionen und Rollen einbezogen werden. Das Buch ist eine großartige Erinnerung daran, dass wir bei diesem Thema alle im selben Boot sitzen.«

– Courtney Kissler, CTO, Zulily

»Heutzutage sind Softwareentwickler auch Security Engineers, selbst wenn sie sich dessen nicht bewusst sind. *Projekt Eureka* veranschaulicht auf einzigartige und fesselnde Weise, wie Sicherheitstests, Audits und Compliance automatisiert werden können, um Unternehmen zu helfen, schneller und sicherer voranzukommen. Diese rasante und unterhaltsame Geschichte beleuchtet ein besonders wichtiges Thema: die Notwendigkeit, Sicherheit, Audits und Compliance aus ihrem Schattendasein herauszuholen und in den Entwickleralltag zu integrieren. Heutzutage gehören Sicherheit, Auditierung und Compliance zum Arbeitsalltag aller Beteiligten. *Projekt Eureka* bringt ans Licht, dass diese grundlegenden Funktionen durch DevOps unterstützt werden.«

– Jim Manico, Founder und Secure Coding Educator, Manicode Security

»Dieses Buch hilft, die Angst und Frustration zu überwinden, die viele Unternehmen im Umgang mit Auditierung und Compliance lähmen. Die Geschichte von *Projekt Eureka* schafft auf unterhaltsame Weise gegenseitiges Verständnis über Funktionen und Rollen hinweg und zeigt uns die praktischen Schritte, mit denen höheres Tempo, Stabilität und Compliance in unseren eigenen Unternehmen wahr werden können.«

– Jeff Gallimore, CTIO, Excella

»Zu den Techniken und Werkzeugen von DevOps gibt es bereits zahllose Bücher. Aber statt eines technischen Leitfadens ist *Projekt Eureka* ein Buch, das viele der Feinheiten und Details abstrahiert und vielmehr eine Geschichte darüber erzählt, wie eine DevOps-Transformation für die Menschen und Teams eines Unternehmens aussehen könnte.«

– Maya Senen, Sr. SRE

»Dieses Buch sollte Pflichtlektüre für jeden Softwareproduktmanager und -entwickler sein. Lernen Sie anhand einer fiktiven Geschichte, die die täglichen Herausforderungen gut beschreibt, wie Sie Sicherheit, Compliance, Auditierung und automatisiertes Testen in Ihrem Unternehmen implementieren können.«

– Thomas Underhill, JD, Director of Trust Engineering Programs, VMware

Projekt Eureka bei Investments Unlimited

Der Roman über DevOps, Sicherheit, Audit, Compliance und Erfolg im digitalen Zeitalter

Helen Beal, Bill Bensing, Jason Cox,
Michael Edenzon, Tapabrata Pal, Caleb Queern,
John Rzeszotarski, Andres Vega, John Willis

Deutsche Übersetzung von Jørgen W. Lang

O'REILLY®

Helen Beal, Bill Bensing, Jason Cox, Michael Edenzon, Tapabrata Pal, Caleb Queern,
John Rzeszotarski, Andres Vega, John Willis

Lektorat: Alexandra Follenius
Übersetzung: Jørgen W. Lang
Copy-Editing: Sibylle Feldmann, *www.richtiger-text.de*
Satz: III-satz, *www.drei-satz.de*
Herstellung: Stefanie Weidner
Umschlaggestaltung: Michael Oréal, *www.oreal.de*, unter Verwendung der iStock-Fotografie ID 115041620 von Sashkinw © iStock by Getty Images sowie der Illustration ID 81901933 von Taiga © Fotolia/Adobe Stock
Druck und Bindung: mediaprint solutions GmbH, 33100 Paderborn

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

ISBN:
Print 978-3-96009-220-9
PDF 978-3-96010-772-9
ePub 978-3-96010-773-6
mobi 978-3-96010-774-3

1. Auflage 2023

Wieblinger Weg 17
69123 Heidelberg

Dieses Buch erscheint in Kooperation mit O'Reilly Media, Inc. unter dem Imprint »O'REILLY«.
O'REILLY ist ein Markenzeichen und eine eingetragene Marke von O'Reilly Media, Inc. und wird mit Einwilligung des Eigentümers verwendet.

