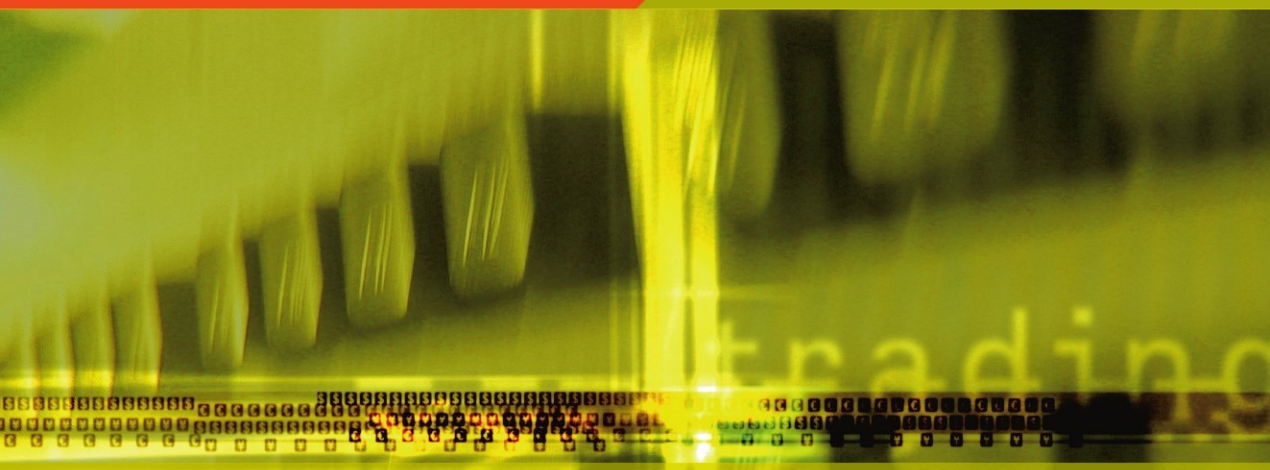
Aleksandra Sowa

Metriken – der Schlüssel zum erfolgreichen Security und Compliance Monitoring

Design, Implementierung und Validierung in der Praxis

PRAXIS



VIEWEG+
TEUBNER

Aleksandra Sowa

Metriken – der Schlüssel zum erfolgreichen Security und Compliance Monitoring

Aleksandra Sowa

Metriken – der Schlüssel zum erfolgreichen Security und Compliance Monitoring

Design, Implementierung und Validierung in der Praxis

Herausgegeben von Stephen Fedtke

Mit 20 Abbildungen

PRAXIS

VIEWEG+
TEUBNER

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.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage 2011

Lektorat: Christel Roß | Maren Mithöfer

Vieweg+Teubner Verlag ist eine Marke von Springer Fachmedien.
Springer Fachmedien ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.viewegteubner.de

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier
Printed in Germany

ISBN 978-3-8348-1480-7

Vorwort

Der Einsatz von Metriken als Instrument der Compliance hat in Deutschland bislang noch relativ wenig Verbreitung gefunden, gewinnt aber in den Unternehmen, die die Effektivität ihrer internen Kontrollsysteme gegenüber sachverständigen Dritten nachweisen wollen (oder müssen), stetig an Bedeutung. Insbesondere die Anfangsphase der Implementierung von Metriken kann sich potentiell als „zäh" aufzeigen. Oftmals liegen noch keine Best Practices oder Industriebeispiele für den direkten Einsatz geeigneter Metriken vor, oder es bestehen – oft unbegründete – Berührungsängste mit der mathematischen Formelwelt der Metriken.

