Sachar Paulus

Basiswissen Sichere Software

Aus- und Weiterbildung
zum ISSECO Certified
Professional for Secure Software Engineering

dpunkt.verlag

iSQI International Software Quality Institute

iSSECO

Was sind E-Books von dpunkt?

Unsere E-Books sind Publikationen im PDF- oder EPUB-Format, die es Ihnen erlauben, Inhalte am Bildschirm zu lesen, gezielt nach Informationen darin zu suchen und Seiten daraus auszudrucken. Sie benötigen zum Ansehen den Acrobat Reader oder ein anderes adäquates Programm bzw. einen E-Book-Reader.

E-Books können Bücher (oder Teile daraus) sein, die es auch in gedruckter Form gibt (bzw. gab und die inzwischen vergriffen sind). (Einen entsprechenden Hinweis auf eine gedruckte Ausgabe finden Sie auf der entsprechenden E-Book-Seite.)

Es können aber auch Originalpublikationen sein, die es ausschließlich in E-Book-Form gibt. Diese werden mit der gleichen Sorgfalt und in der gleichen Qualität veröffentlicht, die Sie bereits von gedruckten dpunkt.büchern her kennen.

Was darf ich mit dem E-Book tun?

Die Datei ist nicht kopiergeschützt, kann also für den eigenen Bedarf beliebig kopiert werden. Es ist jedoch nicht gestattet, die Datei weiterzugeben oder für andere zugänglich in Netzwerke zu stellen. Sie erwerben also eine Ein-Personen-Nutzungslizenz.

Wenn Sie mehrere Exemplare des gleichen E-Books kaufen, erwerben Sie damit die Lizenz für die entsprechende Anzahl von Nutzern.

Um Missbrauch zu reduzieren, haben wir die PDF-Datei mit einem Wasserzeichen (Ihrer E-Mail-Adresse und Ihrer Transaktionsnummer) versehen.

Bitte beachten Sie, dass die Inhalte der Datei in jedem Fall dem Copyright des Verlages unterliegen.

Wie kann ich E-Books von dpunkt kaufen und bezahlen?

Legen Sie die E-Books in den Warenkorb. (Aus technischen Gründen, können im Warenkorb nur gedruckte Bücher ODER E-Books enthalten sein.)

Downloads und E-Books können sie bei dpunkt per Paypal bezahlen. Wenn Sie noch kein Paypal-Konto haben, können Sie dieses in Minutenschnelle einrichten (den entsprechenden Link erhalten Sie während des Bezahlvorgangs) und so über Ihre Kreditkarte oder per Überweisung bezahlen.

Wie erhalte ich das E-Book von dpunkt?

Sobald der Bestell- und Bezahlvorgang abgeschlossen ist, erhalten Sie an die von Ihnen angegebene Adresse eine Bestätigung von Paypal, sowie von dpunkt eine E-Mail mit den Downloadlinks für die gekauften Dokumente sowie einem Link zu einer PDF-Rechnung für die Bestellung.

Die Links sind zwei Wochen lang gültig. Die Dokumente selbst sind mit Ihrer E-Mail-Adresse und Ihrer Transaktionsnummer als Wasserzeichen versehen.

Wenn es Probleme gibt?

Bitte wenden Sie sich bei Problemen an den dpunkt.verlag:
Frau Karin Riedinger (riedinger (at) dpunkt.de bzw. fon 06221-148350).

Basiswissen
Sichere Software

Sachar Paulus ist Professor für Wirtschaftsinformatik, insbesondere Unternehmenssicherheit und Risikomanagement, an der Fachhochschule Brandenburg, Inhaber der Unternehmensberatung für Sicherheit »paulus.consult« und Senior Analyst bei KuppingerCole. Von 2000 bis 2008 war er bei SAP in verschiedenen Leitungsfunktionen zu Sicherheit tätig, u.a. als Leiter der Konzernsicherheit und Leiter der Produktsicherheit, und vertrat SAP als Vorstandsmitglied in den beiden Vereinen »Deutschland Sicher im Netz« und »TeleTrusT«. Weiter war er Mitglied der ständigen Interessenvertretung der ENISA (Europäische Netzwerk- und Informationssicherheitsagentur) und des Forschungsbeirats »RISEPTIS« für Vertrauen und Sicherheit im Future Internet der Europäischen Kommission. Er engagiert sich für sichere Softwareentwicklung und ist Gründer und Präsident des ISSECO e.V.

