INTARGIA
IDEE.IT.ZIEL

Whitepaper: Sichere IT-Systeme

Sicherheitsziele und wirksame Maßnahmen

Kontaktdaten:

IT-RISIKO-
MANAGEMENT

Dr. Thomas Jurisch, Steffen Weber
Telefon: +49 (0)6103 350860
E-Mail: it-risikomanagement@intargia.com
Webseite: http://www.intargia.com

Inhalt

1 Einleitung – Wozu IT-Sicherheit?

Unternehmen im 21. Jahrhundert sind Teil der globalen Informations- und Wissensgesellschaft. Treiber für die zunehmende Bedeutung von Informationen und Wissen sind Internationalisierung und Globalisierung von Märkten, Produkten und Ressourcen, die ansteigende Intensität von elektronischen Informationen und die zunehmende Ubiquität vernetzter Informations- und Kommunikationstechnologie.

Aus Unternehmenssicht ist die Auseinandersetzung mit diesen Themen zwingend notwendig. Unternehmensziele wie Fokussierung auf das Kerngeschäft, „Operational Excellence", effizientes Sourcing, Compliance-Konformität oder organisatorische Umbrüche, z. B. durch Akquisition, Fusion oder Kooperation, sind nur durch eine enge Verzahnung von Unternehmens- und IT-Strategie zu erreichen.

Analog zu der Chance, die diese Entwicklungen Unternehmen bietet, sehen sie sich auch einem wachsenden Risiko gegenüber. Anders als Industriegüter werden Informationen nicht verbraucht, sind leicht zu vervielfältigen, zu verfälschen und zu verteilen. Darauf muss ein Unternehmen reagieren, um seine Informationen zu schützen und deren Integrität, Vertraulichkeit und Verfügbarkeit zu gewährleisten.

Die Notwendigkeit dafür zeigen aktuelle Studien der sogenannten *Big Four*[1]*,* der vier größten Unternehmen der Wirtschaftsprüfungsbranche. Diese Studien eint eine Kernaussage: Die stetig steigende interne und externe Bedrohung der Unternehmens-IT und somit hochsensibler Unternehmensinformationen in Verbindung mit der Professionalisierung der Angriffe.
Wie ernst Unternehmen diese Bedrohung nehmen zeigt z. B. eine aktuelle Umfrage der Unternehmensberatung Capgemini unter deren CIOs. „Security" ist mit großem Abstand und zum wiederholten Male das Top-Thema hinsichtlich Wichtigkeit von IT-Themen in den kommenden Jahren:

Abb. 01: Bedeutung von IT-Themen

Wie wichtig sind die folgenden Themen für Sie in den kommenden Jahren?

		Mittelwerte						
		2008	2007	2006	2005	2004	2003	2002
Security	82%	1,74	1,71	1,71	1,56	1,70	**	**
IT-Infrastruktur- und IT-Service-Management	66%	2,19	2,30	2,59	2,21	2,44	2,65	2,81
Business Intelligence	64%	2,28	2,39	2,67	2,82	2,93	2,55	2,88
Portale	61%	2,54	2,81	2,64	3,01	3,04	2,33	2,58
ERP, Harmonisierung	57%	2,44	2,10	2,17	2,15	2,48	2,83	2,60
Customer Relationship Management (CRM)	56%	2,42	2,62	2,57	2,87	**	**	**
Mobility/Wireless	54%	2,50	2,72	2,80	3,05	3,18	2,83	3,30
Unternehmens-architektur und SOA	45%	2,93	2,58	3,02	2,91	2,96	3,08	3,07
Outsourcing	39%	3,18	**	**	**	**	**	**

Basis: Alle Befragten (n = 91) – Prozentangaben[1], Mittelwerte; **nicht erhoben

[1] Top-2-Box: Werte „1" und „2" auf der Skala von „sehr wichtig" (1) bis „völlig unwichtig" (6)

Capgemini 2008

[1] Siehe die jeweiligen Quellenangabe im Literatur- und Quellenverzeichnis.

Abbildung 1: Bedeutung von IT-Themen, Quelle: Capgemini.