Aus diesem Problem entstand die Motivation für dieses Buch. Es greift das Thema „Metrik" auf eine eigene, über das Ziel besonders motivierende Weise auf und knüpft dabei auch an die englischsprachigen Quellen auf diesem Gebiet an. Bewusst wurde eine kompakte und pragmatische Form gewählt, indem sich das Buch auf die für die Praxis besonders leistungsfähigen und relevanten Metriken konzentriert, hierbei aber auch Methoden wie auch Lösungsoptionen für den praktischen Einsatz und die bedarfsgerechte Fortentwicklung und Adaption aufzeigt. Es stellt somit keinen Anspruch auf allgemeine bzw. wissenschaftliche Vollständigkeit, sondern bietet für die unternehmenspraktische Umgebung die notwendige Hilfe – im Sinne eines erfolgreichen Soforteinstiegs. Als Leser werden Sie deshalb auch zielorientiert und nachhaltig zum eigenen Recherchieren, Interpretieren und Experimentieren mit Metriken befähigt und motiviert – auch ohne mit den mathematischen bzw. methodischen Grundlagen in Berührung zu kommen.

Weshalb bedarf es allgemein noch erhöhter Motivation für den Einsatz von Metriken? Compliance in der Informationstechnologie (IT-Compliance) wird gerne als bloße Verpflichtung betrachtet, deren Umsetzung auf den ersten Blick primär nur – hohe – Kosten verursacht. Dabei kann eine effiziente und effektive Umsetzung regulatorischer Anforderungen an die IT-Kontrollen, bedingt durch die nachhaltig qualitätssichernde Wirkung, regelrecht zu einem Wettbewerbsvorteil werden. Dies aber nur dann, wenn der richtige Ansatz für deren Umsetzung gewählt wird.

Ein solcher Ansatz – eine methodische Vorgehensweise, um durch den Einsatz von Metriken die Effektivität implementierter Kontrollen zu bewerten, Verbesserungspotential zu identifizieren und zu kommunizieren – ist Kernthema dieses Buches. Hierfür wird in den Kapiteln 2 und 3 ein definitorisches Rahmengerüst aufgebaut, um die gängigen Begriffe wie Monitoring, Metrik und Kontrolle voneinander abzugrenzen sowie die gegenseitige Verknüpfungen und Verflechtungen aufzuzeigen. Ergänzend dazu enthält Kapitel 4 einen kurzen Überblick über die Anforde-

rungen an das Monitoring bzw. die IT-Kontrollen am Beispiel ausgewählter regulatorischer Vorgaben, Normen und Standards.

Neben einer Sammlung von Metriken am Ende des Buches, welche nahezu direkt in die Anwendung übernommen werden können, vermittelt das Buch zugleich die notwendige praxistaugliche Methodik zur Entwicklung und Ableitung weiterer eigener Metriken, sowie erfolgreiche Vorgehensweisen zur Aggregation von Metriken bis hin zur Informations- und Entscheidungsvorlage für das Management. Der Leser findet eine anhand von Beispielen veranschaulichte Methode zur Ableitung der Metriken aus den Unternehmenszielen im Kapitel 5. Kapitel 6 ist den Verfahren gewidmet, welche es den Verantwortlichen ermöglichen, die Metriken, die Kontrollen – sowie das Monitoring insgesamt – den jeweils aktuellen Anforderungen entsprechend zu aktualisieren und in die Unternehmensprozesse nachhaltig zu integrieren. Zahlreiche Hinweise zur Gestaltung von Reports und Auswahl der für verschiedene Reporttypen geeigneter Inhalte wurden im Kapitel 7 vorgestellt. In gleicher Weise wird der angemessenen Darstellung der Ergebnisse im Rahmen des Reportings Aufmerksamkeit geschenkt und durch Beispiele dokumentiert. Ein Überblick über die ausgewählten – die aktuell populären und die weniger bekannten – Darstellungsmöglichkeiten wurde im Kapitel 8 dargestellt. Als eine Art Ausblick werden am Ende praxisnahe und erprobte Verfahren um die neuesten theoretischen und wissenschaftlichen Erkenntnisse ergänzt.