Sachar Paulus

Basiswissen Sichere Software

Aus- und Weiterbildung zum ISSECO Certified Professional for Secure Software Engineering

dpunkt.verlag

Sachar Paulus
sachar.paulus@paulus-consult.de

Lektorat: Christa Preisendanz
Copy-Editing: Ursula Zimpfer, Herrenberg
Herstellung: Nadine Thiele
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: M.P. Media-Print Informationstechnologie GmbH, 33100 Paderborn

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-89864-726-7

1. Auflage 20011

Ringstraße 19 B
69115 Heidelberg

5 4 3 2 1 0

Geleitwort von Stephan Goericke

Sicherheit ist gegenwärtig in aller Munde. Ganz gleich, ob es um die Finanzkrise, Erdbeben und Tsunamis, Kernkraftwerke oder Spielekonsolen geht: Sicherheit wird aufgrund der Komplexität unserer Gesellschaft immer wichtiger.

Softwaresicherheit, damit meine ich die Fähigkeit, Software herzustellen, die sowohl Angriffen standhält als auch keine Schäden in ihrer Umwelt verursachen kann, wird in ihrer Bedeutung stark unterschätzt. Es gibt wohl keinen Kompetenzbereich, der einerseits in so vielen Branchen und Technologien erforderlich ist, gleichzeitig aber so stiefmütterlich behandelt wird.

Dabei gilt dies für alle, die in den Herstellungsprozess von Software involviert sind, und zwar unabhängig davon, ob die Software als eigenes Produkt verkauft wird, eine eingegrenzte Hardwarefunktion unterstützt (wie z.B. im Automotive-Bereich), Webanwendungen am Laufen hält oder komplexe technische Anlagen steuert. Betroffen sind alle Stakeholder: solche, die Anforderungen stellen, jene, die entwickeln, diejenigen, die testen, und wiederum die, die Software betreiben und einsetzen. Auch die Größe spielt keine Rolle: Kein Einmannbetrieb kann sich aus der Verantwortung für Softwaresicherheit damit herausreden, sein Unternehmen sei zu klein. Genauso spielt das Business-Modell keine Rolle. Ob »as a Service«, als Produkt oder als Dienstleistung: Immer und überall muss auf Sicherheit während des Produktionsprozesses geachtet werden, damit in unserer stark integrierten und zusammenwachsenden Welt Softwareanwendungen nicht Quelle von Gefahren und Verunsicherung werden.

Sicherheit ist Softwarequalität.

Damit wird dieses Feld »the next big thing«, davon bin ich überzeugt. Genau wie vor 20 Jahren, als das Thema »Softwarequalität« niemanden wirklich interessiert hat, aber zwingend notwendig war, um Software professionell betreibbar zu machen, und damit grundlegend für gewaltige Innovationen wurde, interessieren sich heute viele Anwender für Sicherheit – aber nicht für die dafür erforderlichen Aktivitäten und Skills im Bereich der Softwaresicherheit. Denn so wie man Kernkraft nicht sicher gestalten kann, ohne die physikalischen Prozesse zu kennen, so

kann man Softwareprodukte nicht nachträglich sicher machen, sondern muss bereits im Herstellungsprozess Vorsorge treffen.

Daher begrüße ich die mutigen Streiter und Vorausdenker von ISSECO, die mit ihrem CPSSE-Zertifikat zum richtigen Zeitpunkt auf den Markt gekommen sind. Der »Certified Professional for Secure Software Engineering« war das erste Personenzertifikat zu Softwaresicherheit und ist das einzige in Europa. Der CPSSE kann auch als Baustein für den Quality Assurance Management Professional (QAMP) verwendet werden. Die Anzahl der Zertifizierungen wächst stetig, und durch das vorliegende Buch, dessen bin ich mir sicher, wird die Anzahl der Zertifikate noch einmal stark steigen. Denn die Zielgruppe sind nicht nur Entwickler, sondern eben alle, die mit Softwareentwicklung zu tun haben und wissen sollten, was an Sicherheit für ihre Software erforderlich ist und wie dies umgesetzt werden kann – auf Kunden- wie auf Herstellerseite oder als Berater.

Ich wünsche dem Buch »Basiswissen Sichere Software« und dem Zertifikat »CPSSE« für die Zukunft viel Erfolg.

