

## BSI Forum

offizielles Organ des BSI



Bundesamt  
für Sicherheit in der  
Informationstechnik

**Sonderdruck für**

**CETUS**  
Training & Consulting

<kes>/Microsoft-  
Studie 2012:  
Checkliste zur  
Informations-  
Sicherheit

S. 57

**Business-Continuity:  
Tools und  
Fallstricke**

ab S. 43



# EMERGENCY INSTRUCTIONS

# Kennzahlen fürs ISMS

## Erfolge messen und Security-Management-Systeme gezielt steuern

**Kennzahlen sollen dabei unterstützen, den Erfolg und die Funktionalität eines ISMS zu messen – häufig verwendete, rein technisch orientierte Kennzahlensysteme greifen dabei jedoch zu kurz. Die hier vorgestellte Methodik möchte helfen, aussagekräftigere Ergebnisse zu erzielen.**

Von Frederik Humpert-Vrielink, Schüttorf

Erfolg ist Ziel jedes Managementsystems und trägt maßgeblich zur Akzeptanz in der Fläche bei. Dabei bedeutet der Begriff „Erfolg“, dass die im Top-Level gestalteten Komponenten des ISMS auch auf den operativen Ebenen eines Unternehmens funktionieren und Akzeptanz finden. Kurz: Ein erfolgreiches Informationssicherheits-Managementsystem (ISMS) versagt nicht, wenn die Dokumentationsebene verlassen wird und die Strukturen in den alltäglichen Betrieb überführt werden sollen.

Doch gerade im Bereich des Informationssicherheitsmanagements (ISM) besteht erheblicher Nachholbedarf, da es bisher kaum ausgereifte Systeme oder Strukturen zur Erfolgsmessung gibt. Zwar bieten seit kurzem die ISO/IEC 27004 [1] sowie eine Publikation [2] des US-amerikanischen „National Institute of Standards and Technology“ (NIST) gute Ansätze – die Umsetzung in den tatsächlichen Strukturen lässt jedoch in der Realität oft zu wünschen übrig.

Systeme und Verfahren, die den Erfolg eines Managementsystems zur Informationssicherheit messen sollen, dienen letztlich dazu, Entscheidungen über den Fortgang und die Wirksamkeit eines ISMS fundiert treffen zu können. Ergebnisse der Erfolgsmessung werden sogar als Eingabevariable für die Managementbewertungen der gängigen Managementsysteme wie zum Beispiel der ISO/IEC 27001 gefordert. Diese Vorgabe folgt dem Grundsatz, dass sich Vorgänge, die man nicht messen kann, auch nicht effektiv steuern lassen. Aber wie sehen aussagekräftige Messzahlen und adäquate Messpunkte aus, die Aufschluss über den Erfolg eines ISMS im gesamten Unternehmen liefern?

Die meisten heutigen Kennzahlensysteme zur Informationssicherheit agieren „eindimensional“ auf technischer Ebene – beispielsweise werden Kennzahlen gebildet, die Auskunft geben über

- \_\_\_\_\_ den prozentualen Anteil installierter Sicherheitspatches,
- \_\_\_\_\_ die durchschnittliche Ausfallzeit eines IT-Services,
- \_\_\_\_\_ die Gesamtzahl erkannter IT-Sicherheitsvorfälle oder
- \_\_\_\_\_ die Gesamtzahl unberechtigter Zugriffsversuche auf das Netz.

Natürlich sind diese Kennzahlen nicht „falsch“. Ihre Aussagekraft erschöpft sich jedoch auf technischer Ebene und lässt den Security-Manager keine Aussagen über den tatsächlichen Erfolg des *Managementsystems* treffen – tatsächlich ermöglichen diese Kennzahlenbeispiele nur Aussagen über den Erfolg technischer Sicherheitsmaßnahmen.

### Mehrdimensionale Kennzahlen

Ein ISMS besteht jedoch aus mehr als technischen Sicherheitsmaßnahmen.

