# Kennzahlen im Informationssicherheitsmanagement: Konzeption, Einführung, Weiterentwicklung

Reiner Kraft · Mechthild Stöwer

Fraunhofer-Institut für sichere Informationstechnologie
{reiner.kraft | mechthild.stoewer}@sit.fraunhofer.de

## Zusammenfassung

Die Anwendung von Kennzahlen zur Überwachung des Status der Informationssicherheit wird zwar immer häufiger diskutiert, in der Praxis wird ein solches Instrument jedoch nach wie vor nur sehr eingeschränkt eingesetzt. Einer der wesentlichen Hinderungsgründe liegt in der Problematik, aussagefähige Kennzahlen für alle Bereiche des Sicherheitsmanagements zu finden, die gleichwohl ohne größeren Aufwand zu erheben sind. Darüber hinaus müssen diese Maßzahlen normiert werden, damit sie vergleich- und aggregierbar sind. Diese beiden Aufgaben sind nicht leicht zu lösen. Der vorliegende Artikel zeigt anhand von Praxisbeispielen, dass dies sehr wohl gelingen kann und dass damit Kennzahlen einen Beitrag zur Optimierung des Informationssicherheitsmanagements leisten können. Er soll damit interessierte Institutionen dazu ermutigen, passende aussagefähige Kennzahlensysteme zur Verbesserung des Informationssicherheitsniveaus einzuführen.

# 1 Motivation

Auf anerkannten Standards wie [ISO 27001] und [ISO 27002] oder dem IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik ([BSI08], [GSKAT11]) gründende Managementsysteme mit klar definierten Verantwortlichkeiten und umfassenden technischen und organisatorischen Sicherheitsmaßnahmen erhöhen das Informationssicherheitsniveau einer Organisation signifikant. Sie bieten darüber hinaus auch Organisationen, die einen solchen Nachweis aufgrund der an sie gestellten Compliance-Anforderungen wünschen, die Möglichkeit zur Zertifizierung ihres Informationssicherheitsmanagementsystems (ISMS).

Die Umsetzung der Regelwerke wird durch interne und externe Audits überprüft. Dieses Verfahren ist anerkannt, erlaubt jedoch eine Evaluierung des ISMS immer nur zu festgelegten Zeitpunkten. In diesen Audits wird der Status einer aktuellen Sicherheitsimplementierung gegen ein vereinbartes Zielsystem abgeglichen, werden Defizite erfasst und bewertet. Aus Managementsicht ist es jedoch wünschenswert, zu beliebigen Zeitpunkten über Indikatoren Informationen über den Zielerreichungsgrad einer Organisation zur Informationssicherheit und eventuelle Abweichungen zu erhalten.

Hierfür haben sich Leistungskennzahlen (Key Performance Indicators, KPIs) in vielen Bereichen bewährt. Die Anforderung, den Stand der Informationssicherheit regelmäßig zu messen, war bereits Bestandteil der ersten Fassung der ISO 27001 aus dem Jahr 2005. Die vier Jahr

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 148-156.

später verabschiedete Norm ISO 27004 konkretisierte diese Anforderung und bot ein Vorgehensmodell zur Entwicklung geeigneter Kennzahlen, skizzierte deren Beschaffenheit und ergänzte diese Vorgaben durch eine Reihe von Beispielen im Anhang. In der Ende 2013 überarbeiteten Fassung der ISO 27001 wurde die Anforderung nach einer systematischen Messung der Effizienz und Effektivität noch stärker herausgestellt und in einem eigenen Abschnitt („9.1 Monitoring, measurement, analysis and evaluation“) präzisiert. Eine an ISO 27001/02:2013 angepasste Neufassung der ISO 27004 ist in Bearbeitung.

Der Gedanke, durch ständige Überwachung Zielabweichungen schnell zu erkennen und durch Maßnahmen eine Optimierung des System zu erreichen, liegt auch den Reifegradmodellen zugrunde, wie sie etwa im Rahmenwerk für IT-Governance COBIT formuliert sind, das für reife Prozesse ein Prozesskontrollsystem verlangt.