Dies bringt eine Vielzahl von Implikationen für die IT von Unternehmen mit sich: Sobald IT-Systeme in einem wie auch immer gearteten Netzwerk (dazu zählen lokale Netze, sogenannte LANs (Local Area Networks) genauso wie standortübergreifende Weitverkehrsnetze, sogenannte WANs (Wide Area Networks – das Internet ist sicher das prominenteste davon) miteinander verbunden sind, ist die Gefahr durch unbefugte Zugriffe zu keinem Zeitpunkt auszuschließen. Die Anbindung der lokalen Netze an Weitverkehrsnetze wie das Internet vergrößert diese Bedrohung noch weiter, da Angreifer nun von überall in der Welt versuchen können, IT Systeme zu kompromittieren. Sowohl hochprofessionalisierte Gruppen mit verbrecherischer Absicht wie auch begabte Einzeltäter, denen es in erster Linie auf eine gewisse Bekanntheit durch die Penetration von Sicherheitssystemen bekannter Namen der deutschen Wirtschaft ankommt, stellen eine reale Bedrohung für alle Unternehmen dar.

Im Folgenden sollen nun zuerst die Rahmenbedingungen von IT-Sicherheit aufgezeigt werden. Anschließend sollen unter Zuhilfenahme der wichtigsten Standards[2] für IT-Sicherheit (ISO/IEC 27001, Common Criteria, BSI IT-Grundschutz und IT-SEC) generelle Kriterien für sichere IT-Systeme definiert und vorgestellt werden.

[2] Detailinformationen zu den einzelnen Standards können im Literatur- und Quellenverzeichnis abgerufen werden.

2 Was ist IT-Sicherheit?

Ein IT-System stellt einen systematischen Verbund informationstechnischer Komponenten dar. Für diesen Verbund existieren verschiedene Risiken. IT-Sicherheit bezeichnet die Abwesenheit dieser Risiken für ein IT-System.
Eine weitere Definition liefert das Bundesamt für Sicherheit in der Informationstechnik (BSI): *„IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind.“*[3]

Es existieren verschiedene **IT-Sicherheitsziele**:

- Vertraulichkeit

  Sicherheit vor unbefugtem Zutritt, Zugang oder Zugriff

- Integrität

  Sicherheit vor unbefugter Modifikation von Informationen

- Verfügbarkeit

  Sicherheit vor Beeinträchtigung der Funktionalität von IT-Systemen oder des Zugangs zu IT-Systemen

IT-Sicherheit ist gewährleistet, wenn die Sicherheitsziele für das jeweils betrachtete System durch angemessene Maßnahmen erreicht werden.

Die Erreichung tritt nicht automatisch ein, da für die jeweilige Organisation verschiedene **Bedrohungen** existieren. Eine Bedrohung stellt ein Ereignis dar, „*das die Sicherheitsziele […] eines Wertes der Organisation beeinträchtigt.*“[4] Es wird versucht, „*eine oder mehrere Schwachstellen oder Verwundbarkeiten auszunutzen, um einen Verlust der Datenintegrität, der Informationsvertraulichkeit oder der Verfügbarkeit zu erreichen, oder um die Authentizität von Subjekten zu gefährden.*“[5]

Hierzu zählen folgende Bedrohungen:

- Höhere Gewalt (Erdbeben, Feuer etc.)
- Vorsätzliches Handeln (Manipulation, Hacking, Wirtschaftsspionage etc.)
- Fahrlässigkeit und menschliches Fehlverhalten
- Technisches Versagen (Hardware- oder Stromausfall etc.)

[3] BSI (2007), S. 44.
[4] Kersten (2008), S. 42.
[5] Eckert (2008), S. 15.

- Organisatorische Mängel (Fehlendes oder mangelhaftes Berechtigungskonzept, ungeschultes Personal, Missmanagement etc.)

Als Folge eingetretener Bedrohungen können für Unternehmen unterschiedliche schädliche Szenarien zur Wirklichkeit werden. Eine kleine Auswahl:

- Monetäre Schäden bis hin zur Einstellung des Geschäftsbetriebs
- Imageverlust mit daraus resultierenden Problemen im Bereich Produktvermarktung, Personalmarketing, Kundenbindung etc.
- Verlust der Kreditwürdigkeit führt zu Problemen bei der Kapitalbeschaffung und schlechteren Rating-Ergebnissen.