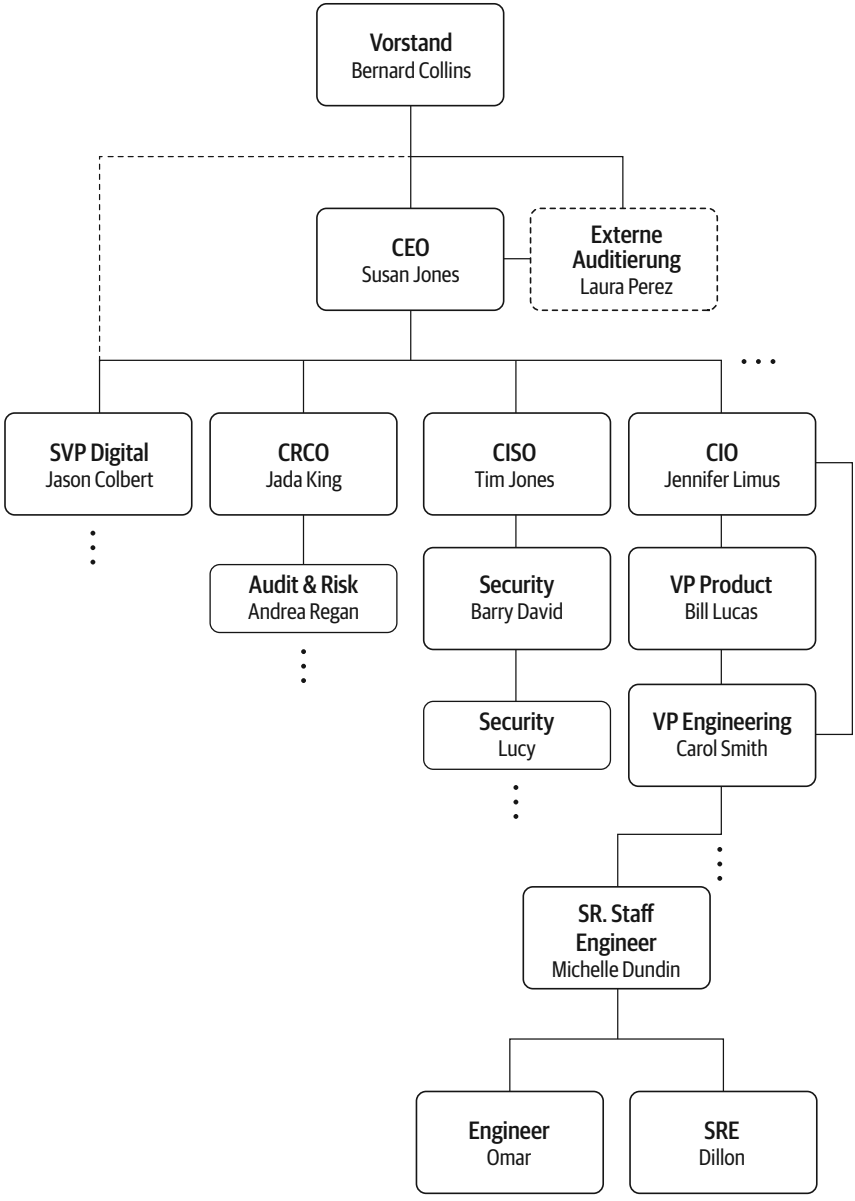
Hinweis:
Dieses Buch wurde mit mineralölfreien Farben auf PEFC-zertifiziertem Papier aus nachhaltiger Waldwirtschaft gedruckt. Der Umwelt zuliebe verzichten wir zusätzlich auf die Einschweißfolie. Hergestellt in Deutschland.

Schreiben Sie uns:
Falls Sie Anregungen, Wünsche und Kommentare haben, lassen Sie es uns wissen: *kommentar@oreilly.de*.

5 4 3 2 1 0

Für alle, die den Wandel in jedem Unternehmen vorantreiben,
die es wagen, den Status quo infrage zu stellen,
die keine Mauern bauen, sondern Brücken,
und die uns in eine grenzenlose Zukunft führen.