In der Praxis werden Sicherheitskennzahlen jedoch nach wie vor kaum oder allenfalls rudimentär verwendet. Wenn überhaupt eingeführt, beschränken sie sich meist auf toolgestützte Systemscans nach Schwachstellen rund um die umgesetzten technischen Sicherheitsmaßnahmen (Firewalls, Virenscanner, Spamfilter etc.) und auf diese bezogenen Richtlinien (z. B. Passwortregeln).

# 2 Ziele für die Nutzung von Kennzahlensystemen

Die Anforderungen der ISO 27001 aber auch eine zunehmende Durchdringung des ISMS durch quantitative Betrachtungen, wie sie etwa das IT-Risikomanagement oder auch Wirtschaftlichkeitsanalysen kennzeichnen, rücken die Integration von Kennzahlen verstärkt in den Blick von IS-Managern. Folgende Ziele können dabei im Vordergrund stehen [KÜ]:

- Darstellung des aktuellen Stands des ISMS sowie von Trends und Soll-Ist-Vergleichen für Managementpräsentationen,
- Identifikation kritischer Bereich des ISMS, die abhängig von den ermittelten Werten einer vertieften Analyse unterzogen werden können,
- Bewertung der Effektivität der umgesetzten Sicherheitsmaßnahmen,
- Bewertung der Effizienz der umgesetzten Sicherheitsmaßnahmen,
- Erhöhung der Awareness für Informationssicherheit bei Anwendern und beim Management.

Sicherheitskennzahlen erlauben zwar einen kontinuierlicheren Blick auf ein ISMS als Audits, ersetzen letztere andererseits aber auch nicht. Die Überwachung des ISMS durch Maßzahlen kann jedoch den Blick auf kritische Bereiche lenken, die durch Audits oder andere Formen der Sicherheitsüberprüfung (z. B. Penetrationstests) vertieft analysiert werden können. Eine solche Vorgehensweise erhöht die Effizienz und die Effektivität von Audits und anderen Maßnahmen zur Prüfung der Effektivität eines ISMS.

Zielgruppen für Kennzahlenanalysen sind primär die Manager der Informationssicherheit, aber auch Entscheidungsträger, die die Wirkungskontrolle von Sicherheitsinvestitionen verantworten, benötigen Kennzahlen. Eine weitere Gruppe sind Administratoren, die für ihre operativen Aufgaben aussagefähige Statistiken zu Sicherheitsvorfällen oder Unterstützung beim Changemanagement benötigen.

# 3 Aussagefähige Kennzahlen

## 3.1 Anforderungen

Die Entwicklung eines Kennzahlensystems, das relevante Aussagen über die Reife eines Informationssicherheitsmanagementsystems ermöglicht und dies zuverlässig überwachen kann, ist eine sehr anspruchsvolle Aufgabe. Dies liegt insbesondere daran, dass ein ISMS viele Aspekte der Informationssicherheit integriert und somit aus verschiedensten Bereichen Kennzahlen extrahiert werden müssen, die unterschiedliche Skalierungen aufweisen werden. Zur Aggregation und zum Vergleich der Maßzahlen müssen diese normiert werden (siehe hierzu [JUL09]).

Die größte Herausforderung liegt jedoch darin, wirklich aussagefähige Kennzahlen zu entwickeln, die leicht zu interpretieren sind. Die Metriken benötigen einen sinnvollen Bezugspunkt. Abweichungen vom Sollwert und Veränderungen im Zeitablauf müssen eine sinnvolle Aussage über den Gegenstand der Beurteilung erlauben, um Input für Managementfragestellungen zu liefern:

- In welchen Bereichen der Infrastruktur der Organisation gibt es Defizite bezüglich der Informationssicherheit?
- Was sind die kritischen Bereiche, welche Probleme sind prioritär zu behandeln?
- Wie soll das knappe Budget verwendet werden?
- Welche Investitionen sind lohnend?
- Hat sich die Informationssicherheit durch vorgenommene Investitionen oder organisatorische Maßnahmen erhöht? Wie groß ist die Verbesserung?
- Wie sicher sind die Unternehmensteile (Standorte)? Sind Benchmarks zwischen den Standorten möglich?

Auch müssen die Kennzahlen mit vertretbarem Aufwand zu erheben sein. Während sich aus der Überwachung technischer Systeme leichter Kennzahlen generieren lassen, ist die Entwicklung geeigneter Metriken für die organisatorischen Aspekte der Informationssicherheit nicht immer einfach [JAQ07].