Um IT-Sicherheit effektiv betreiben zu können bedarf es eines **IT-Sicherheitsmanagements**. Dieses hat zur Aufgabe, *„die zum Teil wechselnden Risikosituationen im Zusammenhang mit Informationen in einem ständigen Prozess festzustellen und den Umständen entsprechend angemessen zu bewältigen."*[6]
Der genannte Prozess beinhaltet die Entwicklung, den Betrieb und die kontinuierliche Verbesserung des Sicherheitsmanagements einer Organisation.
Das IT-Sicherheitsmanagement stellt eine Teilaufgabe des betrieblichen Risikomanagements.

[6] Königs (2006), S. 110.

3 Sicherheitsziele und Maßnahmen für sichere IT-Systeme

Um die Sicherheit einer Software zu gewährleisten, sollten die verschiedenen IT-Sicherheitsziele aus Abschnitt 2 berücksichtigt werden. Konkret auf Software übertragen können folgende Detailaspekte gewährleisten, dass Software die genannten IT-Sicherheitsziele erreicht:

- **Vertraulichkeit der Daten (IT-Sicherheitsziel *Vertraulichkeit)***

IT-Systeme und darauf gespeicherten Daten und Informationen müssen vor unberechtigtem Zugriff geschützt werden. Je größer die physikalischen Zugriffsmöglichkeiten auf die IT-Systeme sind, desto größer sind die Anforderungen an die IT-Sicherheit. Dabei sollte vor allem geachtet werden, dass Daten mit zunehmender Wichtigkeit auch eines größeren Sicherungsaufwands bedürfen: Hoch sensible Daten dürfen unter keinen Umständen in die Hände Unbefugter gelangen.
Des Weiteren muss die Software so konzipiert sein, dass Daten nur für den berechtigten Benutzer sichtbar sind.
Generell kann festgehalten werden, dass bei den im Folgenden genannten IT-Sicherheitsmechanismen immer das Prinzip des „Minimums an Rechten" angewendet werden soll: Wird ein Anwender nicht explizit für einen Dienst, einen System- oder Datenzugriff freigeschaltet, ist das Recht dazu vorerst zu untersagen.

<u>Generische Maßnahmen zu Erreichung dieses IT-Sicherheitsziel:</u>

- Zutrittskontrollen

  Der Zutritt zu Räumlichkeiten, in welchen IT-Systeme mit hochsensiblen Daten vorgehalten werden sollte reglementiert werden. Hierzu zählt in erster Linie das Rechenzentrum oder ähnliche Räumlichkeiten, in welchen die Serversysteme und darauf enthaltenen Daten gehostet werden.

  Beispielhafte Maßnahmen:
  Schließsysteme, Zutrittsmedien wie Chipkarten oder per Code-Eingabe, Zutrittsprotokollierung oder Zutrittsverweigerung für Dritte wie Putzkräfte oder Lieferanten. Diese Zutrittsmöglichkeiten müssen mit Hilfe eines angemessenen Prozesses vergeben, kontrolliert und entzogen werden können.

- Zugangskontrollen

  Auf IT-Systemen und Endgeräten, welche den Zugriff auf sensible Daten gewährleisten, sollten Zugangskontrollen eingerichtet werden. Es geht dabei um eine sichere Identifikation mit anschließender Authentifikation des Nutzers.

  Beispielhafte Maßnahmen:
  Zugang zum System nur mit Passworteingabe (das Passwort sollte eine ausreichende Güte aufweisen, regelmäßig geändert werden müssen und per Bildschirmsperre nach Verlassen des jeweiligen IT-Systems wieder erzwungen werden). Des Weiteren kann z. B. durch eine physikalische

und/oder logische Trennung von Diensteserver (auf welchem z. B. die zentrale Datenbank läuft) und externen Netzen angeführt werden. Dies kann z. B. durch Einsatz von Sicherheitskonzepten wie Firewall, demilitarisierten Zonen oder Abschottung logischer Netzabschnitte durch virtuelle LANs erreicht werden.
Analog zu den Zutrittsmöglichkeiten müssen auch Zugangsmöglichkeiten durch einen angemessenen Prozess vergeben, kontrolliert und entzogen werden.