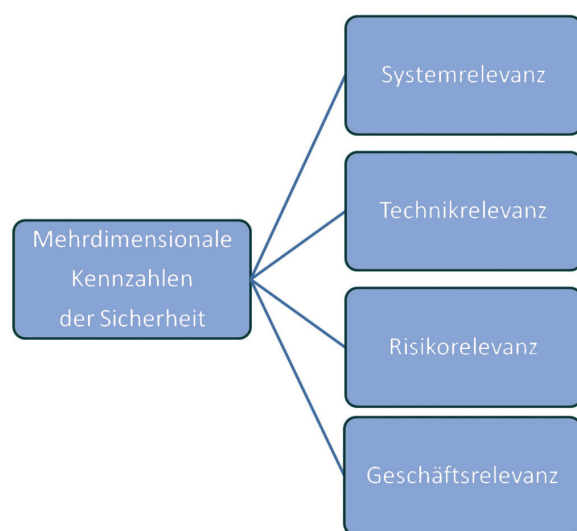


Abbildung 1:  
Vier Dimensionen  
für Kennzahlen

Ein ISMS umfasst nach herrschender Lehre vielmehr die vier Kernkomponenten:

- \_\_\_\_\_ Ressourcen,
- \_\_\_\_\_ Mitarbeiter,
- \_\_\_\_\_ Strategie und
- \_\_\_\_\_ Management-Prinzipien.

Diese Kernkomponenten können jedoch nur bei sinnvollem Monitoring des ISMS optimal alloziert werden. Gerade vor dem Hintergrund fortschreitender Budgetprobleme in Unternehmen – vor allem im IT-Dienstleistungssektor – wächst die Bedeutung des Monitorings von ISMS, um Zusammenhänge zwischen Budgetrestriktionen und Auswirkungen auf die Sicherheitsziele zu visualisieren.

Diese Anforderung bedeutet jedoch, verstärktes Augenmerk auf die Gesamteinbindung eines ISMS zu legen: Jedes ISMS verlangt, die Risiken und Schutzbedarfe auf Basis der Anforderungen der Geschäftsstruktur und der unternehmenseigenen Werte sowie der Strategie festzulegen. Daraus leitet sich ab, dass sich auch das anzuwendende Messinstrument für den Erfolg und die Wirksamkeit des ISMS dieser Struktur zu unterwerfen hat.

Und daraus ergibt sich auch der entsprechende Prozess, um passende Kennzahlen zu entwickeln. Wichtig ist es, hierbei vier Dimensionen zu beleuchten, welche die Basis für die ermittelten Kennzahlen liefern (vgl. Abb. 1):

- \_\_\_\_\_ Systemrelevanz,
- \_\_\_\_\_ Technikrelevanz,
- \_\_\_\_\_ Risikorelevanz sowie
- \_\_\_\_\_ Geschäftsrelevanz.

Systemrelevanz bedeutet dabei, Kennzahlen zu ermitteln, die Auskunft geben, wie funktionsfähig das Managementsystem tatsächlich ist – diese Zahlenmenge bezieht sich also nicht auf technische Systeme, sondern auf die Wirksamkeit des Zusammenspiels zwischen Prozes-

sen und Abläufen des eigentlichen Managementsystems. Technikrelevanz beschreibt hingegen diejenigen Kennzahlen, welche (ähnlich den bereits genannten Beispielen) die technische Dimension der Informationssicherheit abbilden. Risikorelevanz gibt Aufschluss darüber, wie sich das allgemeine Risikomanagement im ISMS zielgerichtet entwickelt. Und Geschäftsrelevanz ermöglicht es, den Erfolg des ISMS mit Auswirkungen auf das Geschäft des Unternehmens in Zusammenhang zu stellen. Beispiele für solche Kennzahlen zeigt Tabelle 1.

## Kennzahlentwicklung als Prozess

Kennzahlen zu bilden ist in jedem Projekt eine Herausforderung. Der entscheidende Punkt ist es, Kennzahlen und Messfaktoren auszuwählen, die auf das eigene Unternehmen und das eigene Geschäft angepasst sind. Wert zu legen ist hier vor allem auf

- \_\_\_\_\_ das strategische Umfeld eines Unternehmens,
- \_\_\_\_\_ das Einbeziehen aller Beteiligten und
- \_\_\_\_\_ ausreichende und geeignete Werkzeuge zur Datensammlung und Datenanalyse.

Der Prozess der Kennzahlenentwicklung läuft als zweiter Aktionspfad parallel zur Analyse eines bestehenden und im ersten Plan-Do-Check-Act-(PCDA)-Durchgang etablierten ISMS (vgl. Abb. 2) – diese Analyse liefert Vorgaben dafür, welche Soll-Ziele und -Zahlen für das ISMS erreicht werden sollen. Grundlage für die Definition sinnvoller Soll-Werte ist naturgemäß das Wissen um die Ziele des ISMS selbst – dementsprechend intensiv sollte man sich daher Gedanken gemacht haben, was man eigentlich mit dem ISMS erreichen will.