Stephan Goericke
Director iSQI GmbH

Geleitwort von Jörg Brinkmann

IT-Management wird eine immer komplexere Aufgabe. Durch die zunehmende Vereinfachung der Informationstechnologie und den Druck, auch im Unternehmen Dienste anzubieten, die die Mitarbeiter aus dem privaten Bereich kennen, stellen sich immer mehr Anforderungen an den Leiter einer IT-Organisation, der sowohl einen effizienten, kostenoptimierten Betrieb gewährleisten will als auch seine Kunden, also die Geschäftsbereiche, zufriedenstellen möchte.

Ein besonders komplexes Aufgabengebiet stellt dabei die IT-Sicherheit dar. Auf der einen Seite sollen die IT-Dienste möglichst leicht und komfortabel verwendbar sein, auf der anderen Seite muss die IT-Leitung Verfügbarkeit, Vertraulichkeit und Integrität der zu verarbeitenden Daten sicherstellen – und wird auch dafür verantwortlich gemacht. Dies ist nicht zuletzt deswegen so aufwendig, weil viele Softwarehersteller und Diensteanbieter im Hinblick auf Sicherheit die Anforderungen der Kunden nicht genügend beachten, und dies oft nur mit teuren Zusatzlösungen oder viel individuellem Aufwand wettgemacht werden kann.

Auftraggeber müssen künftig immer mehr Einfluss auf die Gestaltung der Angebote nehmen – ob als Software, als Dienst oder als mobile »App«. Dies gilt insbesondere für IT-Architekturen, die mit dem Stichwort »Cloud« verbunden sind, ob nun in einer Private, Public oder Hybrid Cloud. Hier ist ein geeigneter Prozess der Anforderungsdefinition schon beim Kunden erforderlich, entsprechende Maßnahmen für die Ermittlung von möglichen Bedrohungen durch Hacker und Spione und andere Sicherheitsanforderungen, wie etwa die Integration in ein Identitätsmanagementkonzept, sind ebenfalls notwendig für eine schlüssige IT-Sicherheitsarchitektur.

Zudem ist es von Vorteil, wenn man als Kunde auch versteht, welche Anforderungen an den Prozess der Entwicklung an Softwarehersteller gestellt werden müssen, damit auch sichere Software erzeugt werden kann. Erst durch das Verständnis dafür, warum das Schützen von Software so schwierig ist und was man tun kann, ist auch der sichere Einsatz von Software und von internetbasierten Diensten nachhaltig möglich.

Aus diesem Grund freue ich mich sehr, wenn eine Initiative wie ISSECO sich um die Qualifizierung für Aspekte der Softwaresicherheit bemüht und ein renom-

mierter Experte wie Prof. Paulus sich die Zeit nimmt, ein Lehrbuch zu sicherer Softwareentwicklung zu schreiben. Denn nur wenn man das Übel an der Wurzel packt, sprich: betroffene Zielgruppen im Entwicklungsprozess über die Risiken ihrer Arbeit aufklärt und ihnen Wege aufzeigt, wie sie diese im Sinne ihrer Kunden beheben können, wird sich die Situation nachhaltig verbessern. Dies gilt auch für die Anwenderunternehmen, die lernen müssen, die »richtigen« Anforderungen an die Lieferanten zu stellen.

Zusammen mit Experten können unsere IT-Mitarbeiter nun durch das vorliegende Buch und die passenden Schulungen und Zertifikate diese Herausforderung annehmen.

Ich wünsche diesem Projekt viel Erfolg!

Jörg Brinkmann
CIO Bilfinger Berger SE

Vorwort

Es hat eine Weile gedauert, bis dieses Buch zustande gekommen ist. Zwar ist die ISSECO-CPSSE[1]-Zertifizierung noch relativ jung – es gibt sie seit Herbst 2009 –, aber die Idee, ein deutsches Lehrbuch zum Thema zu schreiben, hatte ich schon seit längerer Zeit.

Das Feld der Themen, die für sichere Softwareentwicklung relevant sind, ist zudem relativ breit, und eine Auswahl und Zusammenstellung für ein »Basiswissen« ist nicht trivial. Daher war die Anfrage des dpunkt.verlags, zur Zertifizierung ein Buch zu schreiben, der Auslöser, endlich dieses Projekt zu beginnen, und die Ausrichtung am Syllabus des ISSECO CPSSE ist eine willkommene Orientierung gewesen. Die Inhalte der Schulungen habe ich an der einen oder anderen Stelle um aktuelle Informationen ergänzt und erläuternde Hintergrundinformationen hinzugefügt. Damit sollte das Buch auch für die nächste Version des Syllabus »passen«, also als Prüfungsvorbereitung für die Zertifizierung dienen können.