Inhalt


Vorstand
Bernard Collins
CEO
Susan Jones
Externe Auditierung
Laura Perez
SVP Digital
Jason Colbert
CRCO
Jada King
CISO
Tim Jones
CIO
Jennifer Limus
Audit & Risk
Andrea Regan
Security
Barry David
VP Product
Bill Lucas
Security
Lucy
VP Engineering
Carol Smith
SR. Staff Engineer
Michelle Dundin
Engineer
Omar
SRE
Dillon

Mitarbeiterverzeichnis von Investments Unlimited

Bernard Collins, Vorstandsvorsitzender

Susan Jones, CEO

Jason Colbert, Senior Vice President Digital Transformation

Jada King, Chief Risk und Compliance Officer (CRCO)

Tim Jones, Chief Information Security Officer (CISO)

Jennifer Limus, Senior Vice President of Engineering und Chief Information Officer (CIO)

Bill Lucas, **Vice President** of Product

Carol Smith, **Vice President** of Engineering, Digital Banking

Michelle Dundin, Senior Staff Engineer

Barry David, Security

Andrea Regan, Audit & Risk

Omar, Staff Engineer

Dillon, Staff Site Reliability Engineer

Lucy, Security

Laura Perez, Externes Auditierungsunternehmen

Vorwort

Governance. Menschen reagieren sehr unterschiedlich auf dieses Wort. Bei den einen löst es Beklemmung, Frustration, Angst und Wut aus. Bei anderen steht es für die Aufrechterhaltung von Frieden, Ordnung und Sicherheit. Unabhängig davon, wie Sie auf dieses Wort reagieren, werden Sie feststellen, dass Sie auf die eine oder andere Weise für die Einhaltung oder Aufrechterhaltung von Governance verantwortlich sind.

IT-Governance im Unternehmen ist ein komplexes Thema. Unabhängig davon, wie Sie auf das Konzept an sich reagieren, ist eine gute Governance mit vielen Schwierigkeiten verbunden. Wie andere Prozesse versucht auch Governance, Kontrollmechanismen zu schaffen, um die wichtigsten Ressourcen eines Unternehmens zu schützen, seien es Menschen, Daten, Marken oder Produkte. Leider führt die Umsetzung von Governance in der Praxis oft zu enormen Reibungsverlusten, Unzufriedenheit und Misserfolgen für die Teams, die versuchen, für ihr Unternehmen Werte zu schaffen.

Dieses Buch erzählt die Geschichte von Investments Unlimited, Inc (IUI), einem fiktiven FinTech-Unternehmen. Die gleiche Geschichte könnte jedoch für jede Branche und jedes Unternehmen gelten, das sich mit Governance befasst.

Das Buch soll Unternehmen dabei helfen, Governance und die Art und Weise, wie Software im Unternehmen erstellt wird, radikal neu zu denken. Wir stellen Konzepte, Werkzeuge und Ideen vor, mit denen Sie Governance in einem neuen Licht sehen können. Wir wollen eine menschlichere und schnellere Softwarebereitstellung fördern, die Vertrauen schafft und von sich aus sicherer ist.

Wir hoffen, Ihnen auf der Reise durch diese Erzählung auf unterhaltsame Weise einige moderne Vorgehensweisen zu vermitteln, die Ihnen helfen, Governance neu zu betrachten, umzusetzen, gut zu nutzen sowie zu überleben, und Sie dadurch beim Erreichen von Unternehmenszielen zu unterstützen. Am Ende wird es für Sie einfacher, Business Values besser, schneller, sicherer und glücklicher zu erreichen.

– Die Autorinnen und Autoren

Auftakt

»Dad. Schlechte Nachrichten.«

Es war ein wolkenverhangener Nachmittag in Neuengland, USA, und es regnete mittlerweile so stark, dass Greg Dorshaw seine jugendliche Tochter bitten musste, das Gesagte zu wiederholen. Sein altes Klapphandy war immer schwerer zu verstehen.

»Dad, die haben das Spiel abgesagt – wegen des Wetters. Du musst nicht kommen. Also, fahr vorsichtig auf dem Weg nach Hause.«

Dorshaw hatte noch kein einziges Softballspiel seiner Tochter verpasst. Diese Woche war das regnerische Bostoner Wetter dem Aufsichtsbeamten jedoch eine willkommene Ausrede, um länger im Büro zu bleiben und sich eine E-Mail genauer anzusehen, die er am Tag zuvor von seinem Team erhalten hatte.

Um sich besser konzentrieren zu können, schaltete er die Neonbeleuchtung in seinem Büro im Direktorium der US-Zentralbank aus, stocherte ein wenig in seinem Thai-Take-away herum und nahm sich dann die E-Mail vor. Das Gesicht nur vom Monitor beleuchtet, las er:

Betreff: IUI-Ergebnisse der Vorprüfung

Greg, offenbar wiederholt sich mal wieder die Geschichte. Sieht aus, als lege ein weiteres FinTech-Unternehmen es auf eine Unterlassungserklärung an.

