

Was zahlen eigentlich die anderen?

Wie viel darf IT-Sicherheit kosten? Diese Frage beschäftigt Management und Sicherheitsverantwortliche in Unternehmen in Zeiten knapper Budgets ganz besonders. Im Gegensatz zu klassischen Investitionsprojekten ist das **Verhältnis von Kosten und Nutzen** für IT-Sicherungsmaßnahmen aber nur schwer ermittelbar. Hoch im Kurs stehen deshalb Methoden, die eine eigene Positionsbestimmung ermöglichen. Aber gibt es einen solchen Heilsbringer?

Von Gunnar Haderthauer und Friedrich Hueber



IT-Sicherheitsverantwortliche sind in einem permanenten Dilemma: Sie sollen das Unternehmen wirksam vor Angriffen von innen und außen schützen, die Kosten dafür aber möglichst gering halten. Wenn aber nichts passiert, haben CIOs bei ihren Budgetforderungen oft ein Vermittlungsproblem gegenüber ihrer Geschäftsführung.

Entscheidend ist ein nachvollziehbares Verhältnis von Nutzen und Kosten der Sicherheitsmaßnahmen. Doch wie viel Sicherheit braucht man, um sicher genug zu sein? Und wie kann ein Chief Information Security Officer (CISO) seinen Etatansatz rational begründen, wenn eine Bedrohungslage für das eigene Unternehmen nicht schwarz auf weiß nachweisbar ist? Hier hilft eine fundierte Analyse der Kosten und der Notwendigkeit von IT-Sicherheitsmaßnahmen.

Das aber ist leichter gesagt als getan. Denn Praktiker wissen, dass klassische Busi-

ness-Cases mit Break-even-Zeitpunkten und Return-of-Investment-Berechnungen wenig hilfreiche Aussagen für die Planung der IT-Sicherheit bieten. Diese Werkzeuge sind nützlich, wenn bereits eine Strategie ausgearbeitet ist und daraus einzelne Maßnahmen abgeleitet sind. Die zentrale Frage vorher lautet, wie man die richtige Strategie und erfolgreiche Maßnahmen für das eigene Unternehmen findet. Nicht weniger interessant ist die meist im gleichen Atemzug gestellte Nachfrage, was die Umsetzung der geplanten Maßnahmen kostet. Hierauf findet sich mit den aus dem IT-Management bekannten betriebswirtschaftlichen Methoden keine Antwort. Oder doch?

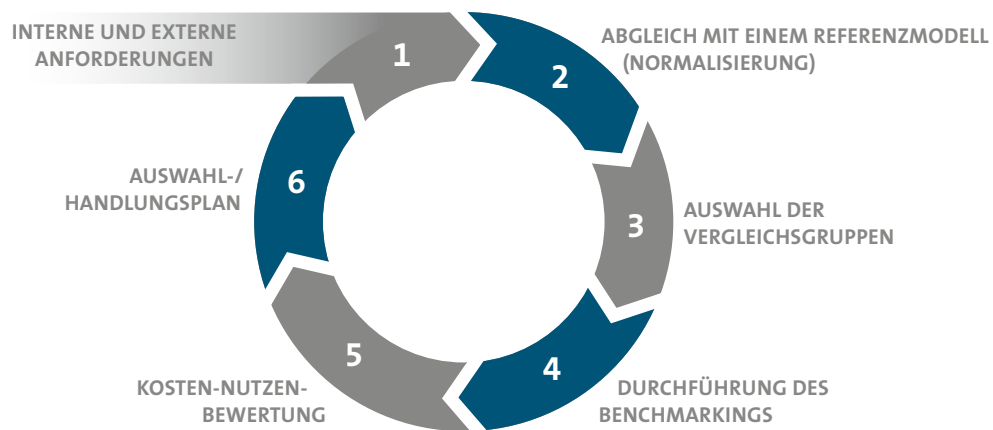
Zunehmend setzt sich das Benchmarking zur Ermittlung marktgerechter Preise auch für die IT-Sicherheit durch. Jenseits unseriöser Anbieter liefert diese Methode bei detaillierter Betrachtung interessante Ergeb-



Der Autor **Friedrich Hueber** ist Junior Consultant bei LEXTA. Er studierte an der TU Berlin Wirtschaftsingenieurwesen mit der Fachrichtung Informations- und Kommunikationssysteme. Bereits während seines Studiums sammelte er erste Erfahrungen in der IT-Beratung mit den Schwerpunkten IT-Sicherheit und IT-Service-Management.



Der Autor **Gunnar Haderthauer** ist Partner bei LEXTA. Bei einem der größten weltweiten Automobilzulieferer gewann er Erfahrung im Betrieb hochverfügbarer Kommunikationssysteme und Rechenzentren und stieg aufgrund seines technischen Wissens sowie seiner Führungsqualitäten schnell zum Assistenten des CIO auf. Zuletzt verantwortete er beim deutschen Marktführer im Bereich Flugbuchungssysteme die Geschäftsführung.