- Zugriffskontrollen

  Auf Basis der Zugangskontrolle (deren Existenz eine notwendige Bedingung für eine effektive Zugriffskontrolle darstellt) baut der Bereich der Zugriffskontrolle auf, mit der Berechtigten (d. h. per Zugangskontrolle authentifizierte Personen) definierte Rechte zum Zugriff auf Dateien, Applikationen und Schnittstellen zugewiesen werden. Zu diesen Rechten zählt z. B. das Löschen, verändern, lesen, sperren oder kopieren von Daten.

  Beispielhafte Maßnahmen:
  Für die Verwaltung von Zugriffsrechten sollte ein Zugriffsrechtekonzept erarbeitet werden, welches auf einem Rollenmodell basiert. Jeder Rolle werden notwendige Systemfunktionalitäten zugewiesen, welche mit den entsprechenden Rechten hinterlegt werden. Somit kann verhindert werden, dass Unberechtigte Zugriff auf für sie nicht relevante Bereiche erhalten. Dieses Berechtigungskonzept sollte mit Hilfe eines Prozesses umgesetzt werden, welcher die Zugriffsberechtigungen systematisch vergibt, kontrolliert und entzieht.

- Übertragungssicherheit

  Daten werden unter Zuhilfenahme von elektronischen Kommunikationsmedien innerhalb einer Organisation und zwischen Organisationen und Dritten versendet. Diese Datenübertragung muss so abgesichert werden, dass Dritte die Daten auf dem Versandweg abfangen und einsehen können.

  Beispielhafte Maßnahmen:
  Übertagung von Daten nur unter Verwendung sicherer Übertragungswege (Beispiele sind z. B. VPN oder sFTP). Des weiteren sollte ein Verschlüsselungskonzept vorhanden sein, welches sowohl eine lokale Verschlüsselung von Daten (z. B. durch eine Software, welche bei Ausschalten von mobilen Geräten den kompletten Dateninhalt verschlüsselt um bei einem Verlust des Geräts die Daten für Dritte nicht zugänglich zu machen) als auch eine Verschlüsselung bei Übertragung (z. B. durch Einsatz von PKI-Systemen bei Datenübertragung per E-Mail) vorsieht.

- **Integrität/Korrektheit der Daten (IT-Sicherheitsziel *Integrität*)**

Die Software muss Eingaben zwingend korrekt verarbeiten und richtige Ergebnisse liefern. Änderungen von Daten müssen sich an die vorgesehenen Art und Weise

orientieren. Datenmanipulationen müssen verhindert werden. Die Nachvollziehbarkeit von Dateneingaben und –Änderungen stellt einen weiteren wichtigen Punkt dar.

Generische Maßnahmen zu Erreichung dieses IT-Sicherheitsziel:

- Im jeweiligen IT-System selbst sollte systemseitig durch effektive Kontrollen vermieden werden, dass es zu fehlerhafter Verarbeitung kommt. Hierzu bieten sich z. B. Plausibilitätschecks an, welche die korrekte Datenverarbeitung überprüfen und somit gewährleisten.
- Fehler bei der manuellen Dateneingabe in ein IT-System sollten dadurch ausgeschlossen werden, indem sie sich an systemtechnischen Vorgaben orientieren, um eine Fehleingabe aufgrund von z. B. falscher Schreibweise zu verhindern.
- Dateneingaben und Änderungen sollten des Weiteren immer anhand des Authentifizierungskonzept nachvollziehbar bleiben, z. B. sollte man immer ermitteln können, wer wann welche Eingaben und/oder Änderungen durchgeführt hat. Hierzu bietet sich ein Protokollierungssystem an. Diese Maßnahmen der Eingabekontrolle dienen zusätzlich der zur Nachvollziehbarkeit auch der Dokumentation der Datenverwaltung und -pflege.

- **Verfügbarkeit des IT-Systems (IT-Sicherheitsziel *Verfügbarkeit*)**

Software hat jederzeit die gewünschte Funktionalität zur Verfügung zu stellen. Sie muss jederzeit in der Lage sein, auf Anfragen in einem angemessenen zeitlichen Rahmen zu reagieren. Sollte die Software abstürzen, sollten Zwischenergebnisse wiederherstellbar sein und der jeweilige Dienst sollte sich, wenn technisch möglich, selbst regenerieren.