Das Team macht sich ziemliche Sorgen ...

Kapitel 1

Montag, 28. März

Susan Jones war nun schon seit fünf Jahren CEO bei Investments Unlimited, Inc. (IUI). Sie war schlagfertig, stellte anscheinend immer die richtigen Fragen und traf die richtigen Entscheidungen. Der Vorstand vertraute ihr. Und obwohl nichts an ihrem Verhalten es erahnen ließ – jetzt war sie in Panik.

Fast keuchend fragte Susan: »Woher weißt du das?« Heute war der traditionelle Familienpizzaabend. ***Trotzdem*** hatte sie die Küche verlassen, um den dringenden Anruf anzunehmen. Die Geräusche der Familie hinter ihr – Rich und Lucas machten Richs berühmte Pizza – schienen zu verblassen. Sie konnte nur noch ihren eigenen Herzschlag hören ... und Jason, den Senior Vice President (SVP) für digitale Transformation.

»Ich habe mich heute mit Bernard zu unserem üblichen Scotch-Abend getroffen. Er sagte mir, dass IUI eine MRIA[1] erhalten würde. Sieht ganz so aus, als sei die Finanzaufsicht hinter uns her. Eigentlich sollen die uns doch helfen, unsere Kunden zu schützen.«

»Du veräppelst mich doch, oder?«, erwiderte Susan immer noch ein wenig atemlos. Sie glaubte aber nicht, dass Jason sie gehört hatte, denn er sprach einfach weiter.

»Es ist nicht ungewöhnlich, dass die MRIA auf inoffiziellem Weg angekündigt wird, um Überraschungen bei der offiziellen Zustellung zu vermeiden. Bernard hat ein gutes Verhältnis zum Direktor der Behörde, die die MRIAs ausstellt. Der Direktor hat Bernard als Zeichen seines guten Willens vorab informiert«, sagte Jason.

Susan musste tief Luft holen. Sie wusste, was MRIAs sind, *Matters Requiring Immediate Attention*. Die Aussicht war alarmierend. Die Finanzaufsicht stellte MRIAs nur aus, wenn eine Bank ernsthaft in Schieflage geraten war. So etwas wird nicht einfach wie Süßigkeiten verteilt. Susan kannte solche Horrorgeschichten von anderen Geldinstituten. In Banken, in denen

1 Genauere Informationen zu MRAs (Matters Requiring Attention – Dinge, die Aufmerksamkeit erfordern) und MRIAs (Matters Requiring Immediate Attention – Dinge, die sofortige Aufmerksamkeit erfordern) finden Sie in Anhang A.

sie gearbeitet hatte, war das noch nie passiert – vor allem nicht in einer Bank, die sie leitete.

»Weißt du, worum es in der MRIA geht?«, fragte Susan.

»Ja. Und der Grund ist – ehrlich gesagt – ziemlich peinlich. Im vergangenen Jahr hat IUI über 15 MRAs (*Matters Requiring Attention*) erhalten. Wir haben für einige eine Verlängerung beantragt, aber offenbar gibt es keinen klaren Plan, wie sie erfüllt werden können. Unser Team hat keinerlei Nachweise für irgendwelche Fortschritte vorgelegt, und jetzt ist die Aufsicht der Meinung, wir hätten ein riesiges Problem.«

»Ich verstehe«, sagte Susan, obwohl sie eigentlich gar nichts verstand. *Wie konnte mein Team das zulassen?*, fragte sie sich. *Wie konnte* ***ich*** *das zulassen?* Ihr Chief Audit Officer hatte ihr immer wieder versichert, dass mit diesen MRAs alles in Ordnung sei. Das war offensichtlich nicht der Fall.