Dieses Vorwort wäre unvollständig ohne ein paar Dankesworte: Mein herzlicher Dank geht an Herrn Dr. Stephen Fedtke für den Ideenreichtum und die anregenden Gespräche. Christian Schulze möchte ich für die spontanen Hinweise und Ergänzungen aus seiner Tätigkeit als EDV-Revisor eines Kreditinstitutes, IT-Sicherheits-Berater und Dozent, sehr herzlich danken. Frau Lisa Reinerth möchte ich überdies danken für den speziell für dieses Buch entwickelten „Don Trust Comic“ zum Thema Metriken. Frau Dr. Christel Roß sowie Frau Maren Mithöfer vom Verlag Vieweg+Teubner waren mir in vieler Weise behilflich; ihnen danke ich für die sehr gute Zusammenarbeit und für die reiche Ausstattung des Buches. Mein größter Dank geht an meine Familie für ihr Vertrauen und ihre Unterstützung.

Bonn, im Februar 2011 Dr. Aleksandra Sowa

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung – Warum Metriken?

„Das Schicksal hat die Bühne verlassen, auf der gespielt wird, um hinter den Kulissen zu lauern, außerhalb der gültigen Dramaturgie, im Vordergrund wird alles zum Unfall, die Krankheiten, die Krisen. [...] So droht kein Gott mehr, keine Gerechtigkeit, kein Fatum wie in der fünften Symphonie, sondern Verkehrsunfälle, Deichbrüche infolge Fehlkonstruktion, Explosion einer Atombombenfabrik, hervorgerufen durch einen zerstreuten Laboranten, falsch eingestellte Brutmaschinen. In diese Welt der Pannen führt unser Weg ...“

Friedrich Dürrenmatt, „Die Panne“

Verslehre ist eine konkrete Wissenschaft. Wer noch nie eine metrische Analyse von Verstexten vorgenommen hat, weiß vermutlich nicht, dass Interpretation von Gedichten ein Handwerk ist, das einen systematischen Ansatz erfordert. „Der Laie hat für gewöhnlich, sofern er ein Liebhaber von Gedichten ist, einen lebhaften Widerwillen gegen das, was man Zerpflücken von Gedichten nennt, ein Heranführen kalter Logik, Herausreißen von Wörtern und Bildern aus diesen zarten blütenhaften Gebilden“ – stellt Berthold Brecht in einem kurzen Prosatext „Über das Zerpflücken von Gedichten“ fest. Das „Zerpflücken“, diese wenig bekannte Wissenschaft der Reim-, Vers- und Strophenlehre, heißt Metrik. Entgegen der verbreiteten Meinung, haben metrische Studien es in keinem Fall nur mit stumpfem Zählen und Verseklopfen zu tun. Ihr Gegenstand ist die „in dem besonderen Sprachgebrauch begründete Sinnlichkeit von Verstexten und die Bedeutung ihrer metrischen Form“ (Moennighoff 2004, 8). Grundkenntnisse der Metrik helfen, Lyrik besser zu verstehen.

Ähnlich verhält es sich mit der Metrik als Instrument des Security und Compliance Monitoring. Nur, dass hier nicht die Reime oder Verse gezählt und analysiert werden, sondern die innewohnenden Merkmale der Informationssicherheit, die dazugehörigen Kontrollen, Prozesse und die an diesen Prozessen beteiligten Menschen. Werden diese Merkmale gemessen, ausgewertet, analysiert und bewertet, helfen sie, den Zustand sowie das Verbesserungspotential der Sicherheit und den Stand der Einhaltung relevanter Standards und regulatorischer Vorgaben (*compliance*) zu identifizieren. So hilft beispielsweise eine gute Sicherheitsmetrik „to evaluate the efficiency, effectiveness and impact of an information security program, and […] identify and diagnose security-related problems“ (Maloney 2009, 1). Im Grunde genommen, erfüllen Metriken für die Informationssicherheit und Compliance eine sehr ähnliche Rolle wie in der Verslehre: Sie helfen, das Unternehmen besser zu verstehen.