Generische Maßnahmen zu Erreichung dieses IT-Sicherheitsziel:

- Das Rechenzentrum mit den zentralen Serversystemen muss gegen Wassereintritt, Feuer etc. geschützt sein. Maßnahmen reichen hier von feuerfesten Türen und Wänden über Outsourcing des Rechenzentrums an einen spezialisierten Anbieter bis hin zu Schaffung von Redundanz durch Errichtung eines zweiten Rechenzentrums.
- Innerhalb des Rechenzentrums ist durch verschiedene Maßnahmen dafür zu sorgen, dass IT-Systeme und Daten jederzeit verfügbar sind. Hierzu zählen eine unterbrechungsfreie Stromversorgung (USV), der Einsatz von Klimaanlagen, Implementierung eines effizienten Datensicherungs- und Wiederherstellungsverfahrens, Spiegelung von Systemen oder der Einsatz eines effektiven Virenschutzkonzepts.
- Trennung der IT-Systeme in Entwicklungs-, Test- und Produktivsysteme um das Schadensausmaß von Fehlern, die die Verfügbarkeit einschränken könnten, zu minimieren.
- Absicherung von Internetdiensten (Webseite, Online-Banking, Kreditkartenzahlung etc.)
- Im Rahmen der Verfügbarkeit sollte auch ein Konzept existieren, welches im Katastrophenfall (z. B. Feuer im Gebäude, welches das Rechenzentrum

zerstört) für einen funktionierenden Notbetrieb und einen reibungslosen Wiederanlauf der IT-Systeme sorgt.

- **IT-Sicherheitsmanagement (Übergreifende IT-Sicherheitsaufgabe)**

Um IT-Sicherheit effektiv betreiben zu können bedarf es einem strukturierten Ansatz im Rahmen des IT-Sicherheitsmanagements. Diese Funktion hat die Entwicklung, den Betrieb und die kontinuierliche Verbesserung des IT-Sicherheitskonzepts einer Organisation zur Aufgabe.

Generische Maßnahmen des IT-Sicherheitsmanagements:

- Erstellung einer IT-Sicherheitsleitlinie, welche die Vorgaben für IT-Sicherheit an die Organisation enthält.
- Etablierung einer effektiven IT-Sicherheitsorganisation, welche diese Teildisziplin der Unternehmens-IT verantwortet.
- Entwicklung der Vertraulichkeitsvereinbarung
- Pflege der Kontakte zu relevanten Behörden und Interessengruppen
- Identifizierung von Risiken durch Kooperation mit externen Dritten
- Zyklische Durchführung von externen IT-Sicherheitsaudits
- Management von Sicherheitsvorfällen

Fazit:

Um ein IT-System sicher zu machen ist eine Reihe an IT-Sicherheitszielen zu erreichen. Diese Ziele können durch eine Auswahl der genannten generischen Maßnahmen erreicht werden. Da es sich jedoch um generische Maßnahmen handelt, sollte beachtet werden, dass ein spezifisches IT-Sicherheitskonzept in einer Organisation immer im Rahmen einer individuellen Risikoanalyse ermittelt, entwickelt, eingeführt und stetig verbessert werden sollte.

Haben Sie weitere Fragen zur Implementierung von IT-Sicherheitskonzepten oder generelle Fragen zu IT-Sicherheit, Datenschutz oder betrieblicher IT-Kontinuität? Bitte sprechen Sie uns direkt an, wir stehen Ihnen gerne für ein Gespräch zur Verfügung!

Kontakt:

Dr. Thomas Jurisch
Geschäftsführender Partner
INTARGIA Managementberatung GmbH
Max-Planck-Straße 20
63303 Dreieich

Telefon: +49 (0)6103 / 5086-0
Telefax: +49 (0)6103 / 5086-45
E-Mail: thomas.jurisch@intargia.com
Internet: http://www.intargia.com

Literatur- und Quellenverzeichnis

BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2007): BSI IT-Grundschutzkataloge, Stand 2007 (9. Ergänzungslieferung), http://www.bsi.bund.de/gshb/deutsch/download/it-grundschutz-kataloge_2007_de.pdf, abgefragt am 19.12.2008.

