Den Erfolg von Sicherheitsmaßnahmen messen – Ein Praxisansatz

Nadine Nagel[1] · Svilen Ivanov[2] · Ralf Schumann[2]

[1]BWI Systeme GmbH
nadine.nagel@bwi-systeme.de

[2]rt-solutions.de GmbH
schumann@rt-solutions.de

Zusammenfassung

Die Bedeutung von IT-Sicherheit in Unternehmen hat in letzter Zeit ein neues Niveau erreicht. Gerade bei dem gestiegenen Bewusstsein in der Unternehmensleitung sind IT-Sicherheitsbeauftragte aufgefordert darzulegen, wie die Lage der IT-Sicherheit im Unternehmen ist und wie effektiv und effizient Investitionen in die IT-Sicherheit sind. Ein IT-Sicherheitskennzahlensystem trägt dazu bei, Investitionen zu rechtfertigen und die Wirksamkeit von Maßnahmen zu evaluieren. Es schafft damit ein nachvollziehbares Informations- und Kontrollsystem. In der Praxis zeigt sich jedoch, dass Kennzahlen nur selten erhoben werden und dass die erhobenen Kenngrößen oft wenig aussagekräftig hinsichtlich der Wirksamkeit umgesetzter Maßnahmen sind – auch die Aggregation zu einem Gesamtbild fehlt häufig. In diesem Beitrag wird anhand eines Praxisbeispiels verdeutlicht, welche Schritte notwendig sind, um ein aussagekräftiges IT-Sicherheitskennzahlensystem zu entwickeln und zu implementieren.

1. Kontext von IT-Sicherheitskennzahlen

1.1 Gründe für Kennzahlen in der IT-Sicherheit

Im Tagesgeschäft eines Sicherheitsbereiches kommen strategische Themen sowie das Reflektieren der Effektivität und Effizienz von Maßnahmen oftmals zu kurz. Dabei ist die kontinuierliche Verbesserung – technisch und prozessual – elementar. „Was du nicht messen kannst, kannst du nicht lenken“ (Peter Drucker) – dies gilt auch für die IT-Sicherheit. Gerade um Investitionen in die IT-Sicherheit gegenüber vorgesetzten Stellen zu rechtfertigen und sowohl Schwachstellen darzulegen als auch die Effektivität von Maßnahmen zu evaluieren, leisten Kennzahlensysteme einen wichtigen Beitrag [Hayd10], [Kütz11], [Parm07].

1.2 Ziele (intern/extern) von Kennzahlensystemen

Häufig werden erhobene Kennzahlen in der IT-Sicherheit nicht zu einem Gesamtbild aggregiert. Doch gerade das Evaluieren – also das Überprüfen und Überwachen – von Maßnahmen in Bezug auf ihre Umsetzung, Wirksamkeit und Effizienz kann durch Kennzahlen geleistet werden. Kennzahlen dienen dazu, die Komplexität in der IT-Sicherheit zu beherrschen, eine

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 212-221.

Risikolage zu beurteilen und die Realisierung von IT-Sicherheitsmaßnahmen unter Berücksichtigung von IT-Sicherheitsmaßstäben zu steuern.

1.3 Ansätze zur Entwicklung von Kennzahlensystemen

Der BSI-Grundschutzkatalog und die ISO 27004 sind etablierte Grundlagen, um ein IT-Sicherheitskennzahlensystem zu realisieren. In dem Praxisbeispiel wurden in einem Vorprojekt die Sicherheitsmanagementprozesse auf Basis des BSI-Grundschutzkatalogs überprüft. Die Leitfrage dabei war, ob die vom BSI empfohlenen Maßnahmen umgesetzt waren. Dieser Frage wurde analog zu einem Basis-Sicherheitscheck bzw. zu einer ISO 27001 Zertifizierung nachgegangen. Die Ergebnisse des Vorprojekts zeigten, dass verschiedene Sicherheitskennzahlen mit sehr unterschiedlichem Aussagegehalt erfasst wurden. So wurden bspw. für Compliance und Rechenzentrumsbetrieb zwar Kennzahlen erhoben, aber die Konsolidierung zu einem Gesamtbild fehlte. Zudem wurden mit Kennzahlen oftmals operative Ergebnisse, wie die Anzahl der gepatchten Systeme, aber weniger die Effektivität oder gar Effizienz von (Sicherheits-) Maßnahmen erfasst. Dies war die Ausgangssituation für ein Projekt zur „Entwicklung eines IT-Sicherheitskennzahlensystems“.