Das Benchmarking gilt als geeignete Methode, um das Preis-Leistungs-Verhältnis von IT-Sicherheit zu ermitteln, zu messen und mit dem Wettbewerb zu vergleichen. Dabei unterteilt sich das Verfahren in sechs Stufen.

nisse zur eigenen Positionsbestimmung. Benchmarking ist ein geeignetes Verfahren, um das tatsächliche Kosten-Leistungs-Verhältnis von IT-Sicherheit objektiv zu messen und mit dem Wettbewerb zu vergleichen.

Ist-Situation erfassen

Wie funktioniert ein Benchmarking für die IT-Sicherheit? Zunächst werden die internen und externen Anforderungen der einzelnen Unternehmensbereiche und des Gesamtunternehmens an die IT-Sicherheit genau erfasst. Eine besondere Rolle spielen dabei Rahmenbedingungen wie Mengengerüste, Branchenspezifika und rechtliche Vorgaben. Sie bilden die Basis für die spätere Auswahl passender Vergleichsunternehmen. Die bisher erbrachten Leistungen werden erfasst und analysiert. Untersucht werden beispielsweise das Angebot an Diensten, deren Qualität und Umfang sowie die Servicelevel. Die ermittelten Rahmenbedingungen, Anforderungsparameter und aktuellen Maßnahmen werden umfassend dokumentiert.

Normalisierung erarbeiten

Der nächste Schritt besteht darin, die bis hierhin ermittelten Ergebnisse mit einem Referenzmodell abzugleichen. Das Referenzmodell muss hinsichtlich des Preis-Leistungs-Verhältnisses nicht zwangsläufig perfekt passen. Vielmehr dient es dazu, den Marktdurchschnitt widerzuspiegeln, sodass nur wenige Anpassungen notwendig sind. Ziel ist, möglichst detaillierte Aussagen zu erhalten, inwieweit die relevanten Einzelparameter vom Marktdurchschnitt abweichen.

Vergleichsgruppe auswählen

Zugegebenermaßen lassen sich die Anforderungen und Bedingungen eines modernen Telekommunikationsunternehmens nur sehr eingeschränkt mit denen eines Automobilzulieferers vergleichen. Deswegen kommt es für den nächsten Schritt darauf an, Unternehmen als »Sparringspartner« auszuwählen, die analoge Strukturen aufweisen. Denn nur wenn die zu betrachtenden Parameter möglichst wenig voneinander abweichen, sind die Analysen wirklich aufschlussreich.

Daten »benchmarken«

All diese vorbereitenden Aufgaben bilden die Grundlage des eigentlichen Benchmarkings. Dazu werden die herausgearbeiteten Diskrepanzen vom Marktdurchschnitt mit den Merkmalen der Unternehmen in der Vergleichsgruppe verglichen. Unterschiede werden erfasst und analysiert. Auf diese Weise lassen sich belastbare Aussagen dazu treffen, an welchen Stellen es zu Abweichungen kommt und welche Konsequenzen dies mit sich bringt.

Kosten bewerten und Handlungsplan erstellen

Liegt der Benchmark auf dem Tisch, der klar macht, ob das Unternehmen zu viel oder zu wenig Sicherheit »produziert«, kann eine umfassende Liste mit Maßnahmen zur Optimierung erstellt werden. Ab hier greifen dann auch im Bereich der IT-Sicherheit die klassischen betriebswirtschaftlichen Mechanismen. Nacheinander werden die einzelnen geplanten Maßnahmen systematisch nach

ihrem Nutzen bewertet, die Investitions- und Betriebskosten beurteilt und daraus ein Ranking der Maßnahmen abgeleitet. Zum Schluss folgt ein detaillierter Handlungsplan. Im Übrigen empfiehlt es sich, diese Analyse in regelmäßigen Abständen zu wiederholen.

Das Fazit: Eine einfache numerische Antwort, wie viel IT-Sicherheit kosten darf, gibt es also nicht. Mit Benchmarking kann aber sichergestellt werden, dass die eigenen IT-Sicherheitsmaßnahmen und deren Kosten sich in einem marktüblichen Rahmen bewegen. Und das gibt den CISOs sicher Munition für die nächsten Budgetverhandlungen mit der Geschäftsführung. ■

DAS SEMINAR

04

Marktgerechte IT-Preise ermitteln – IT-Benchmarking

INHALTE

Das Benchmarking gilt als geeignetes Verfahren, um marktgerechte Preise zu ermitteln. Das Seminar stellt die Theorie des IT-Benchmarkings vor und erläutert anhand von Praxisbeispielen die Vorgehensweise, mögliche Kennzahlen, die Ableitung eines Preismodells und typische Ergebnisse. Zudem werden den Teilnehmern die Steuerung der IT-Benchmarking in Projekten und das Applikationsbenchmarking erläutert.

REFERENT

Matthias Seidl

ORT

Bitkom Tagungszentrum, Albrechtstraße 10, 10117 Berlin

TERMIN

24. März 2010

PREIS (zzgl. USt.)

590,- EUR / 425,- EUR (BITKOM-Mitglieder)