A. Sowa, *Metriken – der Schlüssel zum erfolgreichen Security und Compliance Monitoring*,
DOI 10.1007/978-3-8348-8194-6_1, © Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2011

2 Metrik – Definition und Begriffsabgrenzung

Metriken für Security und Compliance Monitoring – wozu braucht man sie eigentlich?

Um dies zu verstehen, muss man zuerst zu der Erkenntnis gelangen, warum Monitoring der Security und Compliance (*security compliance monitoring*) heute zu den wesentlichen Aspekten des Internen Kontrollsystems (IKS) gehört. Sicherheit und Compliance sind zu bedeutenden Performance-Indikatoren eines Unternehmens geworden. Nicht nur deshalb, weil bei der Nichteinhaltung regulatorischer Vorgaben die Haftungsrisiken für die Unternehmensleitung steigen und oft hohe Strafen drohen[1]. Auch deshalb, weil Reputationsrisiken bei bekannt gewordenen Sicherheitsschwachstellen und/oder Kontrollschwächen drohen, welche die Risikowahrnehmung bei Stakeholder und Shareholder beeinflussen – oft mit entsprechend negativen Konsequenzen für das Geschäft. Auch „wachsende Verwundbarkeit und die Gefahr massiver wirtschaftlicher Schäden in Folge von Risiken bei der Informationsverarbeitung erhöhen den Handlungsdruck", so das Bundesamt für Sicherheit in der Informationstechnik (BSI 2009, 6).

Sicherheit ist ein Prozess. Compliance dagegen wird als ein Zustand definiert[2]. Informationssicherheit ist geprägt durch den ständigen Kampf zwischen Code-Designer und Code-Brechern (Dobbertin 2002). Sie wird durch drei Grundwerte beschrieben: Vertraulichkeit (*confidentiality*), Verfügbarkeit (*availability*) und Integrität (*integrity*). Diese sind wie folgt definiert:

- Vertraulichkeit: Schutz vertraulicher Informationen (Daten) vor unbefugter Preisgabe.
- Verfügbarkeit: Verfügbarkeit von Dienstleistungen, Funktionen oder Informationen zum geforderten Zeitpunkt (ad hoc und ex post). Dies umfasst auch kontrollierte und sichere Aufbewahrung (Archivierung) von Daten und Datenträgern.
- Integrität: Vollständigkeit und Unverändertheit der Daten. Der Verlust der Integrität von Informationen kann bedeuten, dass diese unerlaubt oder zufällig verändert, Angaben zum Autor verfälscht wurden, oder der Zeitpunkt der Erstellung manipuliert wurde (BSI 2009).

1 Auf die regulatorischen Anforderungen an die Sicherheit wird im Kapitel 4 eingegangen.

2 Neben der Compliance als Zustand ist oft von einem Compliance-Prozess die Rede. Dabei handelt es sich um einen Prozess zur Herstellung bzw. Erreichung des Compliance-Zustandes.

A. Sowa, *Metriken – der Schlüssel zum erfolgreichen Security und Compliance Monitoring*,
DOI 10.1007/978-3-8348-8194-6_2, © Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2011

Verbreitet ist die Aussage, dass es eine 100-prozentige Sicherheit nicht geben kann. Dies steht nicht im Widerspruch zu der Aussage, dass sich ein Unternehmen Ziele für die Informationssicherheit setzen und eine 100-prozentige Erreichung dieser Ziele anstreben kann. Compliance-Nachweis gemäß IDW PS 951, CMMI Reife 5,0 oder ISO 27001-Zertifizierung des Sicherheitsmanagementsystems sind Beispiele für solche Ziele.