2. Praxisbeispiel: Kennzahlensystem IT-Sicherheit

Anhand eines Praxisbeispiels wird dargestellt, in welchen Schritten ein IT-Sicherheitskennzahlensystem entwickelt und aufgebaut werden kann, das die Ziele „Messung der Effektivität von Maßnahmen“, „Bewertung der Prozesse“ und „Aggregation zu einem Gesamtbild“ verfolgt. Dabei wird auf die verschiedenen Phasen zur Entwicklung des IT-Sicherheitskennzahlensystems eingegangen.

2.1 Festlegung Projektziel

In dem Projekt sollten die vorhandenen Sicherheitskennzahlen bezüglich ihrer Steuerungswirkung überprüft und optimiert werden und bei Bedarf zusätzliche aussagekräftige Kennzahlen auf Basis der vorherigen Prüfung gegenüber BSI-Grundschutz entwickelt werden. Kennzahlen aus den vorhandenen unterschiedlichen Reporting-Quellen waren in eine übersichtliche, einheitliche und aussagekräftige Darstellungsform zu integrieren. Das regelmäßige Reporting sollte der kontinuierlichen Verbesserung der Sicherheitsprozesse dienen. Zur Umsetzung des Projektes wurde dieses in die Phasen „Grobkonzept“, „Feinkonzept“ und „Implementierung“ unterteilt.

2.2 Grobkonzept: Risikoszenarien und Kennzahlen

In der Phase „Grobkonzept“ wurden geeignete Kennzahlen identifiziert und hinsichtlich ihrer Akzeptanz und Steuerungswirkung sowie ihrer Effizienz und Umsetzbarkeit (Erhebbarkeit) ausgewertet.

Der erste Prozessschritt zur Einführung der kennzahlenbasierten Steuerung ist ein kombinierter Top-Down- und Bottom-Up-Ansatz, der in Abbildung 1veranschaulicht wird. Die Top-Down-Richtung ist entscheidend für die Qualität der Kennzahlen und der primäre Ansatz, um die aus Steuerungssicht grundsätzlich am sinnvollsten erscheinenden Kennzahlen zu identifizieren. Die Bottom-Up-Analyse stellt zu einem frühen Zeitpunkt sicher, dass die Quellen der Kennzahlen

mit angemessenem Aufwand erschlossen werden können. Dieser Ansatz erhöht die Wahrscheinlichkeit einer fundierten und gleichzeitig praxistauglichen, umsetzbaren Lösung.

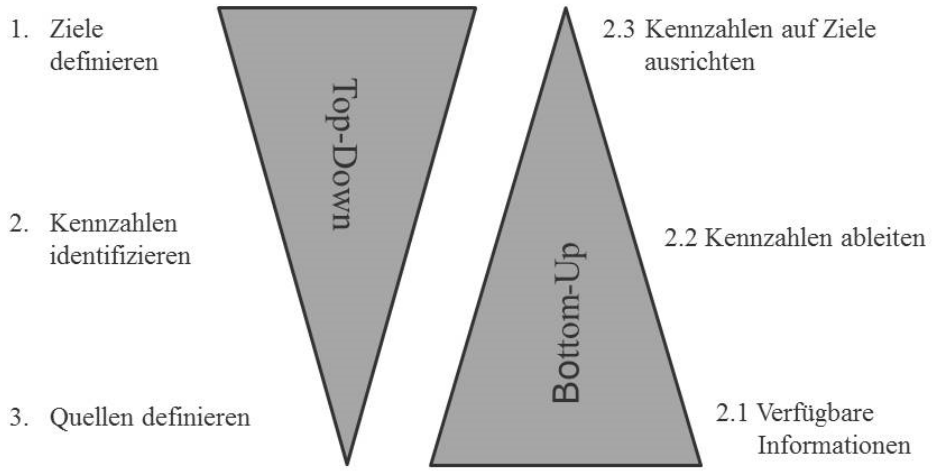

Abb. 1: Kombinierter Top-Down- und Bottom-Up-Ansatz

2.2.1 Definition von Risikoszenarien

In Top-Down-Richtung werden zunächst die relevanten Steuerungsziele und Entscheidungsträger identifiziert. Im Anschluss erfolgen die Definition der Kennzahlen und die Festlegung der Quellen. Zunächst muss beantwortet werden, was gesteuert wird und welche Ziele damit verfolgt werden.