Ich möchte mich bei den folgenden Personen bedanken, ohne die dieses Buch nicht entstanden wäre: bei den Kollegen von ISSECO, und zwar bei allen, die beim Syllabus und der Entwicklung der ersten Schulungsunterlagen mitgeholfen haben, im Speziellen bei Petra Barzin und Peter Trommler. Beide haben auch dankenswerterweise als Korrekturleser bereitgestanden. Weiterhin möchte ich mich bei iSQI[2] und natürlich speziell bei Stephan Goericke bedanken, ohne die es ISSECO nicht geben würde. iSQI hat die Gründung des Vereins tatkräftig unterstützt und bildet ein stabiles organisatorisches Rückgrat für den Verein. Auch die Damen von dpunkt, namentlich insbesondere Christa Preisendanz, verdienen meinen Dank, sie haben immer wieder Feedback gegeben und sind letztlich dafür verantwortlich, dass das Buch auch in die Reihe »Basiswissen« passt.

Schließlich möchte ich mich bei meiner Familie bedanken, meiner Frau Diana und meinen beiden Kindern Mika und Gina, die mir in den letzten Monaten verziehen haben, dass ich mich nicht so um sie gekümmert habe, wie ich es hätte

1. ISSECO: International Secure Software Engineering Council (*www.isseco.org*);
   CPSSE: Certified Professional for Secure Software Engineering
2. iSQI: International Software Quality Institute

machen sollen, speziell da wir in dieser Zeit wieder Nachwuchs bekommen haben. Der kleinen Lola wünsche ich alles Gute für ihr Lebensabenteuer.

Ich hoffe, dass Sie das Buch nicht nur als Lehrgrundlage gut verwenden können, sondern auch ein wenig Spaß beim Lesen haben und dass Sie vielleicht ein klein bisschen von der Faszination erhaschen können, ein Softwareprodukt gleichzeitig elegant und sicher zu machen.

Sachar Paulus
Neckargemünd, im Mai 2011

Inhaltsverzeichnis

1 Einleitung

Sichere Software ist Software, die gegen absichtliche Angriffe auf die Software geschützt ist. Jeder im Softwareentwicklungsprozess sollte an dieser Eigenschaft einer Software interessiert sein, da Software leider selten »automatisch« sicher ist. Da Sicherheit durch die Abwesenheit von erfolgreichen Angriffen gegeben ist, muss die Software jedem möglichen Angriff standhalten können. Dieses Buch richtet sich an Softwareentwicklungsverantwortliche und Qualitätsverantwortliche, die Sicherheit im Entwicklungsprozess verankern wollen, aber auch an Sicherheitsexperten, die sich der Thematik »wie mache ich Software sicher?« widmen wollen.

1.1 Ziele dieses Buches

IT-Systeme sind nur sicher, wenn alle Elemente, die zum IT-System gehören, sicher sind. Der in der Vergangenheit übliche Gedanke, dass die Sicherheit von der Infrastruktur und dem Perimeter erbracht werden kann (also Firewalls, Antivirus-Software, Betriebssystemsicherheit), ist nicht mehr richtig. Eigentlich war der Gedanke noch nie richtig, aber da die wertvollen Informationen in den Anwendungen hinter hohen (virtuellen) Wänden lagen und dort meist ungeschützt, bestand das Ziel darin, Löcher in der Infrastruktur zu finden, so wie es im Mittelalter das Ziel war, Zugang in ein Burg zu bekommen, denn innerhalb der Mauern war der Schatz meist nicht gut gesichert.

Aus zwei Gründen ist dieser Vergleich nicht mehr verwendbar: Zum einen werden immer mehr Anwendungen aus der Burg herausgeholt bzw. sprechen mit Kunden jenseits der Burgmauern und zum anderen sind die Löcher in den Burgmauern weitestgehend gestopft und es ist einfacher für Angreifer, direkt die Anwendungen anzugreifen. Moderne IT ist eher mit einer Stadt zu vergleichen als mit einer mittelalterlichen Burg.