Compliance wird definiert als ein Zustand, in dem regulatorische Anforderungen, Gesetze und Vorschriften sowie vertragliche Verpflichtungen eingehalten werden (ISACA 2010). Der Weg zur IT-Compliance (auch: Compliance in der IT) ist hingegen ein Prozess. Prof. Klotz schlägt zwei Begriffsdefinitionen für die IT-Compliance vor und unterscheidet hier zwischen der sog. „weiten" und „engen" Fassung des Begriffes. Eine weite Fassung: „IT-Compliance bezeichnet einen Zustand, in dem alle für die IT des Unternehmens relevanten bzw. als relevant akzeptierten internen und externen Regelwerke nachweislich eingehalten werden" (Klotz 2008, 9). Im engeren Sinne (auch als „legal IT compliance" bezeichnet) bezeichnet IT-Compliance „einen Zustand, in dem alle für die IT des Unternehmens relevanten, allgemein geltenden rechtlichen, d. h. regulatorischen Vorgaben nachweislich eingehalten werden" (Klotz 2008, 8).

Unternehmen sehen sich heute mit zahlreichen – direkten und indirekten – Anforderungen an die Informationssicherheit konfrontiert. Um die Umsetzung und Einhaltung dieser Anforderungen gegenüber Dritten nachweislich zu belegen, ist ein effektives Monitoring und Reporting notwendig. Andererseits stellt Monitoring selbst eine der Compliance-Anforderungen dar, da er unter anderem vom Committee of Sponsoring Organizations of the Treadway Commission (COSO) als Teil des effektiven IKS gesehen und gefordert wird(vgl. COSO 2007).

Angemessene Metriken sind die Grundlage des Monitoring. In den Metriken wird festgelegt, was, wann und in welchem Umfang gemessen werden muss, um eine zuverlässige Auskunft über den Zustand der sogenannten *security compliance* (sowie ihr Verbesserungspotential) zu gewährleisten.

2.1 Metrik: Definition und Kategorisierung

Das National Institute of Standards and Technology (NIST) hat in der Special Publication (SP) 800-55 folgende, allgemein geltende Definition der Metrik vorgeschlagen:

„Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions, based on observed measurements"(Maloney 2009, 1).

Generell werden die Metriken in drei Hauptgruppen unterteilt: die

- *strategischen Metriken*,
- *Management-Metriken* (taktische Metriken) und
- *operativen Metriken* (vgl. Brotby 2009).

In der Informationstechnologie sind die operativen bzw. technischen Metriken am stärksten verbreitet. Oft sind sie leicht zu erzeugen und liegen in Maß und Fülle vor. Allerdings sind sie wenig oder gar nicht geeignet, wenn es um Entscheidungsunterstützung hinsichtlich Strategie, Compliance oder Management des gesamten Sicherheitsprogramms im Unternehmen geht. „The majority of organisations … attempt to operate security using primarily operational information, which makes as much sense as flying aircraft without knowing position or destination, attitude or altitude", stellte Brotby (2009, 28) fest.

Alle Metriken – unabhängig von der Art – sollen dem Zweck dienen, eine Basis für Entscheidungen zu liefern (auf strategischer, taktischer oder technischer Ebene).

In den folgenden Abschnitten werden zwei in der Informationstechnologie bekannte und verbreitete Metriken kurz vorgestellt: die Sicherheitsmetrik und die Softwaremetrik. Der Abgrenzung dieser Metriken von der Metrik als Instrument des Security und Compliance Monitoring (sog. *security compliance metrics*) sowie Definition der Letzteren ist das abschließende Kapitel gewidmet.

2.1.1 Sicherheitsmetriken

Für das interne Kontrollsystem spielen die Sicherheitsmaßnahmen eine besondere Rolle. So zählen unter anderem die Zugriffs- und Zugangskontrollen zu den fünf wesentlichen Kontrollen in der IT (sog. *IT general controls*, ITGC), welche bei jeder Abschlussprüfung berücksichtigt werden müssen (Singleton 2010). Es wundert also nicht, dass ausgerechnet „security of data, code and communication / data security and document retention / security threats" von dem American Institute of Certified Public Accountants (AICPA) in seinem „Top Technology Initiatives Survey" im Jahr 2010 zu den „top ten technology considerations" erhoben wurden, welche die Unternehmen heute vertreiben/nutzen (AICPA 2010).