Dabei wurde der Steuerungsgegenstand der in diesem Beispiel besonders relevanten Bereiche anhand ausgewählter Risikoszenarien für bestehende und neue Kennzahlen festgelegt. Diese Risikoszenarien setzen sich zusammen aus relevanten Informationswertklassen, Gefährdungen, potentiellem Schadensausmaß und Kontrollmaßnahmen, die einen Steuerungsgegenstand für das Kennzahlensystem beschreiben, wie z.B. Datenabfluss, Umgang mit Berechtigungen, Schadcode-Befall für Arbeitsplatzrechner sowie Server-Systeme. Die Abhängigkeiten der Elemente werden in Abbildung 2 dargestellt, können aber nur für konkrete Risikoszenarien analysiert werden.

Die Elemente eines Risikoszenarios und deren Abhängigkeiten untereinander werden anhand des in Tabelle 1 dargestellten Beispiels für die Definition des Risikoszenarios „Arbeitsplatzrechner“ erklärt. Gefährdungen (Angreifer, Schadcode) nutzen die Schwachstellen (unzureichende Patch-Stände) von Informationswerten (Arbeitsplatzrechner) aus, um Schaden (Ausfall) anzurichten. Die Maßnahmen (siehe Tabelle 1) werden eingesetzt, um die Schwachstellen zu schließen. Damit sind Maßnahmen und Schwachstellen zwei Seiten derselben Medaille. Die drei Komponenten „Gefährdungen“, „Schwachstellen/nicht umgesetzte Maßnahmen“ und „Informationswerte“ bilden Risiken (potentieller Schaden). Die Risiken können sich in Vorfällen manifestieren (tatsächlicher Schaden).

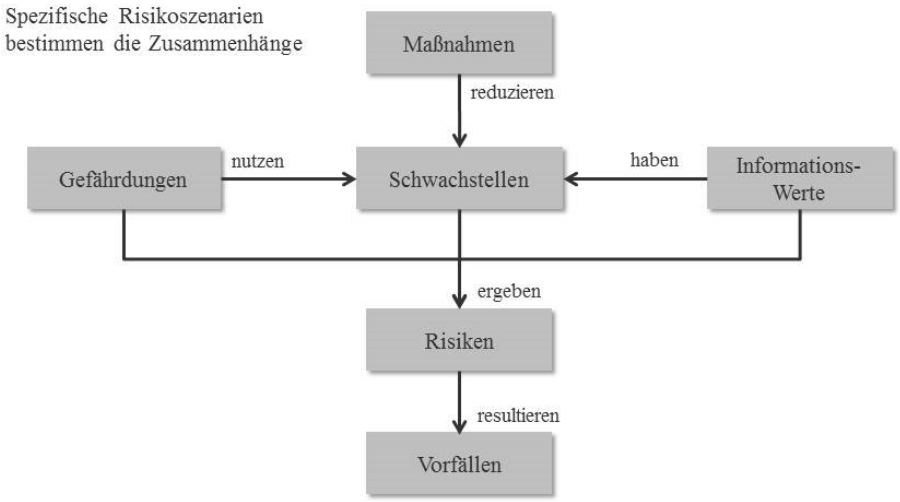

Abb. 2: Allgemeine Abhängigkeiten eines Risikoszenarios

Es wurden zunächst Risikoszenarien in den Bereichen „Server“, „Arbeitsplatzrechner“ und „Informationssicherheitsmanagement“ betrachtet.

Tab. 1: Beispiel Risikoszenario „Arbeitsplatzrechner“

Risikoszenario	Schadcode-Befall für Arbeitsplatzrechner
Informationswerte	• Alle Arbeitsplatzrechner
Gefährdungen	• Alle Schadcode-Typen (z.B. Virus, Spyware)
Potentieller Schaden	• Ausfall von Arbeitsplatzrechnern
Maßnahmen/ Schwachstellen	• Personen: Mitarbeiterschulung und -verpflichtung • Prozesse: Patch-Management • Technik: Antivirus-Software
Risiken	• Unsichere Version eines Browsers ist ausgerollt und kann nicht aktualisiert werden wegen einer Applikationsabhängigkeit
Vorfälle	• Ausfall hoher Anzahl von Arbeitsplatzrechnern wegen Schadcode-Infektion

