IT-SICHERHEIT: ÖKONOMISCH PLANEN UND BEWERTEN

Heutige Ansätze zur Planung und Bewertung von IT-Sicherheitsmaßnahmen basieren oftmals auf Methoden der Investitionsrechnung, oder es kommen allgemeine Frameworks zum IT-Service-Management zum Einsatz. Bessere Möglichkeiten bietet der „Resource-based View" (RBV).

Cyberangriffe auf Firmen, öffentliche Einrichtungen und Privatpersonen haben in jüngster Zeit drastisch zugenommen, wie Angaben des Bitkom und des Bundesministeriums für Bildung und Forschung (BMBF) belegen. Angriffe auf IT-Systeme und insbesondere Cyberangriffe können die Betroffenen auf diverse Arten schädigen:

» Im industriellen Umfeld können Unterbrechungen von Produktionsprozessen zu ökonomischen Schäden in Form von Produktivitätseinbußen, entgangenem Gewinn und der Nichteinhaltung von vereinbarten Lieferterminen führen.

» Bei einer Cyberattacke auf den zweitgrößten US-Krankenversicherer Anthem Inc. im Jahr 2015 gelang Angreifern der Zugriff auf persönliche Daten (Name, Geburtsdatum, Adresse und Sozialversicherungsnummer) von ungefähr 80 Millionen Personen. Zwei Monate später meldete der US-Krankenversicherer Premera Blue Cross sogar den unautorisierten Zugriff auf medizinische Daten von über 11 Millionen Kunden. In solchen Fällen greift das US-amerikanische HIPAA-Gesetz (Health Insurance Portability and Accountability Act), das die Sicherheit von Patienteninformationen regelt und im Fall von Anthem Zivilklagen ermöglicht, da Sozialversicherungsnummern und Geburtstage unverschlüsselt gespeichert wurden.

Unternehmen reagieren auf wachsende Cybergefahren durch hohe Investitionen in technologische, organisatorische und personelle Sicherheitsmaßnahmen. 2014 wuchsen nach Angaben von Gartner die weltweiten Ausgaben für IT-Sicherheit um 7,9 Prozent im Vergleich zum Vorjahr auf 71,1 Milliarden US-Dollar. Damit versuchen Unternehmen nicht nur ökonomischem Schaden vorzubeugen, sondern sie müssen auch rechtliche und regulatorische Vorgaben implementieren (z.B. Sarbanes-Oxley Act und HIPAA im US-amerikanischen Raum, Basel III/Capital Requirements Directive im europäischen Raum).

Unternehmen sehen sich heute vielfältigen technologischen Cybergefahren ausgesetzt, deren Abwehr durch IT-Sicherheitsmaßnahmen im ökonomischen, organisatorischen und rechtlichen Kontext betrachtet und gemanagt werden muss. Das IT-Sicherheitsmanagement muss dabei sowohl planerische Anforderungen einschließlich des Risikomanagements („Ex ante"-Perspektive) als auch evaluationsbezogene Anforderungen („Ex

post"-Perspektive) umsetzen. Diese Anforderungen lassen sich in folgende zentrale Fragen kondensieren:

» Welche Assets einer Organisation bedürfen welchen Schutzes?

» Welche technischen, organisatorischen und personellen Maßnahmen ermöglichen diesen Schutz?

» Welche Investitionssumme sollte mit welcher Maßnahme verbunden werden?

» Inwiefern waren IT-Sicherheitsinvestitionen effektiv und effizient?

Heutige Ansätze zur Planung und Bewertung von IT-Sicherheitsmaßnahmen basieren oftmals auf Methoden der Investitionsrechnung z.B. Return on Security Investment (ROSI). Darüber hinaus kommen allgemeine Frameworks zum IT-Servicemanagement wie z.B. COBIT und ITIL zum Einsatz. Diese Maßnahmen zur Operationalisierung der Nutzenbewertung von IT-Sicherheitsmaßnahmen sind nur begrenzt geeignet, Unternehmen bei der Beantwortung der obengenannten Fragen zu helfen. Ihre begrenzte Nützlichkeit besteht u.a. darin, dass

» nicht nur die Kosten, sondern auch der Nutzen in Form von vermiedenem Schaden (Opportunitätsleistung) berücksichtigt werden muss und

