IT-Risikomanagement

als wirtschaftlicher Erfolgsfaktor

Die meisten Unternehmen sind schon einmal Opfer von IT-Sicherheitsangriffen geworden. Dahinter stecken häufig wirtschaftliche oder auch politische Motive; manchmal aber auch nur „Spaß" oder Langeweile von Jugendlichen. Die Schadenshöhe kann für Unternehmen existenzgefährdend sein. Umso erstaunlicher ist, dass in den meisten Unternehmen Wirtschaftlichkeitsüberlegungen zum IT-Risikomanagement kaum eine Rolle spielen. Aber wie viel sollte ein Unternehmen eigentlich in IT-Sicherheit investieren und welche Systeme sollten ausgewählt werden? Vor diesem Hintergrund entwickeln wir ein Entscheidungsmodell für das Management von IT-Risiken.

IT Risk Management as economic factor of success

Most companies already fell victim to IT security attacks. Often, these attacks are motivated economically or politically, but sometimes they are done by young people just for fun or out of boredom. The potential losses can jeopardize whole businesses and it is remarkable that most companies do not consider economic aspects in their IT risk management. But how much should a company invest in IT security and what systems should be secured? Against this background, we develop a decision model for the management of IT risks.

Peter Buxmann, Tobias Ackermann • Die zunehmende Vernetzung und die rasante Fortentwicklung der Informations- und Kommunikationstechnologie haben die Gesellschaft und die Unternehmenswelt nachhaltig verändert. So ist die IT-Unterstützung von inner- und zwischenbetrieblichen Geschäftsprozessen heute genauso eine Selbstverständlichkeit wie das Googeln nach Informationen oder die mobile Nutzung von Apps. Es entstehen ständig neue Plattformen, Anwendungen und Dienste – und damit auch immer neue Sicherheitsrisiken.

Neben „Worst case-Szenarien", wie wir sie beispielsweise aus vielen Spielfilmen kennen, in denen es Terroristen gelingt, die Gewalt über Computersysteme zur Steuerung von Verkehrssystemen, Atomkraftwerken oder Energieversorgungssystemen zu übernehmen, ist die Liste von Sicherheitslücken und -vorfällen lang und betrifft unterschiedlichste Bereiche.

So kommt es immer wieder vor, dass Unternehmen nicht mehr auf ihre Anwendungen und Daten zugreifen können. Selbst großen und in der Regel hochprofessionell arbeitenden Anbietern gelingt es nicht immer, Systemabstürze zu vermeiden. Dies zeigen beispielsweise die Server-Ausfälle bei Amazon, Google und Salesforce.com. Die Kosten für Ausfallzeiten in Unternehmen sind branchenabhängig unterschiedlich hoch. So setzen Studien beispielsweise die Ausfallkosten in der Logistik auf 90.000 Euro an, während sie für Online-Broker-Systeme auf 6,5 Millionen Dollar geschätzt werden – pro Stunde Downtime. Zu den unmittelbaren Ausfallkosten kommen außerdem die schwer zu quantifizierenden Schäden durch Imageverlust bei verärgerten Kunden und Lieferanten hinzu.

Andere Sicherheitsvorfälle betreffen den Verlust oder die Verletzung der Vertraulichkeit von Kundendaten. Bei T-Mobile USA wurden beispielsweise Daten von tausenden Sidekick-Nutzern durch einen Serverfehler gelöscht und konnten teilweise nicht wieder hergestellt werden. Heise titelte: „Ein Schatten legt sich auf die Cloud". Bei der Internet-Jobbörse Monster wurden Datensätze von mehr als 4,5 Millionen Betroffenen gestohlen, die unter anderem sensible Informationen wie Passwörter, E-Mail-Adressen, Namen und Telefonnummern enthielten. Viele Social-Network-Plattformen lassen sich relativ leicht hacken, um Zugriff auf persönliche Daten, wie Freundeslisten, Gästebücher etc. zu erhalten. Die Attacken sind zum Teil wirtschaftlich, teilweise aber auch politisch motiviert, wie der Hackerangriff auf Google in China zeigt.

Eine Studie des Ponemon Instituts schätzt, dass ein durchschnittlicher IT-Sicherheitsvorfall zu einem Schaden von 6,75 Mio. US-Dollar führt. In einer Umfrage gaben über zwei Drittel der befragten Unternehmen an, dass sie bereits Opfer von Internetangriffen wurden, z. B. durch Malware wie Viren, Würmer und Trojaner oder „Denial of Service"-Angriffe. Ein Drittel dieser Attacken war erfolgreich. Zu den Folgen zählten Ausfallzeiten, Diebstahl von

Fachgebiet Information Systems/Wirtschaftsinformatik
Prof. Dr. Peter Buxmann
Tel. 06151/16-4826
E-Mail: buxmann@is.tu-darmstadt.de

Dipl.-Wirtsch.-Inform. Tobias Ackermann
Tel. 06151/16-70473
E-Mail: tobias.ackermann@cased.de
www.is.tu-darmstadt.de