2.2.2 Kennzahlen und deren Dokumentation

Für die definierten Szenarien wurden in einem nächsten Schritt jeweils fünf bis zehn relevante Kennzahlen definiert und hinsichtlich ihrer Steuerungswirkung und Wirtschaftlichkeit bewertet. Hierzu wurde ein Kennzahlensteckbrief mit wesentlichen Attributen, wie beispielsweise Kategorie, Maßnahme, Bezeichnung, Beschreibung, Bewertungsschema, Analysedimensionen und Quellsystem pro Kennzahl erstellt. Tabelle 2 listet die Kennzahlen für das Risikoszenario „Arbeitsplatzrechner“ auf. Die Kennzahlen-Kategorien bilden dabei die Kernelemente der Risikoszenarien und deren Zusammenhänge ab.

Tab. 2: Beispielkennzahlen für das Risikoszenario „Arbeitsplatzrechner (APC)“

	Kennzahlen-Kategorie			
	Abdeckungs-grad	Umsetzungsgrad	Externer Risikoeinflussfaktor	Effektivität
Beispielkenn-zahlen	% betrachtete Client-Sys-teme	% gepatchte Client-Systeme % Client-Systeme mit aktuellem Virenschutz % Client-Systeme mit ordnungsgemäßer Software % geschulte Mitarbeiter % der rechtzeitig behobenen Schwach-stellen für APC	Schwachstellenlevel für die Warenkorb-Software Gefährdungslevel für Schadcode	# Sicherheits-vorfälle mit Client-Systemen # Risiken mit Client-Systemen
Aussagekraft	Welcher As-set-Anteil ist im Kennzah-lensystem ab-gebildet und kann dadurch gesteuert wer-den?	Sind die Maßnahmen für die Assets korrekt umgesetzt worden?	Welches Gefahren-potential haben ex-terne nicht steuer-bare Risikofaktoren (z.B. Schwachstellen ohne Patch, Schadcode-Aktivi-tät)?	Zu welchem Ergebnis füh-ren die Sicher-heitsmaß-nahmen?

Zur Identifikation der Kennzahlen wurde – wie beschrieben – ein kombinierter Top-down- und Bottom-Up-Ansatz verwendet:

Top-Down: Erarbeitung von Kennzahlen, die die Kernelemente der Risikoszenarien abbilden.

Bottom-Up: Identifikation der Quellsysteme für die Datenerhebung auf Basis des Wissens und der Erfahrung der Projektbeteiligten im Unternehmen.

Tabelle 3 gibt ein Beispiel für die Kennzahlendefinition.

Tab. 3: Beispiel Kennzahlendefinition

Kennzahl	Anteil der rechtzeitig behobenen Schwachstellen	
Kategorie	Umsetzungsgrad der Kontrollmaßnahmen	
Maßnahme	Schwachstellen-Management-Prozess	
Beschreibung	Prozentualer Anteil der Schwachstellen, für die die Maßnahmen zur Behebung rechtzeitig umgesetzt wurden.	
Berechnungs-schema	• X = A / B * 100 % • A: Anzahl der Schwachstellen aus der Menge „B“, für die die Maßnahmen bis zum Zieltermin umgesetzt sind. • B: Anzahl der Schwachstellen, für die der Zieltermin für die Maßnahmenumsetzung im betrachteten Zeitraum liegt.	
Bewertungs-schema	Geringes Risiko (grün)	Kennzahlenwert = 100 % für Schwachstellen mit Kritikalität Hoch UND Kennzahlenwert > 90 % für Schwachstellen mit Kritikalität Mittel
	Mittleres Risiko (gelb)	Voraussetzungen für geringes Risiko und hohes Risiko treffen nicht zu
	Hohes Risiko (rot)	Kennzahlenwert < 90 % für Schwachstellen mit Kritikalität Hoch ODER Kennzahlenwert < 75 % für Schwachstellen mit Kritikalität Mittel
Analyse-dimensio-nen	Zeit, Schwachstellen-Kritikalität, Schwachstellen-Verantwortliche, Schwachstellen-Maßnahmenbereich, Informationswertekategorie (Arbeitsplatzrechner, Server).	
Adressat	IT-Sicherheitsbeauftragter	
Zweck	Sicherstellen, dass die Schwachstellen zeitnah behoben werden.	
Quellsysteme	Schwachstellen-Management-Datenbank	