Zudem ist der Informationsbedarf der verschiedenen Zielgruppen sehr unterschiedlich. Ein kennzahlenbasiertes Monitoring- und Reporting-System muss sowohl den Controlling-Anforderungen der Geschäftsleitungsebene entsprechen als auch die Analyseaufgaben der operativen Ebene unterstützen. Diese beiden Zielgruppen benötigen unterschiedliche Informationen und vor allem in unterschiedlichen Aggregationsgraden. Geeignete Kennzahlensysteme müssen beides liefern.

## 3.2 Beispiele

Es finden sich in der Literatur inzwischen vielfältige Vorschläge für Informationssicherheitsmaßzahlen, darunter auch solche, die alle wesentlichen Aspekte der Informationssicherheit abbilden sollen. Hier ließen sich die „20 Critical Security Controls for Effective Cyber Defense“ [CSIS] oder die von [JAQ07] formulierten technischen oder organisatorischen Kennzahlen sowie die Vorschläge des Centers for Internet Security [CIS] und der US-amerikanischen Normungseinrichtung NIST [NIST 800-55] anführen. All diese Veröffentlichungen sind zwar mög-

liche Quellen für organisationsspezifische Maßzahlen, sie können jedoch kaum als „Best Practice“-Systeme übernommen werden, da dokumentierte Praxiserfahrungen weitgehend fehlen [ACC11].

Die am häufigsten aufgeführten Kennzahlen sind im Bereich des Incident Managements, des Vulnerability oder des Patch Managements angesiedelt. Diese Kennzahlen reflektieren zwar wichtige Aufgabenbereiche der Informationssicherheit, sind aber für einen ganzheitlichen Ansatz unbedingt durch weitere Kennzahlen zu ergänzen.

Eine gute Quelle zur Ableitung von Kennzahlen bietet die ISO 27001/27002 mit ihren Regelungsbereichen (control clauses) und Regeln (controls). Folgende Tabelle zeigt mögliche Kennzahlen und ihren Bezug zur ISO 27001.

**Tab. 1:** Beispielkennzahlen und ihre Beziehung zur ISO 27001

| Kennzahl | | ISO 27001 Bezug | |
|---|---|---|---|
| Bezeichnung | Berechnung | Nr. | Regelungsbereich |
| Management Reporting IT-Sicherheit | # der Sitzungen der Geschäftsführung mit IT-Sicherheitsberichten / # aller Sitzungen der Geschäftsführung | 6.1 | Internal organization |
| IT-Sicherheitsbudget | IT-Sicherheitsbudget / IT-Budget | 6.1 | Internal organization |
| Schulung | # Anzahl der Teilnehmer an IT-Sicherheitsschulungen / # aller Angestellten | 7.2 | Human ressource security |
| Grad der Sensibilisierung | Durchschnittliche Punktzahl in Abschlusstests / erzielbare Punktzahl | 7.2 | Human ressource security |
| Asset Inventory | # fehlerhafter Einträge im Asset Inventory / # aller Einträge | 8.1 | Asset Inventory |
| Asset Owner | # aller Assets ohne Asset Owner / # aller Einträge | 8.1 | Asset inventory |
| Informationsklassifizierung | # aller Dokumente, die policykonform sind / # aller geprüften Dokumente | 8.2 | Information classification |
| Zugriffsrechte | # aller korrekt dokumentierten Zugriffsrechte / # aller dokumentierten Zugriffsrechte | 9.2 | User access management |
| Privilegierte Benutzer | # Anzahl der Benutzer mit Administrationsrechten / # Anzahl der Benutzer | 9.2 | User access management |
| E-Mail-Verschlüsselung | # verschlüsselter interner E-Mails / # aller internen E-Mails | 10.1 | Cryptographic controls |
| Gebäudesicherheit | # dokumentierter Sicherheitsverletzungen im Journal des Sicherheitsdienstes / # aller Einträge | 11.11 | Physical security perimeter |
| Change Management | # der Changes mit Sicherheitsaudits / # aller Change Requests | 12.1 | Operational procedures and responsibilities |
| Malware auf Client Systemen | # maleware incidents auf den Clientsystemen / # aller identifizierten malware am Gateway | 12.2 | Protection from malware |