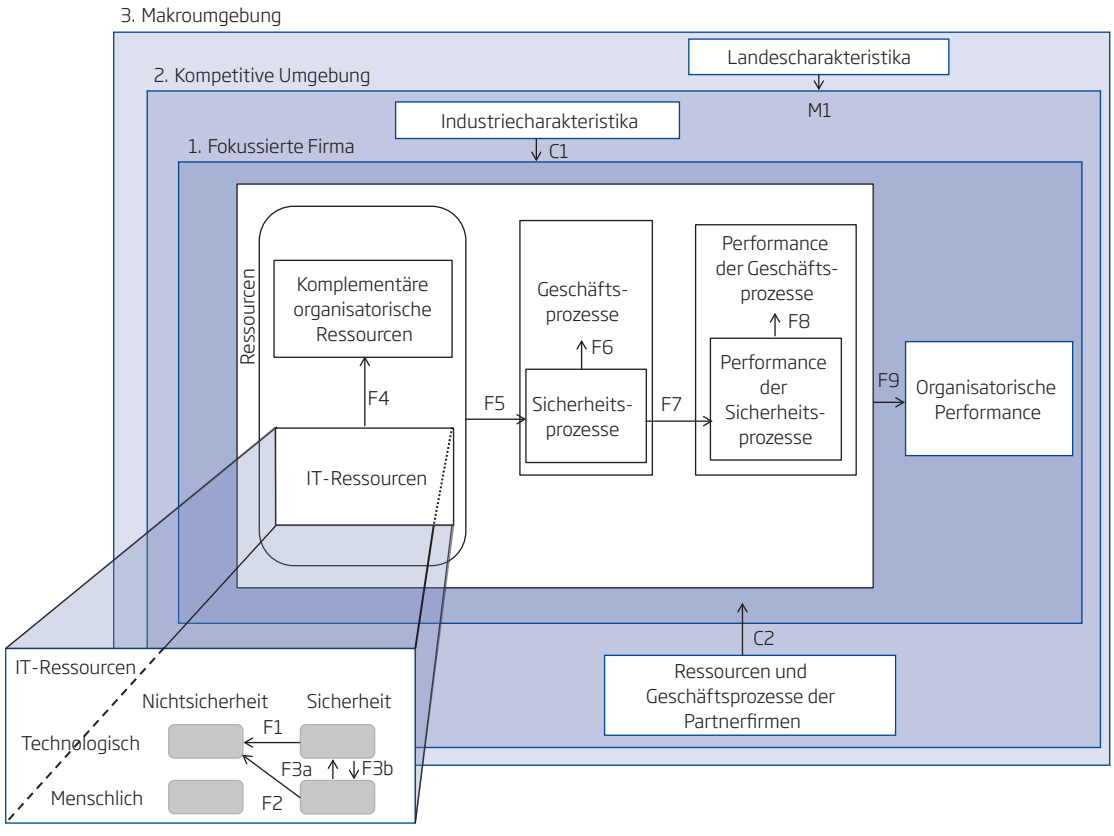
» auch nichtquantifizierbarer Nutzen wie zum Beispiel Wettbewerbsvorteile und Reputation beachtet werden müssen.

Eine ressourcenbasierte Perspektive auf IT-Sicherheit

Betrachtet man Angriffe auf IT-Systeme eines Unternehmens als Angriffe auf seine Ressourcen, so bietet sich zur Konzeptualisierung von IT-Sicherheit und ihrer unternehmensweiten Auswirkungen die bereits in ande-

WETTBEWERBSUMGEBUNG EINGESCHLOSSEN

Eine ressourcenbasierte Perspektive (RBV) auf IT-Sicherheitsinvestitionen in einem Unternehmen



Quelle: Weishäupl, E., Yasasin, E. und Schryen, G. (2015), IT Security Investments through the Lens of the Resource-based View: A new theoretical Model and Literature Review. Proceedings der 23rd European Conference on Information Systems (ECIS), Münster, 26. – 29. Mai 2015.

ren ökonomischen Kontexten angewendete „Resource-based View" (RBV) an. Ihre Anwendung gestattet es zum einen, angreifbare IT-Ressourcen sowohl im Kontext ihrer Wechselwirkungen mit anderen Ressourcen als auch in ihrer Bedeutung für Unternehmensprozesse und -performance zu betrachten. Zum anderen öffnet sie den Blick nicht nur auf diese unternehmensfokussierte Sicht, sondern auch auf Anforderungen aus der Wettbewerbs- und Makroumgebung, die – wie oben geschildert – Einfluss auf IT-Sicherheit(sinvestitionen) nehmen.