2.3 Feinkonzept: Datenschnittstellen und Reporting

Um ein möglichst automatisiertes Kennzahlensystem zu entwickeln, ist es notwendig, die Datenschnittstellen von den Quellsystemen in das Kennzahlensystem zu definieren. Dabei ist zu überprüfen, ob die erforderlichen Daten in der notwendigen Qualität und Aktualität in den Quellsystemen vorliegen und wie diese exportiert werden können. Ziel ist es, ein automatisiertes System aufzubauen, das Daten in hoher Qualität und Aktualität liefert. Dieses ist die Basis des Berichtssystems. Hierzu wurden rund zehn unterschiedliche Quellsysteme betrachtet und auf die o.g. Punkte hin überprüft. Falls nicht alle Punkte durch die Quellsysteme erfüllt wurden, wurden die Kennzahlen ggf. unter Berücksichtigung ihrer Aussagekraft angepasst, um eine Erhebung und ein Reporting zu ermöglichen. Die Definition des Reporting-Systems (Architektur, Datenverarbeitung und Benutzerschnittstellen) ist ein wichtiger Bestandteil des Feinkonzeptes.

2.3.1 Kerninhalte des Feinkonzeptes

Bei der Erstellung des Feinkonzeptes haben sich einige Inhalte herauskristallisiert, deren Spezifikation von besonderer Bedeutung in der Praxis ist:

- **Datenschnittstellen:** Spezifikation, welche Daten in welchem Format aus welchen Quellsystemen wie exportiert und wie übertragen und in welcher Form gespeichert werden.
- **Systemarchitektur:** Spezifikation, welche Systemkomponente welche Funktionen erfüllt und wie diese zusammenhängen (siehe Abbildung 3).
- **Benutzerschnittstellen:** Spezifikation der Berichte für die Benutzerdarstellung der Kennzahlen in unterschiedlichen Aggregationsstufen und Analysedimensionen (siehe Abbildung 4).
- **Datenmodell:** Spezifikation, wie die Daten im Data Warehouse verarbeitet und gespeichert werden. Hierzu werden Standard Business Intelligence Werkzeuge verwendet [Kimb09].
- **Berechtigungssystem:** Spezifikation, wie die Berechtigungen in dem Kennzahlensystem verwaltet werden und welche Mitarbeiter welche Inhalte sichten dürfen. Es hat sich bewährt, das Berechtigungssystem an der Organisationsstruktur zu orientieren und die entsprechenden Daten (z.B. Mitarbeiter- und Kostenstellen-Hierarchie) des Unternehmens im Kennzahlensystem abzubilden.

Die Systemarchitektur ist nach dem Standard-Business-Intelligence-Ansatz in mehreren Schichten aufgebaut. Die produktiven Quellsysteme in Verantwortung des Systembetreibers bilden die unterste Schicht. Die Daten aus den Quellsystemen werden in eine zentrale Pre-Staging-Datenbank exportiert. Das Kennzahlensystem umfasst mehrere Schichten für die Datenverarbeitung:

- Datenintegration: Zusammenfassung und Normierung der Daten aus unterschiedlichen Datenquellen.
- Data Warehouse (DWH): Speicherung der Daten.
- Analytische Datenverarbeitung (OLAP): Verarbeitung der im DWH gespeicherten Daten für eine performante und mehrdimensionale Analyse.
- Berichtswesen: Darstellung der Daten in Form von vordefinierten Web-Berichten.

Die Benutzer haben zwei Möglichkeiten für den Zugriff auf die Kennzahlen: Web-Reporting für Standard-Nutzer und Datenanalyse auf OLAP-Ebene für fortgeschrittene Nutzer.

Aus dieser Systemarchitektur ergeben sich verschiedene Vorteile:

- Einsatz von Standard-Business-Intelligence-Werkzeugen.
- Klare Trennung der Verantwortlichkeiten zwischen Datenbereitstellung (IT Service Provider) und Kennzahlensystem (IT-Leitung).
- Export aller Daten in einheitlichem Format (SQL) und zentral im Pre-Staging-Bereich für die Weiterverarbeitung durch das Kennzahlensystem. Dies vereinfacht den Datenimport und minimiert operative Risiken.