| Kennzahl | | ISO 27001 Bezug | |
|---|---|---|---|
| Bezeichnung | Berechnung | Nr. | Regelungsbereich |
| Zentral überwachte Systeme | # zentral überwachter Systeme / # aller administrierten Systeme | 12.4 | Logging and monitoring |
| Schwachstellenmanagement | Durchschnittliche Dauer vom Bekanntwerden bis zur Behebung einer Schwachstellen | 12.6 | Technical vulnerability management |
| Patchmanagement | Durchschnittliche Dauer zwischen dem Bereitstellen und Einspielen eines Patches | 12.6 | Technical vulnerability management |
| Durchdringungsgrad der Informationssicherheit bei Softwareentwicklung | # der SW-Entwicklungsprojekte mit Begleitung durch IT-Sicherheitsbeauftragte / # aller IT-Projekte | 14.2 | Security in development and support processes |
| Sicherheit in der Beziehung zu Zulieferern | # der Verträge mit Zulieferern, in den explizit das Thema Informationssicherheit spezifiziert wird / # aller Verträge | 15.1 | Information security in supplier relatonships |
| Anteil der Security Incidents | # der Security Incidents / # aller Incidents in der Berichtsperiode | 16.1 | Management of information security incidents and improvements |
| Durchdringungsgrad des Notfallmanagements | # der Geschäftsprozesse mit Notfallplan / # aller dokumentierten Geschäftsprozesse | 17.1 | Information security continuity |

Auch aus den „Goldenen Regeln“, die den Grundschutzkatalogen beigefügt sind, lassen sich sinnvolle Kennzahlen ableiten [BSI08].

# 4 Vorgehensmodell

Die ISO 27004 beschreibt ein Vorgehensmodell für die Entwicklung eines Systems von Maßzahlen für Informationssicherheit, das dem PDCA-Zyklus folgt [ISO27004]. Am Ausgangspunkt eines Projekts für die Implementierung eines Kennzahlensystems stehen die Informationsanliegen einer Organisation. Aus dem betrieblichen Regelwerk, das sich aus Standards und Normenwerken speist, können geeignete Kennzahlen abgeleitet, durch Berechnungsverfahren operationalisiert und mit geeigneten Sollwerten versehen werden. Diesen Sollwerten werden nun die tatsächlich erhobenen Werte gegenübergestellt, bewertet und aufbereitet. Diesen Prozess zeigt folgende Abbildung.