»Das ist keine Kleinigkeit, und das weißt du«, sagte Jason. »Bernard hält große Stücke auf dich. Er weiß, was du kannst. Ich erinnerte ihn daran, dass er ohne dich niemals in Rente hätte gehen können. Er stimmte mir zu.«

»Danke, Jason. Das ist wirklich nett von dir. Als Erstes müssen wir morgen früh das gesamte Team zusammenrufen, um herauszufinden, wie wir überhaupt in diesen Schlamassel geraten konnten. Mehr können wir heute Abend nicht tun.«

»Klingt gut«, antwortete Jason. »Bitte entschuldige die abendliche Störung, aber ich wusste, dass du darüber informiert werden wolltest. Wir reden morgen weiter. Gute Nacht.«

»Ja, Jason, vielen Dank! Ich bin froh, dass du dich gemeldet hast. Gute Nacht.« Susan legte auf und setzte sich langsam an den Esszimmertisch, der so groß war, dass gut und gerne 15 Personen Platz fänden, und er war immer so eingedeckt, als könnte jeden Moment eine Dinnerparty stattfinden. Die sorgfältige Anordnung des Geschirrs vor ihr schien sich über sie lustig zu machen, während sie über die Folgen des Gesprächs mit Jason nachdachte. Ihr Verstand suchte fieberhaft nach Antworten und Lösungen.

Sie saß einfach da und wartete darauf, dass ihre Benommenheit nachlassen und ihre rasenden Gedanken wieder zur Ruhe kommen würden.

»Schatz, geht's dir gut?«, fragte Rich vorsichtig, als er aus der Küche kam.

»Ja, alles in Ordnung. Gib mir eine Minute, und ich komme rüber und helfe euch mit der Pizza«, antwortete Susan. Sie konnte die Tomatensoße, die Rich nach einem alten sizilianischen Rezept kochte, geradezu riechen. Es war eines seiner Lieblingsrezepte, das von seiner Urgroßmutter stammte und das seine Mutter an ihn weitergegeben hatte. Sie atmete tief ein. Das

köstliche Aroma war wie eine Therapie. Anscheinend fühlte sie sich schon besser – vielleicht hatte sie einfach nur Hunger. Jedenfalls ging sie in die Küche.

Als Susan sich umsah, war alles, was sie sah, eine große Unordnung. Die Arbeitsfläche und der Boden waren mit weißem Mehl bedeckt. Es sah aus, als hätte es in ihrer Küche geschneit.

»Also, *diese* Angelegenheit hier erfordert auf jeden Fall meine sofortige Aufmerksamkeit.« Susan ging hinüber zu ihrem sechsjährigen Sohn Lucas, der unbeschwert Smileys mit dem Finger ins Mehl auf dem Küchentresen malte.

»Musst du dich heute noch mit Jason treffen?«, wollte Rich wissen. »Nein, der Anruf hat schon genug angerichtet für einen Abend«, antwortete Susan und band sich die Küchenschürze um.

»Ohhh, ist Mama in Schwierigkeiten?«, fragte Lucas und wischte seine mehlbedeckten Hände an Susans vormals sauberer Schürze ab.

»Na, na, Lucas«, tadelte Rich ihn sanft. »Nein, Mama ist nicht in Schwierigkeiten. Es gibt nur ein Problem bei der Arbeit. Aber sie bringt das in Ordnung. Deshalb ist sie auch die Chefin«, sagte Rich und schenkte dabei seiner Frau ein Lächeln. Gleichzeitig warf er ein rundes Stück Pizzateig auf den Tresen vor ihnen. Mehl wirbelte in die Luft, und Lucas musste lachen.

»Was denn für ein Problem?«, wollte Lucas wissen, während Susan die Soße auf dem Teig verteilte. »Hast du deinen Chef nicht ausreden lassen? Oder eine Regel missachtet? Weil, Xian hat heute nämlich in der Pause eine Regel gebrochen und musste den Rest der Pause sitzen bleiben und durfte überhaupt nicht spielen.«

»Nein, ich habe keine Regeln gebrochen«, antwortete Susan. »Es gibt bei der Arbeit nur ein paar Sachen aufzuräumen, die nicht so gelaufen sind, wie sie sollten. Und jetzt müssen wir in kurzer Zeit eine Menge Dinge in Ordnung bringen.«

»Ist das so, wie wenn Oma zu Besuch kommt und du ganz verrückt wirst?«, wollte Lucas wissen und fuchtelte dabei dramatisch mit den Armen herum.

Mühsam ein Lachen unterdrückend, wandte sich Rich den Belägen für die Pizza zu.

»Nein, nein. Das ist eher so, wie wenn ich dir sage, dass du dein Zimmer aufräumen sollst. Das ist dann eine MRA, eine Sache, die Aufmerksamkeit erfordert«, antwortete Susan, und ihre Stimme klang dabei so ernst, als moderierte sie einen Filmtrailer.