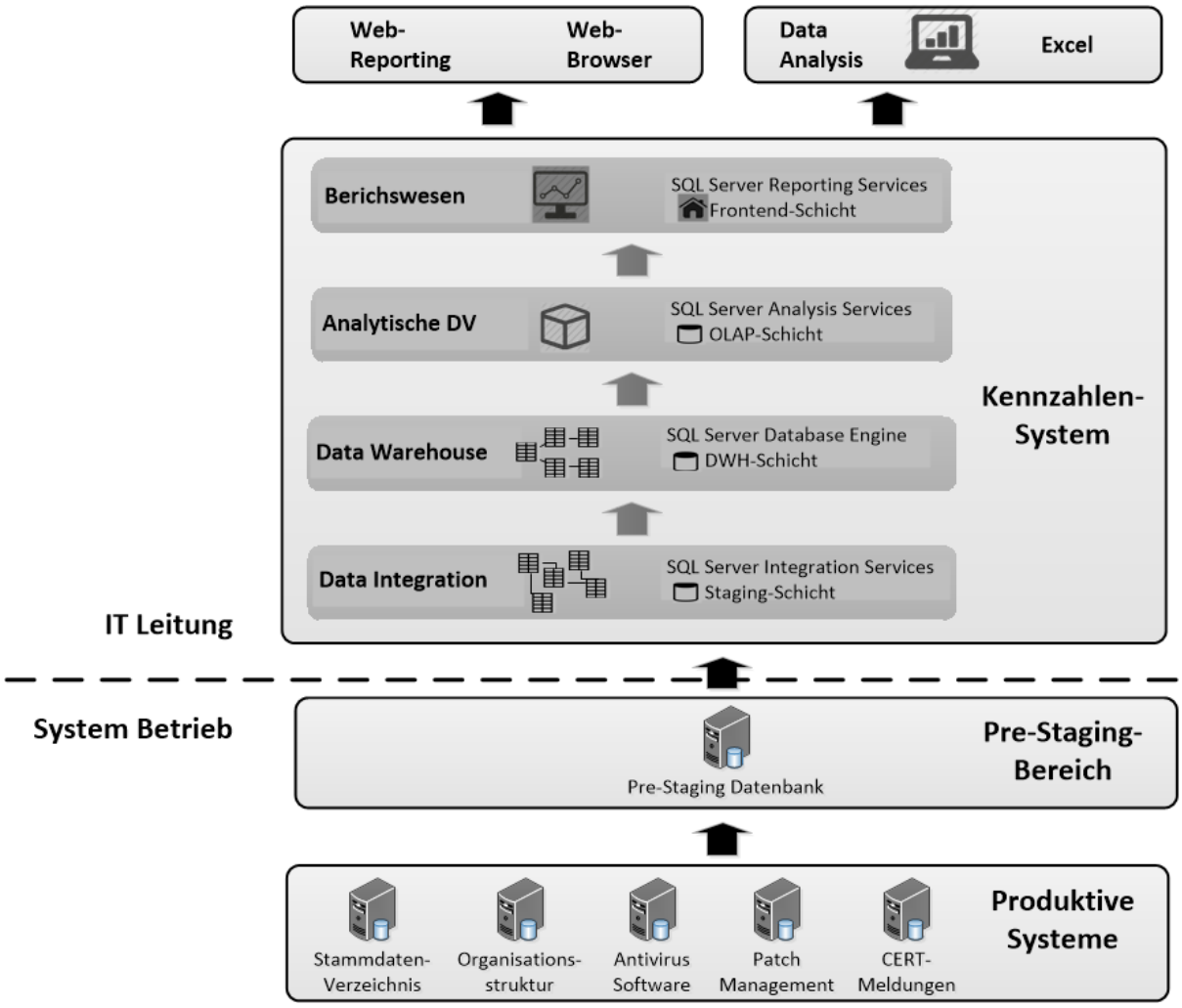

Abb. 3: Auszug aus der Systemarchitektur

2.3.2 Darstellung der Kennzahlen

Für die Darstellung der Kennzahlen für die Benutzer ist es wichtig, neben den Schwellwerten auch zu definieren, nach welchen Analysedimensionen die Kennzahlen dargestellt werden sollten. Die Analysedimensionen sollten so gewählt sein, dass die Benutzer die Möglichkeit haben, auf die Frage „Woran liegt es?“ eine Antwort zu bekommen. In dem in Abbildung 4 dargestellten Beispiel ist ersichtlich, dass die Probleme mit fehlenden Patches vermehrt bei kundenbetriebenen Systemen auftreten und dass Java, Adobe Acrobat und Adobe Flashplayer erheblich vom Zielwert abweichen. Als weitere Detaillierungsstufe empfiehlt sich eine Systemliste mit dem entsprechenden Status. Damit können die Benutzer die Probleme gezielt angehen.