Ideale Eingabevariablen für die Kennzahlenentwicklung sind zum Beispiel die Berichte interner ISMS-Audits. Hieraus und aus den Ergebnissen von Korrektur- und Vorbeugemaßnahmen lässt sich entnehmen, wie sich das ISMS entwickelt – und daraus lassen sich entsprechende Kennzahlen ableiten.

Tabelle 1:  
Beispiele für  
Kennzahlen

| Kennzahl                      | Ziel                                                                                                     | Dimension       | Beschreibung                                                                                                                                                                                                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security-Budget               | Sicherstellen einer ausreichenden Finanzierung der Informationssicherheit                                | Systemrelevanz  | Diese Kennzahl misst den Anteil des Budgets für Informationssicherheit vom gesamten IT-Budget. Es gilt zur Interpretation generell: Je höher das Budget desto höher die Wahrscheinlichkeit erfolgreicher Sicherheitsbestrebungen. Generell ist die genaue Zielzahl organisationsabhängig. |
| Zugriffskontrolle             | Begrenzen des Zugriffs auf verfügbare Informationen nur für berechnigte Mitarbeiterinnen und Mitarbeiter | Technikrelevanz | Diese Kennzahl misst die Anzahl der unautorisierten Zugriffsversuche in Relation zu den vorhandenen Zugriffspunkten. Ziel der Kennzahl sollte ein möglichst geringer Prozentsatz sein.                                                                                                    |
| Sensibilisierung und Schulung | Sicherstellen einer starken Durchdringung der Belegschaft mit Sensibilisierung und Schulung              | Risikorelevanz  | Diese Kennzahl misst den Anteil der geschulten und sensibilisierten Mitarbeiter am Gesamtmitarbeiterstamm, bereinigt um Fluktuationen. Sie gibt Aussage über den Erfolg der Sensibilisierung.                                                                                             |

Die zu definierenden Soll-Zahlen und -Ziele liefern gleichzeitig Verbesserungspotenzial für das ISMS und so wiederum die Zielvorgaben, wie sich die Kennzahlen entwickeln sollen (s. Abb. 2). Im Ergebnis entsteht mit sinnvollen Kennzahlen eine aussagekräftige Messstruktur des Erfolgs der Informationssicherheit.

Neben den bezeichneten Handlungssträngen und Umweltvariablen ist es zusätzlich wichtig, zu identifizieren, welche Rollen im Unternehmen an der Kennzahlenbildung beteiligt werden sollten. Die Herausforderung hierbei ist es, im Kopf der Wunschteilnehmer des Kennzahlenentwicklungsprogramms ein Umdenken hervorzurufen. Zumeist ignoriert die Managementebene nicht vollständig, dass Geschäft, ISMS, (IT-)Strategie und Geschäftsprozesse immer stärker konvergieren. Aber dennoch ist die Führungsebene von der Realität oft weit entfernt.

## Werkzeuge zur Steuerung

Nach der endgültigen Festlegung der Kennzahlen und -ziele besteht die nächste Aufgabe des Security-Managements darin, ein passendes Werkzeug zur Steuerung

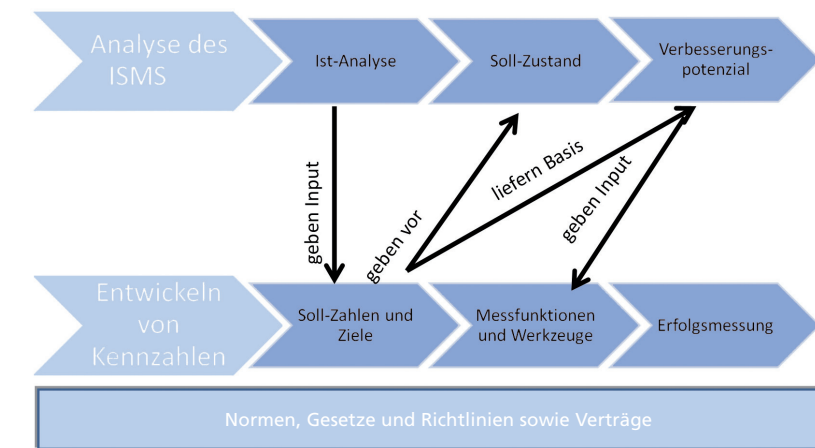


Abbildung 2: ISMS-Analyse und Kennzahlenentwicklung bilden parallele, aber stark verknüpfte Aktionspfade.

und Dokumentation dieser Kennzahlen zu entwickeln. Passend bedeutet dabei:

- \_\_\_\_\_ eine Dokumentation der Kennzahlen und Ziele im Zeitverlauf,
- \_\_\_\_\_ eine Visualisierung und Interpretation von Abhängigkeiten untereinander sowie
- \_\_\_\_\_ Möglichkeiten zu schaffen, Kennzahlen über mehrere Ebenen zu aggregieren.