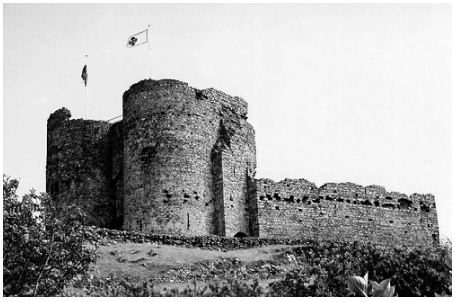

Abb. 1–1 *So nehmen heute noch die meisten IT-Sicherheit wahr – eine dicke Mauer mit wenigen Durchgängen (Quelle: www.copyrightfreephotos.com).*

Abb. 1–2 *Und so sollte Sicherheit in der heutigen Welt aussehen – sehr individuell, massentauglich und auf das jeweilige Risiko abgestimmt (Quelle: www.copyrightfreephotos.com).*

Daher ist es nicht nur wichtig, sichere Infrastrukturkomponenten zu bauen, sondern alle Softwareelemente eines IT-Systems müssen sicher sein. Sicher heißt, dass sie nicht durch Angriffe auf Daten in ihrer Funktionalität verändert werden können, Daten kopiert, manipuliert oder gelöscht werden können oder ihre Verfügbarkeit eingeschränkt werden kann. Die Informationen sollen stets verfügbar, integer und vertraulich verarbeitet werden. Das heißt, egal, ob Sie Softwareprodukte entwickeln, softwarebasierte Steuerungen für Anlagen bauen oder Webanwendungen konfigurieren, Ihre Software ist jetzt das Ziel der Hacker und nicht nur das Ziel, sondern – wenn Sie schlechte, sprich: unsichere Software bauen – auch das Werkzeug, unfreiwillig. Die meisten Angriffe auf Daten sind heutzutage auf unsichere Software und Systeme zurückzuführen, Systeme, die eine Schwachstelle haben, die von Angreifern ausgenutzt werden kann – und ausgenutzt wird.

Dieses Buch hat zum Ziel, zu vermitteln, wie man sichere Software entwickeln kann. Dabei werden alle wichtigen Bereiche der Softwareentwicklung besprochen und aufgezeigt, was für Sicherheit getan werden kann – und muss.

1.1.1 Warum brauchen wir sichere Software?

Die Mehrzahl der Angriffe auf Daten finden heute über das Internet statt unter Verwendung von komplexen Werkzeugen wie trojanischen Pferden, Botnetzen, Rootkits usw. Auch wenn wir sehen werden, dass das Bild in dieser Deutlichkeit nicht ganz richtig ist: Heute kann ein Hacker im Prinzip vom heimischen Sofa aus (fast) alle IT-Systeme dieser Welt angreifen. Und sind diese nicht gut geschützt bzw. nicht sicher in sich selbst, dann auch erfolgreich.

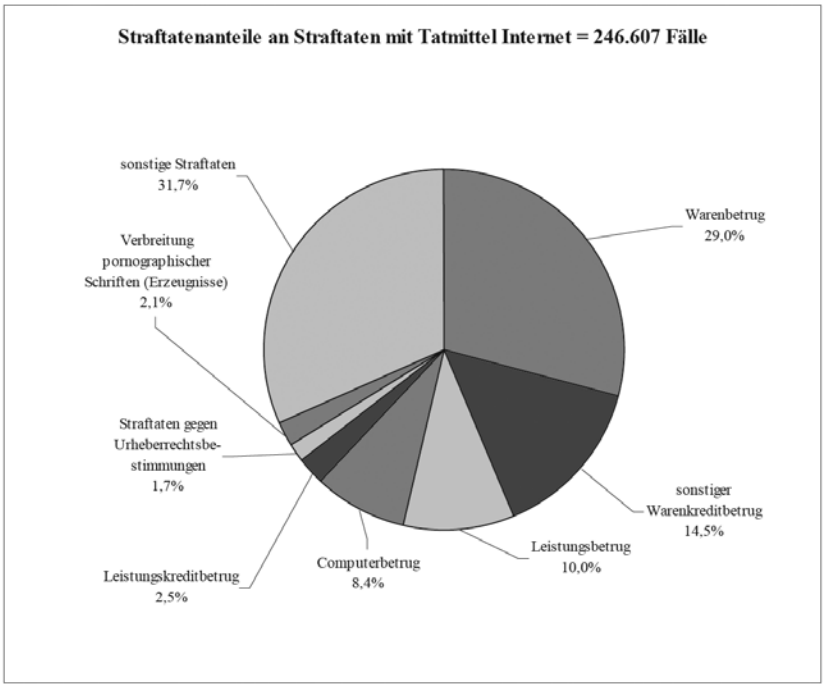

Abb. 1–3 *Aus der polizeilichen Kriminalstatistik 2010 (Quelle: www.bka.de/pks/pks2010/download/pks2010_imk_kurzbericht.pdf, S. 15)*