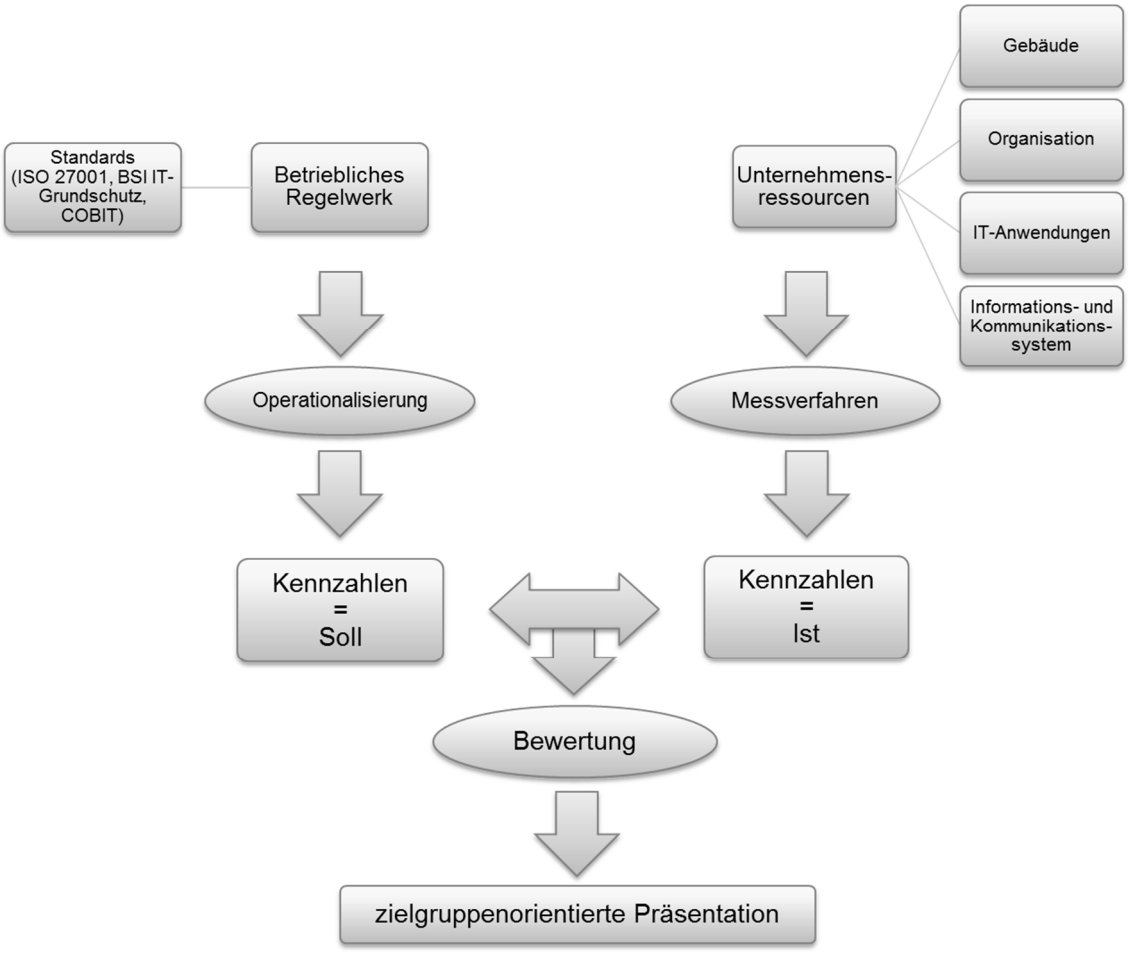


**Abb. 1:** Vorgehen zur Nutzung von Kennzahlen

Bei der Konzeption und Implementierung von Kennzahlen lassen sich grundsätzlich zwei Strategien verfolgen:

- Überwachung und Kontrolle besonders kritischer Bereiche, für die Kennzahlen abgeleitet werden. Diese Strategie kann in eine IT-Risikoanalyse eingebunden werden.
- Die Einbeziehung alle Bereiche der Informationssicherheit über ein System von Kennzahlen.

Dabei bindet die Einführung eines alle Aspekte der Informationssicherheit reflektierenden Kennzahlensystems erhebliche Ressourcen und kann Investitionen in Werkzeuge zur Erhebung und Präsentation erfordern. Bei der Umsetzung einer solchen Strategie hat es sich gezeigt, dass es daher auch hier sinnvoll ist, zunächst mit wenigen Maßzahlen zu beginnen.

Im Folgenden werden Erfahrungen, die in der Umsetzung dieser beiden Strategien aus Praxisprojekten gewonnen werden konnten, kurz skizziert.

Grundsätzlich ist es zu empfehlen, zunächst ein Pilotvorhaben aufzulegen und mit einer begrenzten Auswahl geeigneter Maßzahlen zu beginnen. Die gewonnenen Erkenntnisse können dann genutzt werden, um das System zu modifizieren und zu erweitern. Nach und nach können so alle gewünschten Aspekte der Informationssicherheit abgedeckt und die unterschiedlichen Zielgruppen mit den sie interessierenden Informationen versorgt werden.

# 5 Erfahrungen aus Kennzahlenprojekten

Die Konzeption und Implementierung eines auf alle Bereiche des ISMS bezogenen Kennzahlensystems war im Blick eines Pilotprojekts des Europäischen Satellitenkontrollzentrums ESOC in Darmstadt. Diese Organisation hat für ihren IT-Dienstleistungsbereich ein Informationssicherheitsmanagementsystem etabliert, das sich an den Vorgaben der ISO 27001 orientiert. Diese Aktivitäten sollen durch die Einführung eines Systems von Maßzahlen ergänzt werden, das den Status der Informationssicherheit kontinuierlich reflektiert. Im Rahmen dieses Projektes wurden 15 Kennzahlen formuliert, die nach der Evaluierung der Ergebnisse um weitere Kennzahlen und Funktionalitäten ergänzt werden sollten.

Das Projekt verfolgt Ziele sowohl auf der strategischen als auch auf der operativen Ebene.

