Konzeption eines Modells zur Bestimmung des optimalen Investitionsbeitrags in IT-Sicherheits- bzw. IT-Notfallmaßnahmen unter Berücksichtigung Compliance-bedingter Anforderungen

Stefan Alexander Kronschnabl

ibi research an der Universität Regensburg GmbH

Da die IT immense Bedeutung für nahezu sämtliche Geschäftsprozesse hat, muss diese durch geeignete Sicherheits- und Notfallmaßnahmen abgesichert werden (Kronschnabl 2008, S. 3). Hierbei gilt es eine Vielzahl relevanter rechtlicher und aufsichtsrechtlicher Rahmenbedingungen zu berücksichtigen. Aufgrund eines in der Regel begrenzten Budgets sind zudem je nach Bedeutung und monetärem Wert des Geschäftsprozesses sowie erwarteten Schadenswahrscheinlichkeiten geeignete Absicherungs- und Notfallmaßnahmen zu treffen. Das IT-Risikomanagement kann hierzu einen wichtigen Beitrag leisten. Es gilt sinnvolle Maßnahmen zu finden und entsprechend dem Budget zu priorisieren. Ziel ist es ein Modell zu konzipieren, welches eine aussagefähige Net Present Value (NPV) Verteilung möglicher Maßnahmen liefert, um so die angemessenste Maßnahme zu identifizieren und umzusetzen.

Zur Konzeption eines Modells zur Bestimmung des optimalen Investitionsbeitrags in IT-Sicherheits- bzw. IT-Notfallmaßnahmen wurden eine Reihe von relevanten Modellen in Wissenschaft und Praxis ausgewählt und analysiert. Exemplarisch kurz aufgeführt werden die Modelle nach Gordon/Loeb (2002), Soo Hoo (2000) Cavusoglu et al. (2004), Schechter (2004) und Sonnenreich et al. (2006). Diese Modelle weisen jedoch zwei Schwächen auf: Zum einen unterstützen sie keine mehrperiodische Betrachtung. Zum anderen stellt die Komplexität der Datenbasis, auf denen die Modelle beruhen, in der Praxis ein Problem dar.

Als Grundlage für das konzipierte Modell diente schließlich das Modell von Faisst et al. (2007) in Verbindung mit dem Verfahren von Conrad (2005). Um der Realität Rechnung zu tragen, dass eine IT-Sicherheitsmaßnahme die Opportunitätskosten sinken lässt, wurde jedoch eine erweiterte Formel erarbeitet, deren Ziel es ist, die Opportunitätskosten mit und ohne IT-Sicherheitsmaßnahmen der jeweils gleichen Periode zu vergleichen. Die Unsicherheit und ihre Auswirkung wurde mithilfe der integrierten Monte-Carlo Simulation anschaulich dargestellt. Die resultierenden Diagramme stellen dabei sowohl für IT-Risikomanager als auch für Budget-Entscheider eine gute und nachvollziehbare Entscheidungsgrundlage für

Investitionen dar. Budget-Entscheider haben so die Möglichkeit bestehende Modelle, wie beispielsweise einen NPV-Ansatz, weiterhin zu verwenden, IT-Sicherheitsexperten sind nicht mehr gezwungen, sich im Rahmen der Abschätzung sehr unsicherer Werte, wie der Angriffshäufigkeit, auf eine einzige Zahl festzulegen.

Literatur

Cavusoglu H, Mishra B, Ragunathan S (2004) A model for evaluating IT security investments. Communications of the ACM 47 (7): 87-92.

Conrad J (2005) Analyzing the risks of information security investments with Monte-Carlo Simulations. http://infosecon.net/workshop/pdf/13.pdf. Abruf am 2009-04-15.

Faisst U, Prokein O, Wegmann N (2007) Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. ZfB 77 (5): 511-538.

Gordon L, Loeb M (2002) The economics of information security investment. ACM Transactions on Information and System Security 5 (4): 438-457.

Kronschnabl S (2008) IT-Security Governance. Bankinnovationen Band 23. Universitätsverlag Regensburg.

Schechter S (2004) Computer security strength & risk – a quantitative approach. Dissertatiton Cambridge. Massachusetts.

Sonnenreich W, Albanese J, Stout B (2006) Return on security investment (ROSI) – A practical quantitative model. JRPIT 38 (1): 45-55.

Soo Hoo K (2000) How Much Is Enough? A Risk-Management Approach to Computer Security. http://iis-db.stanford.edu/pubs/11900/soohoo.pdf, 2000. Abruf am 2009-01-06.