Neben dem reinen finanziellen Schaden, den ein Hacker anrichten kann, ist in der Konsequenz auch oft das Image des Herstellers wie auch des Kunden, der die Systeme betreibt und bei dem Daten gestohlen oder manipuliert werden konnten, in Mitleidenschaft gezogen. Zudem werden – man geht von einer deutlich höheren Dunkelziffer aus – die meisten Angriffe vermutlich gar nicht entdeckt: Wissensvorsprung wandert zum Konkurrenten, Industriegeheimnisse zur fremden Macht, IT-Systeme werden zur langsamen Sabotage genutzt. Die Liste ist lang.

Aber warum schützen uns die Sicherheitsprodukte nicht vor diesen Angriffen? Sind denn die Investitionen in Antivirus-Software und Firewalls, in Verschlüsselung und Data Leakage Prevention nicht genau dafür da, dies zu verhindern? Ein

einfacher Vergleich: Nur weil ein Auto einen Sicherheitsgurt hat, muss die Bremse nicht zuverlässig funktionieren. Im Web ist das ähnlich. Anwendungen müssen sich selbst schützen, die genannten Sicherheitsprodukte schützen zwar jeweils bestimmte Technologien gegen bestimmte Angriffe, aber auch nur diese Technologien gegen genau diese Angriffe. Es gibt ja auch keinen Impfstoff gegen alle Krankheiten dieser Welt. Und wenn gestern das Wichtigste war, sich gegen Cholera zu schützen, dann kommt heute die Hauptbedrohung vielleicht von Grippenviren. Am besten ist ein gut funktionierendes Immunsystem. Auch dann kann man Infektionen nicht vollständig vermeiden, aber meist lebt man damit deutlich länger – und besser.

Der erste Schritt zu einem guten Immunsystem ist, Einfallstore zu schließen, und Angriffsflächen zu verkleinern. Und in der aktuellen Zeit – Technologie verändert sich ja zunehmend schneller – sind die meisten IT-Technologien HTTP-basiert und Zugriffe auf Daten sollten von überall ohne Hürden erfolgen können. Gegen Angriffe auf Anwendungsebene können Firewalls, die dazu da sind, unerlaubte Zugriffe auf Netzwerkebene abzuweisen, und Antivirus-Software, die bösartige E-Mail-Anhänge erkennen soll, eben nichts tun. Da sind andere Techniken gefragt. Doch am besten schützt die Software sich selbst.

1.1.2 Warum wird Sicherheit bei Softwareentwicklung oft vernachlässigt?

Wenn ein gutes Immunsystem so wichtig und so sinnvoll ist, warum gibt es das nicht bei Software? Was läuft schief bei den meisten Softwareentwicklungen, dass eben der Eigenschutz der Software gegen Angriffe nicht funktioniert? Hierfür gibt es eine Reihe von Gründen.

- Softwarehersteller, wie auch viele Kunden, reden nicht gerne über Sicherheitsprobleme oder Schwachstellen, denn sie fürchten **Imageprobleme** und **Reputationsverlust** mehr als den möglicherweise entstehenden Schaden. Darüber nicht zu reden ist eigentlich widersinnig, denn natürlich gibt es eine Bedrohung, und kein Produkt der Welt ist perfekt, also sollte man sich genau damit auseinandersetzen, um Größe zu demonstrieren. Studien von Krisen, in denen Unternehmen unterschiedlich offenes Krisenmanagement betrieben haben, zeigen, dass die Unternehmen, die proaktiv mit einer Krise umgegangen sind (z. B. eine Airline nach einem Flugzeugabsturz), in der Wahrnehmung und sogar in der börslichen Bewertung besser geworden sind. Ein Grund, warum dennoch die Auseinandersetzung mit dem Thema IT-Sicherheit vermieden wird, ist möglicherweise, dass man damit zugeben müsste, dass man die IT nun doch nicht vollständig beherrscht und insbesondere Unternehmenslenker sich auf etwas verlassen, das sie gar nicht verstehen.
- Viele Entscheider **schätzen** die mit IT-Sicherheit verbundenen **Risiken falsch ein**. Das ist systemimmanent, denn der Job von Entscheidern besteht gerade darin, Chancen zu nutzen und dafür Risiken einzugehen. Ihnen ist aus diesem