Peter Buxmann

Mitarbeiter- oder Kundendaten sowie der Verlust von Kreditkarteninformationen.
Umso erstaunlicher ist es vor diesem Hintergrund, dass Entscheider der wirtschaftlichen Analyse von Investitionen zur Vermeidung bzw. Reduzierung von IT-Risiken offenbar eine relativ geringe Bedeutung beimessen. So gaben in einer Studie unter 1.000 IT-Entscheidungsträgern etwa die Hälfte an, keine Kenntnisse über potenzielle Schadenshöhen aufgrund von Sicherheitslücken zu haben.
Interessanterweise steigt die Sensibilität der Unternehmen für das Thema Sicherheit, wenn Daten oder auch Prozesse nach außen gegeben werden sollen, etwa an Outsourcing-, Software-as-a-Service- (SaaS) oder Cloud-Computing-Anbieter. Im Rahmen mehrerer empirischer Untersuchungen der Software Economics Group Darmstadt-München haben wir Anwender nach den Chancen und Risiken des Einsatzes von SaaS befragt. Dabei sind gemäß einer Befragung von 349 IT-Entscheidungsträgern die (subjektiv wahrgenommenen) IT-Risiken zurzeit der wichtigste Grund, nicht auf solche SaaS-Lösungen umzusteigen. Interessant ist, dass SaaS-Kunden und Nicht-Kunden diese Risiken unterschiedlich bewerten. Nicht-Kunden betrachten SaaS noch mit Argusaugen und trauen dem Fremdbezug von IT-Diensten noch nicht so richtig über den Weg. Diejenigen Firmen, die sich jedoch für eine SaaS-Nutzung entschieden haben, bewerten die Risiken durchwegs geringer.
Flankierend haben wir Fallstudien zur Bereitschaft der Verlagerung von Diensten nach außen geführt, die zeigen, dass insbesondere kleine und mittlere Unternehmen zögern, Services und Daten nach außen zu verlagern. Diese Skepsis verstärkt sich, wenn es darum geht, Daten und Prozesse an Offshore-Standorte zu verlagern.

IT-Risikomanagement

Der IT-Risikomanagementprozess wird meistens als Vorgehensweise bestehend aus vier Phasen beschrieben: Die Identifikation hat die Ermittlung unternehmensrelevanter Bedrohungen zum Ziel. In der Phase der Quantifizierung werden für die Bedrohungen die beiden Größen Eintrittswahrscheinlichkeit und Schadenshöhe geschätzt. Die Steuerung der Risiken erfolgt durch gezielte Implementierung von Gegenmaßnahmen, während die Kontrolle dazu dient, die Entscheidungen in den vorangegangenen Phasen zu evaluieren. IT-Risikomanagement ist ein kontinuierlicher Prozess, da sich die Werkzeuge der Angreifer, aber auch die verfügbaren Sicherheitstechnologien ständig weiterentwickeln.

Ein Entscheidungsmodell zum Management von IT-Risiken

Vor diesem Hintergrund haben wir im Rahmen unseres CASED-Teilprojekts ein Modell zum Management von IT-Risiken entwickelt. Das Ziel besteht darin, Anwendern eine Entscheidungshilfe bei der Auswahl alternativer Maßnahmen zum IT-Risikomanagement zur Verfügung zu stellen. Ausgangspunkt ist eine Modellierung der Geschäftsprozesse der beteiligten Unternehmen. Im Anschluss werden auf Basis eines Risikokatalogs für die Funktionen der Prozesse sowie die Kommunikation zwischen diesen Sicherheitslücken identifiziert. Darauf aufbauend werden für die identifizierten Risiken das Schadensausmaß für verschiedene Szenarien und die jeweiligen Eintrittswahrscheinlichkeiten geschätzt.
Entscheidend für die Anwendung des Modells in der Praxis ist die Bestimmung der Parameter. Um möglichst realistische Werte zu erhalten, arbeiten wir am CASED eng mit Juristen und Informatikern zusammen. Rechtswissenschaftler können beispielsweise helfen, Prozesskosten für alternative Szenarien abzuschätzen.
Informatiker wiederum bringen fundiertes Wissen über die Wahrscheinlichkeit ein, mit der bestimmte

Peter Buxmann ist Professor für Wirtschaftsinformatik an der Technischen Universität Darmstadt und befasst sich u. a. mit den Spielregeln der Softwareindustrie, Software-as-a-Service und IT-Sicherheit. Er ist zudem Principal Investigator des LOEWE-Zentrums CASED.

Tobias Ackermann ist wissenschaftlicher Mitarbeiter am Fachgebiet Information Systems/Wirtschaftsinformatik an der TU Darmstadt und Stipendiat der CASED-Graduiertenschule.