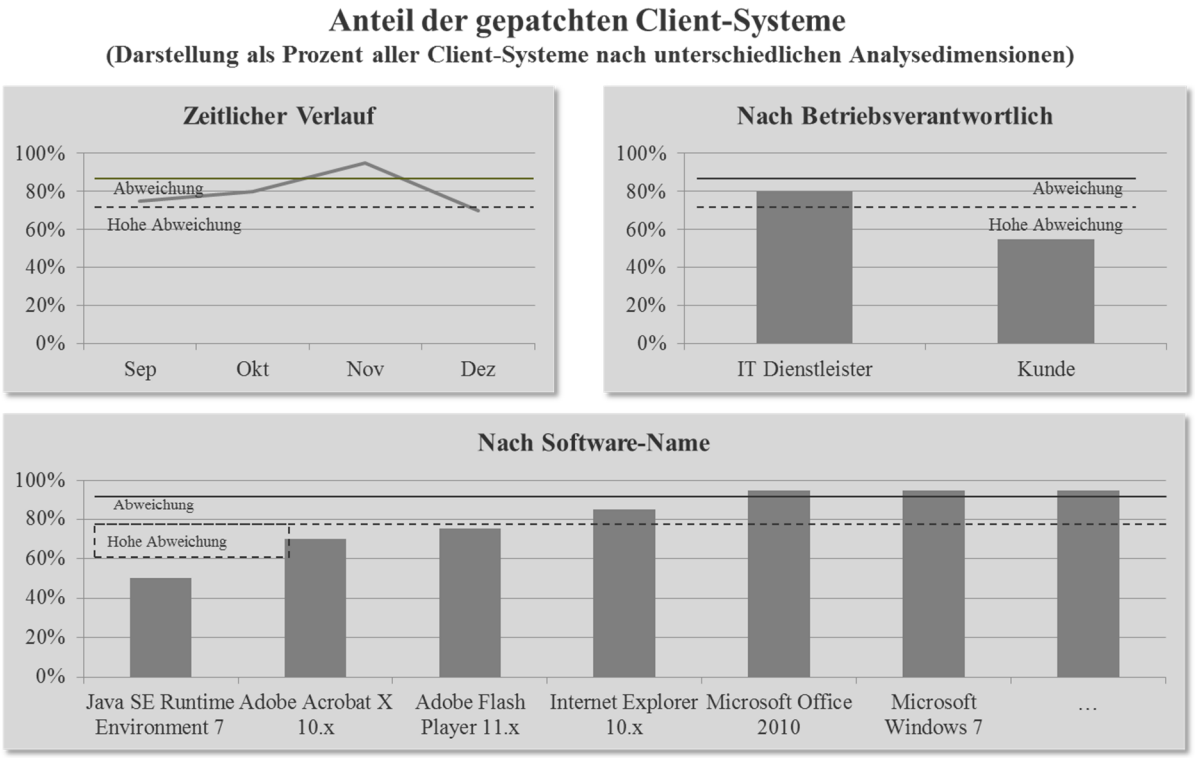

Abb. 4: Visualisierungsmöglichkeit für die Kennzahl „Gepatchte Client-Systeme [%]“

2.4 Implementierung

Die Implementierung beinhaltet die Einführung des fertigen Reporting-Systems für die ausgewählten Risikoszenarien und Kennzahlen zur Bewertung und Steuerung der Informationssicherheit. Dabei untergliederte sich die “Implementierung“ in die Arbeitsschritte „Prototyp“, „Umsetzung und Test“ sowie „Einführung“. Eine wichtige Rahmenbedingung bei der Implementierung war die Forderung nach der Anpassbarkeit der Risikoszenarien und Kennzahlen, um auf neue Entwicklungen und geänderte Rahmenbedingungen flexibel und zeitnah reagieren zu können.