Die vordringlichen strategischen Ziele sind:

- Reflektion des Reifegrades des Sicherheitsmanagementsystems,
- Messung des Umsetzungsgrades des ISO-Standards und der Effizienz des Managementsystems,
- Unterstützung für strategische ISMS-Entscheidungen.

Die Zielgruppen für diese Informationen sind Entscheidungsträger im Management der Organisation, die Informationssicherheitsmanager und interne Auditoren.

Die Kennzahlen, wurden anhand der Control Objectives der ISO 27002 identifiziert. Hierzu wurde eine Sammlung von 36 möglichen Kennzahlen abgeleitet, aus denen 15 Metriken für die Pilotphase des Projekts ausgewählt und beschrieben wurden [KAM].

Kriterien hierzu waren:

- die Relevanz hinsichtlich der Zielstellung,
- eine Aufwandsabschätzung für die Pilotimplementierung sowie
- eine möglichst breite Abdeckung aller Bereiche der Informationssicherheit und das Potential zur Schärfung des Bewusstseins für die Belange der Informationssicherheit.

Durch dieses Vorgehen wurde sichergestellt, dass nicht nur leicht zu erhebende, sondern auch aussagekräftige Metriken in das Pilotvorhaben einflossen. Zudem konnten durch die Erhebung und Präsentation von Kennzahlen aus allen Bereichen der Informationssicherheit Erfahrungen für die Erweiterung des Programms gewonnen werden.

Sollen die einzelnen Metriken verglichen und in einem System von Kennzahlen aggregiert werden, muss hierfür eine einheitliche Skalierung gefunden werden. Dieses Problem wurde in dem Projekt dadurch gelöst, dass die Messergebnisse für jede Metrik nach Bestimmung der Sollwerte in einer Zehner-Skalierung abgebildet wurden. Dabei standen die Skalenwerte 1 bis 5 für mangelhafte, die Werte 6 bis 8 für eine weitgehend noch ausbaubedürftige und die Werte 9 und 10 für eine gute und sehr gute Zielerreichung. Für jede Metrik wurden die Messergebnisse an dieser Skala gespiegelt.

Die Überprüfung, ob Teile eines Organisationsverbunds kritisch sein können, ist Ziel eines weiteren Kennzahlenprojekts. Dieses Vorhaben wurde von einem Unternehmen initiiert, das eine Vielzahl von Dienstleistern in die Leistungserbringung integriert und sicherstellen will, dass alle beteiligten Institutionen ein definiertes Informationssicherheitsniveau einhalten. In diesem

Vorhaben steht deswegen im Zentrum das Bedürfnis, einen ersten Eindruck über das Sicherheitsniveau bei den einbezogenen Dienstleistern zu erhalten, der es erlaubt, kritische Bereiche zu identifizieren und einen möglichen Bedarf an detaillierten Audits abzuleiten.

Dieses Beispiel zeigt, dass Kennzahlensysteme nicht nur zur Überwachung des in der eigenen Organisation implementierten ISMS von Relevanz -sein können, sondern auch Dritten Aufschlüsse über das ISMS erlauben können. Mit Kennzahlen können beispielsweise Zulieferer dem belieferten Produktionsunternehmen, unabhängige Einrichtungen in einem Dienstleistungsverbund einer Koordinierungsstelle oder aber auch Cloud-Anbieter ihren Kunden Aufschluss über den Stand des ISMS geben. Für diese Art der Nutzung von ISMS-Kennzahlen ist naturgemäß essentiell, dass die zugrunde liegende Datenbasis sowie die Verfahren zur Berechnung der Kennzahlen hinreichend vertrauenswürdig sind. Dies setzt zum einen deren Transparenz, zum anderen Mechanismen voraus, die Missbräuche und Fehler bei der Generierung von Messwerten und der Berechnung der Kennzahlen erkennbar werden lassen. Kennzahlen für Cloud-Anwendungen und ein geeignetes Vorgehensmodell zur Implementierung werden in dem aktuellen Projekt VerMetrix untersucht, bei dem ein besonderer Fokus auf der Überprüfbarkeit der Einhaltung Datenschutzvorgaben bei Cloudanbietern liegt (www.verimetrix.de). Die Fälschungssicherheit und damit Vertrauenswürdigkeit derartiger Kennzahlen ist hier eine besondere Herausforderung.