Sicherheitsmetriken (*security metrics*) bilden eine beachtliche Untermenge aller IT-bezogener Metriken. Die Sicherheitsmetriken beziehen sich konkret auf Informationssysteme (Applikationen und Infrastruktur) sowie IT-Projekte und andere, sicherheitsrelevante Prozesse. Laut Chapin und Akridge (2005), wird eine Sicherheitsmetrik als Messung der Effektivität und Effizienz von Sicherheitsbestrebungen, -bemühungen und -leistungen in einer Organisation im Zeitablauf definiert.

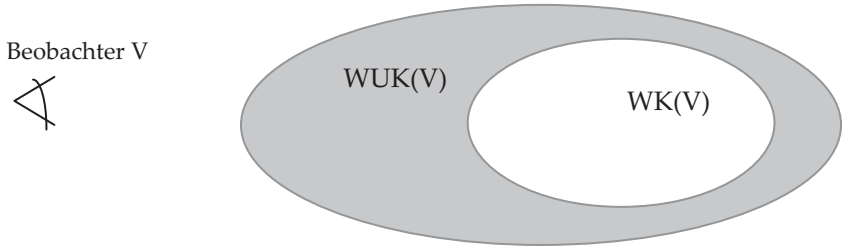
Sicherheitsmetriken können – abhängig von dem Zweck und der Zielgruppe, für welche sie bestimmt wurden – unterschiedliche Detaillierungsgrade aufweisen. Sie können sowohl in detaillierten Auswertungen der Logfiles resultieren, welche für Mitarbeiter mit technischer Expertise bestimmt sind, als auch eine Übersicht erfolgter (erfolgreicher und nicht-erfolgreicher) Angriffsversuche auf die internen Sys-

teme (nach Angriffsart) beinhalten, welche für das Risikomanagement bzw. die Unternehmensleitung relevant sind (z.B. Incident Reports)[3].

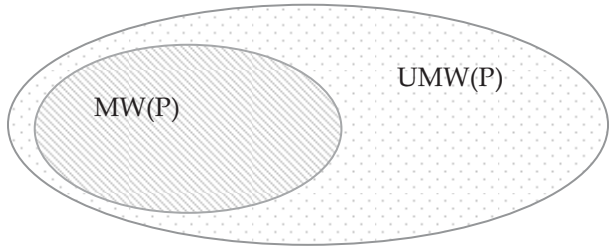
Exkurs zum Thema Sicherheitsmetriken

Wie Mark Torgerson in seinem kurzen Vortrag zum Thema „Security Metrics" bewiesen hat, „no metrics exists that can tell you how secure your system is in an absolute sense" (Torgerson 2007).

In seinem Beweis berücksichtigte er einen Angreifer *V*, welcher sowohl das notwendige Wissen als auch die Ressourcen für die Durchführung eines Angriffs besitzt. Als externer Beobachter des Systems *S* (die Gesamtmenge aller Systemschwächen wird als *W* bezeichnet), sieht oder vermutet er eine Menge an Schwächen *WK(V)*; es existiert auch eine Menge von Schwächen im System, *WUK(V)*, welche dem Angreifer unbekannt ist.



Andererseits wird das System *S* durch eine Reihe von Sicherheitsmaßnahmen *P* geschützt, welche einen bestimmten Anteil an Schwächen, *MW(P),* abdecken. Es gibt auch einen Teil an Schwächen, die nicht durch ein Sicherheitssystem abgedeckt sind: *UMW(P)*.



Dem Angreifer sind also nur diese Schwächen, *E*, ausgesetzt, die er vermutet und welche zugleich durch das Sicherheitssystem *P* nicht abgedeckt sind, das heißt wir reden hier über die Schnittmenge von beiden:

$E(P, V) = UMW(P) \cap WK(V)$.

Ein System *S* ist dann sicher gegen den Angreifer V, wenn $E(P, V) = \emptyset$.

3 Beispiele für Sicherheitsmetriken finden sich in der Metrik-Sammlung.