Innerhalb des Unternehmens lassen sich Ressourcen differenzieren in organisatorische Ressourcen und IT-Ressourcen, die sich ihrerseits in zwei Dimensionen und vier Typen untergliedern lassen. Es bestehen vielfache Wechselwirkungen zwischen den Ressourcentypen (Pfeile F1–F3b in nebenstehender Grafik), beispielsweise können (Investitionen in) IT-Sicherheitsschulungen von Mitarbeitern mit Fokus auf Passwortsicherheit (Wahl eines sicheren Passwortes, regelmäßiges Ändern des Passwortes) Auswirkungen auf den Schutz von CRM- und ERP-Systemen und ihren Daten haben (Pfeil F2).

Des Weiteren können Investitionen in sicherheitsbezogene IT-Ressourcen auch Auswirkungen auf organisatorische Ressourcen haben, so wirkt sich zum Beispiel eine Investition in ein biometrisches Authentifikationssystem, das den Zugang zu einem Firmengebäude kontrolliert, auf die Sicherheit der Büroräume, Akten, Daten und auch der Mitarbeiter aus (Pfeil F4). Diese Investition gestattet Mitarbeitern durch einen Fingerabdruck oder Irisscan einen schnelleren und sicheren Zugang zum Firmengebäude als bei der Verwendung von Schlüsseln, Passwörtern oder Smartcards (Pfeile F5 und F7). Dies erhöht die Effizienz von Geschäftsprozessen, da Mitarbeiter schneller am Arbeitsplatz sind und weniger Unberechtigte einen Zugang zur Firma erhalten (Pfeile F6 und F8).

Die höhere „Performance" der Sicherheitsprozesse lässt sich dabei z.B. mittels der Klassifikationsfehler („false positives" und „false negatives") erfassen, die der Geschäftsprozesse durch Produktivitätsmaße. Eine höhere Performance von Prozessen wirkt letztendlich auch auf eine höhere organisatorische Performance des Unternehmens, zum Beispiel bezüglich Gewinn, Shareholdervalue, Wettbewerbsfähigkeit und Reputation (Pfeil F9).

Anforderungen und Einflüsse auf IT-Sicherheitsinvestitionen bestehen nicht nur aus unternehmensinterner Sicht, sondern können auch aus der Wettbewerbs- und aus der Makroumgebung resultieren. Beispielsweise ergeben sich aus dem Regelwerk Basel III des Baseler Ausschusses für Bankenaufsicht sowie aus den US-amerikanischen Gesetzen Sarbanes-Oxley Act und HIPAA mittelbare und unmittelbare Anforderungen an die IT-Sicherheit(sinvestitionen) von Unternehmen (Pfeile C1 und M1). Auch Kooperationen mit Partnerfirmen können IT-Sicherheitsmaßnahmen beeinflussen, wenn beispielsweise im Rahmen von interorganisationalen Wertschöpfungsketten gemeinsame IT-Ressourcen und Daten genutzt werden und geschützt werden müssen (Pfeil C2).

Operationalisierung der RBV als Herausforderung

Die ressourcenbasierte Perspektive bietet sich sowohl als Entscheidungsgrundlage als auch für die Evaluierung von IT-Sicherheitsmaßnahmen an. Zur Operationalisierung im unternehmerischen Kontext müssen jedoch noch einige Herausforderungen gemeistert werden. Zentrale Fragestellungen sind dabei die folgenden:

- Welche Metriken sind geeignet, um die Auswirkungen von IT-Sicherheitsmaßnahmen zu messen?
- Welche Daten zur Anwendung der Metriken sind erforderlich/verfügbar oder müssen verfügbar gemacht werden?
- Wie können die potenziell unterschiedlichen Sichtweisen mehrerer Stakeholder und organisatorischer Untereinheiten innerhalb eines Unternehmens in die Planung und Bewertung von IT-Sicherheitsmaßnahmen einbezogen werden?
- Wie können Managementprozesse zur Planung und Bewertung von IT-Sicherheitsmaßnahmen etabliert werden, die eine kontinuierliche Verbesserung der IT-Sicherheit gestatten, indem Evaluationsergebnisse bei der (nächsten) Planung berücksichtigt werden?

Zusammenfassend lässt sich festhalten, dass die ressourcenbasierte Perspektive ein integriertes und ganzheitliches Management von IT-Sicherheit(sinvestitionen) gestattet, dessen Operationalisierbarkeit jedoch noch gemeinsamer Forschungsaktivitäten von Wissenschaftlern und Unternehmen bedarf.

Prof. Dr. Guido Schryen
ist Professor für Wirtschaftsinformatik an der Universität Regensburg und ist Co-Sprecher des Bayerischen Forschungsverbundes "FORSEC – Sicherheit hochgradig vernetzter IT-Systeme".

Eva Weishäupl
ist Wissenschaftliche Mitarbeiterin an der Professur für Wirtschaftsinformatik der Universität Regensburg.