# 6 Aggregation zu Score Card Systemen

Scorecards sind ein verbreitetes Mittel, erhobene und berechnete Kennzahlen zusammen mit den gewünschten Zielwerten übersichtlich zu präsentieren. In einer solchen Darstellung bietet es sich an, thematisch verwandte Kennzahlen zusammenzufassen. Mögliche Dimensionen einer solchen Security Scorecard können beispielsweise sein,

- Organisatorische Sicherheit – hierunter fallen etwa Kennzahlen zur Überwachung der Informationssicherheit durch das Management, zur Sensibilisierung der Belegschaft oder zur Berücksichtigung der Sicherheitsaspekte in Verträgen mit Dritten.
- Netz- und Systemsicherheit mit Kennzahlen zum Status der Überwachung von Clients, Servern und Netzkomponenten, zur Effizienz der Malware-Erkennung oder zur Qualität des Vulnerability- und des Patch-Management.
- finanzielle Kennzahlen, die Aufschluss über die Wirtschaftlichkeit der Maßnahmen geben, die zur Erhöhung der Informationssicherheit getroffen wurden.

Bei der Aggregation zeigt sich, wie wichtig die Normierung der Kennzahlen ist. Nur so gelingt es, Kennzahlen zusammenfassend abzubilden und – dies ist noch wichtiger – zu vereinheitlichten Bewertungen zu kommen.

Score Cards sind gute Instrumente, um dem Management aggregierte Informationen im Zeitablauf zu präsentieren.

# 7 Fazit und Ausblick

Die Vorgehensweise, in einem Pilotprojekt mit einem reduzierten Set von Metriken zu beginnen, erscheint empfehlenswert. Bei einem zu unbedachten Vorgehen können Kennzahlenprojekte deutlich mehr Ressourcen binden als ursprünglich gedacht. Sie erfordern darüber hinaus die dauerhafte Unterstützung des Managements und die Mitwirkung von Unternehmensbereichen über die eigentliche ISMS-Organisation hinaus. Wenn etwa die Informationssicherheit in

3rd-Party-Kooperationen erfasst werden soll, müssen die Unternehmensbereiche, die die Vertragswerke steuern, Informationen bereitstellen. Dies erfordert Überzeugungsarbeit und kontinuierliche Motivation. Auch die Spezifikation der Messverfahren und die Formulierung von geeigneten Sollwerten gelingen häufig nicht bei der ersten Konzeption. In diesen Fällen ist ein Re-Design erforderlich.

Die Einführung eines ISMS-Kennzahlensystems erfordert auf jeden Fall einen „langen Atem" und die Bereitschaft des Managements, über einen längeren Zeitraum an diesem Vorhaben festzuhalten und es kontinuierlich auszubauen.

## Referenzen

[ACC11] Global Information Security Study 2011: Traditional approaches to information security are no longer sufficient (www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Global-Security-Research-2011.pdf).

[BSI08] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Informationssicherheit und IT-Grundschutz – BSI-Standards 100-1, 100-2 und 100-3, Bundesanzeiger Verlag, 2. Auflage 2008.

[CIS10] The Center for Internet Security (Hrsg.): The CIS Security Metrics, v.1.1.0, 2010

[CSIS11] Center for Strategic and International Studies: Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines, 2011 (www.sans.org/critical-security-controls/).

[GSKAT11] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutz-Kataloge, 12. Ergänzungslieferung, Bundesanzeiger Verlag, 2011.

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

[ISO 27002] International Organization for Standardization (Hrsg.): ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security management.

[ISO 27004] International Organization for Standardization (Hrsg.): ISO/IEC 27004:2009, Information technology – Security techniques – Information security management – Measurement.

[JAQ07] Security Metrics: Replacing Fear, Uncertainty, and Doubt, 2007.

[JUL09] Julisch, Klaus: A Unifying Theory of Security Metrics with Applications, IBM Research Report, Rüschlikon 2009.

[KAM11] Kammerhofer, Sabine: Implementierung von Sicherheitskennzahlen in den IT-Grundschutz, 2011.

[KÜ11] Kütz, Martin: Kennzahlen in der IT, Heidelberg 2011.

[NIST08] National Institute of Standards and Technology (Hrsg.): NIST 800-55: Performance Measurement Guide for Information Security, 2008