Unabhängig von der technischen Umsetzung ist es notwendig, zunächst eine Methodik auszuwählen, der das Werkzeug folgen soll. Hierbei hat sich die Struktur einer „Balanced Scorecard“ als sinnvoll und anwendbar erwiesen. Abbil-

dung 3 zeigt eine beispielhafte Struktur einer solchen Balanced Scorecard.

Als ersten Schritt auf dem Weg zur passenden „Balance“ sollte das Management definieren, welche Ziele tatsächlich erreicht werden sollen. Hierzu erscheint auch eine Betrachtung der Umgebungsvariablen, in denen sich das Unternehmen bewegt, unumgänglich – so werden sich Ziele in Behörden anders darstellen, als Ziele in Unternehmen.

Danach ist es notwendig zwischen den Anforderungen des Geschäfts und den Zielen der Informationssicherheit eine Brücke zu schlagen. Hierzu ist es notwendig,

Abbildung 3:  
Mögliche Struktur  
einer Balanced  
Scorecard als grund-  
legende Methodik  
zur Dokumentation  
von Kennzahlen.

| Systemrelevante Komponenten |      | Technische Komponenten          |      |
|-----------------------------|------|---------------------------------|------|
| Kennzahl S.1                | Ziel | Kennzahl T.1                    | Ziel |
| Kennzahl S.2                | Ziel | Kennzahl T.2                    | Ziel |
| Kennzahl S.3                | Ziel | Kennzahl T.3                    | Ziel |
| Risikorelevante Komponenten |      | Geschäftspolitische Komponenten |      |
| Kennzahl R.1                | Ziel | Kennzahl G.1                    | Ziel |
| Kennzahl R.2                | Ziel | Kennzahl G.2                    | Ziel |
| Kennzahl R.3                | Ziel | Kennzahl G.3                    | Ziel |

einen Blick auf die Zusammenhänge der unternehmerischen Disziplinen des Sicherheitsmanagements, des Geschäftsprozessmanagements und der IT-Architektur zu werfen – Abbildung 4 stellt die Abhängigkeiten dieser Disziplinen untereinander grafisch dar.

Auffällig ist hierbei, dass sich diese drei Disziplinen auf verschiedene Wege gegenseitig bedingen. So ähnlich verhält es sich auch mit den beschriebenen Dimensionen der Kennzahlen zur Erfolgsmessung: Sie hängen voneinander ab und eine geschickte Auswahl ermöglicht es direkt nachzuweisen, welche Auswirkungen bestimmte Entscheidungen auf den Erfolg eines ISMS haben können. Auf Basis dieser Zusammenhänge kann man letztlich für die definierten Kennzahlen entsprechende Zielwerte festlegen, die dann in der Balanced Scorecard festgelegt werden (vgl. Abb. 3).

Der Vorteil des Balanced-Scorecard-Modells liegt in dieser Anwendung vor allem darin, mehrere

Dimensionen von Kennzahlen in einer ausgewogenen und übersichtlichen Form darzustellen. Ferner ermöglicht es diese Darstellung, schnell Zusammenhänge zwischen Entscheidungen und Zielerreichung zu erfassen: Bleiben beispielsweise mehrere Kennzahlen über einen Zeitverlauf hinweg konstant, deutet dies darauf hin, dass diese Dimensionen nicht nur voneinander abhängig sind, sondern getroffene Entscheidungen mehrdimensionale Auswirkungen haben. So bedeutet zum Beispiel eine konstante Risikokennzahl bei konstantem Budget und steigender Erfüllung von Sicherheitszielen, dass die Mittel optimal eingesetzt werden.