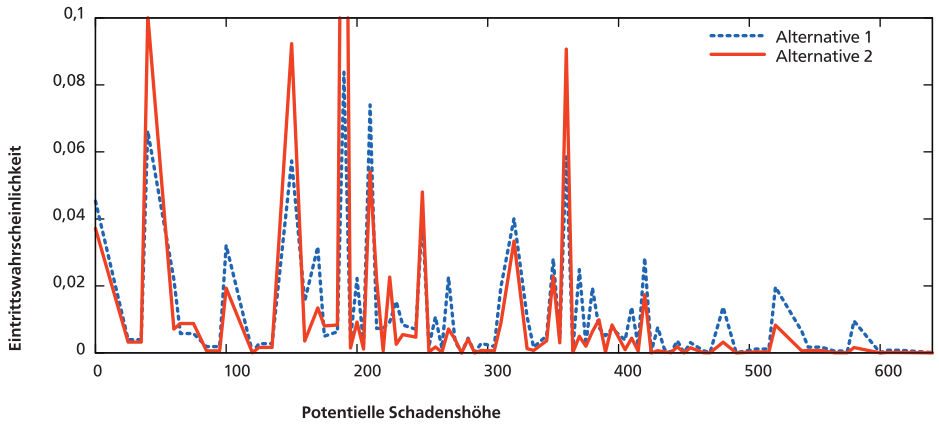

Abbildung 1
Visualisierung der potentiellen Schadensverteilung für zwei alternative Sicherheitsszenarien.
Anhand der Eintrittswahrscheinlichkeiten für bestimmte Schadenshöhen und anderen Kennzahlen wie dem durchschnittlichen Schaden, der Breite der Schwankungen oder der Schadenshöhe, die mit einer gegebenen Wahrscheinlichkeit nicht überschritten wird, lassen sich die beiden Alternativen vergleichen. Das Modell liefert auf diese Weise eine Entscheidungshilfe, um zwischen verschiedenen Sicherheitsniveaus abzuwägen.

Systeme ausfallen oder gebrochen werden. Das Modell erlaubt auch die Abbildung von Prozessen im „Internet of Services“, bei denen Dienste unterschiedlicher Anbieter zu einer auf die Bedürfnisse der Kunden zugeschnittenen Lösung kombiniert werden.
Auf Grundlage des Entscheidungsmodells ist es möglich, alternative Investitionen in IT-Sicherheit zu bewerten und auszuwählen. Beispielsweise lässt sich abwägen, ob eine zusätzliche Ende-zu-Ende-Verschlüsselung eingesetzt werden sollte oder ob Standard-Verfahren wie SSL ausreichend sind, um die Vertraulichkeit von Daten zu schützen. Mit Hilfe von Modellanalysen lässt sich zeigen, dass aus ökonomischer Sicht ein optimales Sicherheitsniveau existiert, das häufig nicht dem technischen entspricht.
Aber nicht nur auf Nutzerseite lassen sich mit Hilfe des Modells Entscheidungen unterstützen. So gilt grundsätzlich, dass Unternehmensstrategien, auf die Kundenbedürfnisse abzustimmen sind. Konkret betrifft das die Preis-, Produkt-, Vertriebs- und Kommunikationspolitik. Die Idee besteht also darin, Sicherheitsmechanismen in die Herstellerstrategien zu integrieren. So könnten die Anbieter auf Basis der Risikopräferenzen und Zahlungsbereitschaften der Kunden beispielsweise eine Preis- und Produktdifferenzierung etablieren. Dabei handelt es sich um eine bewährte strategische Maßnahme, um die unterschiedlichen Zahlungsbereitschaften verschiedener Kundengruppen abzuschöpfen. Darüber hinaus könnten die Anbieter das Thema IT-Sicherheit bzw. die Maßnahmen, um diese zu gewährleisten, in ihre Kommunikationsstrategie integrieren. Auf diese Weise bietet sich ihnen die Chance das notwendige Vertrauen aufzubauen, um Neukunden zu gewinnen bzw. bestehende Kunden an sich zu binden. Dies könnte insbesondere auch für deutsche IT-Sicherheitsfirmen von Interesse sein, die in der international geprägten Softwareindustrie bislang nur eine Nebenrolle spielen.

Praxisprojekte

- Im Rahmen des BMBF-Projekts Premium Services werden u. a. in Kooperation mit SAP Research und dem Fraunhofer-Institut SIT die Nutzerpräferenzen und Zahlungsbereitschaften für einen dort entwickelten Sicherheitsdienst untersucht. Die Ergebnisse sollen als Eckdaten für die ökonomische Entwicklung von IT-Sicherheitsstrategien aus Anbietersicht genutzt werden.

- Für die Darmstädter Momax GmbH wurde eine wirtschaftliche Risiko- und Sicherheitsevaluation ihres Micropayment-Systems miniPay durchgeführt. Der Zahlungsdienst ermöglicht es seinen Kunden, beispielsweise Verlagen, digitale Inhalte an Endkunden auf einfache Art per Lastschrift zu verkaufen. Im Rahmen des Projektes wurden die Systemkomponenten, deren Zusammenspiel untereinander und die verwendeten Protokolle für den Zahlungsablauf systematisch untersucht und bewertet.

- In Kooperation mit einem Praxispartner aus dem öffentlichen Bereich wurde ein Entwurf eines IT-Sicherheitskonzepts für einen Teilbereich der IT-Landschaft erstellt. Dieses Dokument enthält eine individuelle Analyse möglicher Angriffs- und Schadenszenarien und empfiehlt Maßnahmen, um ein definiertes Schutzniveau zu erreichen.