3. Fazit „Entwicklung Sicherheitskennzahlensystem“

Dieser praxisorientierte Beitrag stellt ein unternehmensneutrales Projektvorgehenskonzept für die Einführung eines Sicherheitskennzahlensystems vor. Somit können andere Unternehmen bei ähnlichen Fragestellungen von den Projekterfahrungen profitieren. Im Laufe des Projekts zeichneten sich verschiedene Faktoren ab, die für die Einführung eines solchen Kennzahlensystems von Bedeutung waren:

- Damit das Projekt erfolgreich sein kann und unterstützt wird, muss das Bewusstsein für Kennzahlen in der IT-Sicherheit bei den beteiligten Akteuren und den angrenzenden Bereichen geschaffen werden. Vor allem sollte der Mehrwert auch für angrenzende Bereiche transparent sein. Nur so kann die notwendige Unterstützung erreicht werden.
- Um die Kennzahlen sinnvoll für die Steuerung der IT-Sicherheit und das Treffen von risikobasierten Entscheidungen im Unternehmen einsetzen zu können, müssen sie die komplexen Abhängigkeiten zwischen Informationswerten, Bedrohungslage, potentiellem

Schadensausmaß und eingesetzten Sicherheitsmaßnahmen realistisch abbilden. Dies wurde erreicht, indem der Steuerungsgegenstand des Kennzahlensystems in Form von Risikoszenarien definiert wurde und die Kennzahlen die wesentlichen Elemente daraus darstellten.

- Um sich nicht in der Komplexität eines allumfassenden Kennzahlensystems zu verlieren, hat es sich bewährt, mit einem eng abgesteckten Umfang, z.B. 3 Risikoszenarien und max. 15 Kennzahlen zu beginnen. Dies sichert den Verantwortlichen zeitnahe Projektresultate und bildet eine gute Basis für einen sukzessiven Ausbau des Kennzahlensystems.
- Ein kombinierter Top-Down- und Bottom-Up-Ansatz hat dazu beigetragen, dass die Kennzahlen eine hohe Steuerungswirkung haben und wirtschaftlich erhoben werden können. Die Bottom-Up-Betrachtung wurde frühzeitig im Grobkonzept durchgeführt. Das heißt: es wurden möglichst automatisiert erhebbare und mit vertretbarem Aufwand messbare Kennzahlen gewählt, um a) die Akzeptanz des Systems zu sichern, b) die Aktualität der Kennzahlen zu gewährleisten und c) das System nicht zu einem zusätzlichen Aufwand werden zu lassen.
- Bereits bei der Konzeption des Kennzahlensystems wurde auf eine variable Gestaltung Wert gelegt, so dass Anpassungen und Erweiterungen (z.B. weitere Risikoszenarien, weitere Kennzahlen, Übertragung der Kennzahlen auf andere Organisationseinheiten) möglich sind.
- Um einen schnellen Projektstart zu ermöglichen, wurden bereits erfasste Kennzahlen zur Orientierung herangezogen und ausgewertet. Wo es für das Gesamtbild erforderlich war, wurden neue Kennzahlen definiert und erfasst.
- Die Kennzahlen wurden definiert, implementiert und werden regelmäßig berichtet, d.h. für die regelmäßige Bewertung und Verbesserung der IT-Sicherheit im Unternehmen eingesetzt.

Mit der Etablierung der Infrastruktur für die automatisierte Erfassung von Sicherheitskennzahlen wurde die Basis geschaffen, bisher unabhängig voneinander erstellte oder noch gar nicht erfasste Kennzahlen automatisiert zu einem Gesamtbild zusammenzuführen und somit den Sicherheitsmanagementprozess – operativ wie auch strategisch – fundierter steuern zu können.

Literatur

[Hayd10] Lance Hayden. IT Security Metrics. McGrawHill. 2010.

[Kimb09] R. Kimball, M. Ross, W. Thorthwaite, B. Becker, J.Mundy. The data warehouse lifecycle toolkit – expert methods for designing, developing & deploying data warehouse. s.l. : Wiley-India, 2009. 8126516895.

[Kütz11] M. Kütz. Kennzahlen in der IT. Dpunkt.verlag. 2011.

[Parm07] D. Parmenter. Key Performance Indicators: Developing, Implementing, and Using Winning KPIs. John Wiley & Sons, Inc. 2007.