Ein weiterer Vorteil der Scorecard-Darstellung ist die Möglichkeit, Messwerte auf verschiedenen Ebenen zu aggregieren. Daraus lassen sich dann wieder Rückschlüsse über die tatsächliche Wirksamkeit eines Managementsystems unterhalb des Top-Levels ziehen. Gerade in größeren Konzernen ist es sinnvoll, die Messverfahren auf die weiter unten in der Struktur angesiedelten Ebenen herunterzubrechen – erst dann liefert ein Kennzahlensystem Aussagen über die Funktionalität des ISMS unterhalb der Regelungsebene.

## Management ist gefordert

Generell ist das Management als Treiber und Sponsor gefor-

dert, Kennzahlen so zu definieren, dass damit eine Steuerung des Managementsystems möglich ist. Sofern man verhindern will, dass ein ISMS letztlich im Räderwerk versagt, ist es notwendig, strukturiert in jeden Bereich eines größeren Unternehmens hereinzuschauen und genau zu definieren, welche Faktoren Aufschluss über die Funktionsfähigkeit geben. Erst dann kann man durch verschiedene Aggregationsebenen ein Datenmodell entwickeln, dass eine Steuerung der Sicherheit so ermöglicht, dass gesetzte Ziele wirklich erreicht werden.

Sofern die Organisation, die eine ISMS betreibt, sich nicht konkret damit befasst,

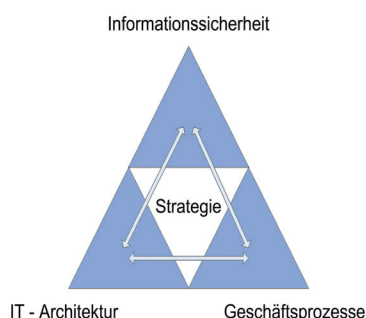
\_\_\_\_\_ was,  
\_\_\_\_\_ auf welchem Weg und  
\_\_\_\_\_ mit welchem Ressourceneinsatz

im ISMS erreicht werden soll, werden Kennzahlen immer nur dazu dienen, diejenigen Ergebnisse zu liefern, die man sehen möchte. Erst wenn die oben beschriebenen Anforderungen durch das Top-Management als Hauptunterstützer erfüllt werden, wird es möglich sein, objektivere Aussagen zu treffen – erst wenn diese Basis gelegt ist, besteht die Chance, die Wirksamkeit eines ISMS wirklich sinnvoll zu messen.

Erforderlich hierfür ist es, in einem weiteren Schritt festzulegen, welche Reifegrade mit welcher Kennzahl korrelieren: Der Reifegrad bezeichnet dabei die erzielte Durchdringung der Organisation mit „lebendiger“ Informationssicherheit. Damit geht das Modell des Reifegrades weit über die reine Auswertung angewandeter Controls oder umgesetzter Maßnahmen hinaus.

Allerdings ist es schwierig, diesen Reifegrad wie in einem Governance-Modell zu standardisieren – dafür ist die Kalibrierungsgrundlage der Informationssicherheit viel zu stark abhängig vom individuellen Risikokontext der betrachteten Or-

Abbildung 4:  
Zusammenhang  
verschiedener  
Management-  
Disziplinen



ganisation. Daher kann an dieser Stelle auch keine weitere Vertiefung und Definition allgemein gültiger Reifegradstufen erfolgen.

## Fazit

Die kennzahlenbasierte Steuerung von Managementsystemen ist eine Herausforderung auf allen Ebenen eines Unternehmens. Ein solches Projekt betrifft nicht nur Security-Manager, sondern auch Controller und Führungskräfte. Nur wenn alle Ebenen an der Zieldefinition beteiligt werden, ist es möglich, eine Steuerungsmöglichkeit zu entwickeln, die sinnvolle Ergebnisse liefert. Und erst wenn das Management Klarheit darüber gewonnen hat, welchen Reifegrad das ISMS im Gesamtkontext des Geschäfts erreichen soll, kann dann eine regelmäßige Verbesserung erfolgreich und zielgerichtet umgesetzt werden. ■

*Frederik Humpert-Vrielink ist ISO-27001-Auditor und Handlungsbevollmächtigter der CETUS Consulting GmbH.*

## Literatur

[1] International Organization for Standardization (ISO), Information technology – Security techniques – Information security management – Measurement, ISO/IEC 27004:2009, erhältlich u. a. über [www.iso.org/iso/store.htm](http://www.iso.org/iso/store.htm)

[2] National Institute of Standards and Technology (NIST), Performance Measurement Guide for Information Security, NIST SP 800-55, Revision 1, Juli 2008, PDF-Download über <http://csrc.nist.gov/publications/PubsSPs.html>