Capgemini (2008): Studie IT-Trends 2008 – IT-Leiter im Spagat zwischen Dienstleister und Business Partner, http://www.de.capgemini.com/m/de/tl/IT-Trends_2008.pdf, abgefragt am 19.10.2008.

CCRA (Hrsg.): Common Criteria for Information Technology Security Evaluation, Version 3.1, http://www.commoncriteriaportal.org/thecc.html, abgefragt am 19.12.2008.

Deloitte (2007): Global Security Survey – The shifting security paradigm, http://www.deloitte.com/dtt/cda/doc/content/ca_en_Global_Security_Survey.final.en.pdf, abgefragt am 21.12.2008.

Dierstein, R. (2004): Sicherheit in der Informationstechnik – der Begriff IT-Sicherheit in Spektrum der Informatik, Nr. 27/2004.

Eckert, C. (2008): IT-Sicherheit. Konzepte, Verfahren, Protokolle, Oldenbourg Wissenschaftsverlag GmbH, München.

Ernst & Young (2007): Global Information Security Survey 2007, http://www.ey.com/global/Content.nsf/International/Assurance_&_Advisory_-_Technology_and_Security_Risk_-_Global_Information_Security_Survey_2007, abgefragt am 21.12.2008.

ISO: ISO/IEC 27001:2008-09, Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme - Anforderungen (ISO/IEC 27001:2005), http://www.beuth.de/langanzeige/DIN+ISO%2FIEC+27001/en/103960154.html&limitationtype=&searchaccesskey=SALL, abgefragt am 21.12.2008.

ISO: ISO/IEC 27002:2008-09, Informationstechnik – IT-Sicherheitsverfahren, Leitfaden für das Informationssicherheits-Management (ISO/IEC 27002:2005), http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297, abgefragt am 21.12.2008.

ITSEC - Information Technology Security Evaluation Criteria, http://www.bsi.de/zertifiz/itkrit/itsec-dt.pdf, abgefragt am 21.12.2008.

Kersten H. und J. Reuter und K.-W. Schröder (2008): IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz – Der Weg zur Zertifizierung (Edition <kes>), Vieweg+Teubner Verlag/GWV Fachverlage GmbH, Wiesbaden.

KPMG (2007): Anti Fraud Management – Best Practice der Prävention gegen Wirtschaftskriminalität, http://www.kpmg.de/docs/Anti_Fraud_Management_Best_Practice_der_Praevention_gegen_Wirtschaftskriminalitaet_de.pdf, abgefragt am 21.12.2008.

Königs, H.-P. (2006): IT-Risiko-Management mit System - Von den Grundlagen zur Realisierung - Ein praxisorientierter Leitfaden (Edition <kes>), Vieweg+Teubner Verlag/GWV Fachverlage GmbH, Wiesbaden.

Münch, I. (2007): IT-Grundschutz zum Bewältigen von IT-Risiken in Unternehmen in Managementhandbuch IT-Sicherheit – Risiken, Basel II, Recht, Erich Schmidt Verlag GmbH & Co., Berlin.

Pohlmann, N. und H. Blumberg (2004): Der IT-Sicherheitsleitfaden – Das Pflichtenheft zur Implementierung von IT-Sicherheitsstandards im Unternehmen, Verlag Moderne Industrie Buch AG & Co. KG., Bonn.

PwC (2007): The global state of information security, http://www.pwc.com/extweb/pwcpublications.nsf/docid/114E0DE67DE69653852573410 05AED7B/$FILE/PwC_GISS2007.pdf, abgefragt am 21.12.2008.

Rauschen, T. und G. Disterer (2004): Identifikation und Analyse von Risiken im IT-Bereich in HMD – Praxis der Wirtschaftsinformatik, Heft 236 – IT-Sicherheit, April 2004, dpunkt.verlag GmbH, Heidelberg.

Speichert, H. (2007): Praxis des IT-Rechts - Praktische Rechtsfragen der Internetnutzung und IT-Sicherheit (Zielorientiertes Business Computing), Vieweg+Teubner Verlag/GWV Fachverlage GmbH, Wiesbaden.

Witt, B. (2006): IT-Sicherheit, (Edition <kes>), Vieweg+Teubner Verlag/GWV Fachverlage GmbH, Wiesbaden.