



Gefördert durch das
Bundesministerium
für Wirtschaft
und Technologie



Netzwerk Elektronischer
Geschäftsverkehr



Handlungsanleitung für die Praxis

Sichere Geschäftsprozesse: Umsetzung im Unternehmen – Branchenbeispiel Maschinenbau 2

www.ec-net.de

Text und Redaktion

SAGeG Chemnitz – Kompetenzzentrum Elektronischer Geschäftsverkehr

KECoS Schwaben – Kompetenzzentrum Electronic Commerce Schwaben

MECK Würzburg – Mainfränkisches Electronic Commerce Kompetenzzentrum

ECC Handel – E-Commerce-Center Handel Köln

Layout und Satz

ECC Handel – E-Commerce-Center Handel Köln

Bildquelle

www.photocase.de

Herausgeber

KECoS Schwaben – Kompetenzzentrum Electronic Commerce Schwaben

Stand

Mai 2008

1 Vorwort

2 Ausgangssituation

3 Untersuchungsmodell

4 Allgemeine Prozessauswertung

4.1 Netzwerkstatus

4.2 Firewall-System

4.3 Anbindung externer Teile-Datenbank

4.4 Sicherstellung des laufenden Geschäftsbetriebs

4.5 Organisatorisches Sicherheitsmanagement

4.6 Personalsicherheit

5 Fazit: Aufgaben für die Unternehmensführung

6 Anhang

6.1 Das Netzwerk Elektronischer Geschäftsverkehr

6.2 Verbundprojekt „Sichere E-Geschäftsprozesse in KMU und Handwerk“

6.3 Kompetenzzentren vor Ort

7 Weiterführende Literatur

7.1 Die Reihe „Sichere Geschäftsprozesse: Umsetzung im Unternehmen“

7.2 Fachzeitschriften

7.3 Fachbücher

7.4 Websites

Sichere Geschäftsprozesse: Umsetzung im Unternehmen

1 Vorwort



Angriffe auf Firmennetze häufen sich und werden immer raffinierter. Obwohl Computerviren und andere „Schädlinge“ Millionen-schäden anrichten, unterschätzen vor allem kleine und mittelständische Unternehmen (KMU) sowie Handwerksbetriebe noch immer das Risiko.

Informations- und Netzwerksicherheit wird häufig auf technische Aspekte und schwerpunktmäßig auf Sicherheit gegen Viren reduziert. Folglich wird das Aufgabenspektrum zur IT-Sicherheit auf die Ebene der IT-Administration delegiert oder an externe Dienstleister ausgelagert. Nur in seltenen Fällen engagiert sich die Unternehmensleitung persönlich in dieser Thematik. Angesichts der Abhängigkeit vieler Unternehmen von der IT können Sicherheitsdefizite jedoch gravierende, im Extremfall sogar existenzbedrohende Folgen haben.

Bereits mit der Studie „IT-Sicherheit in Unternehmen 2007“ wurde eindrucksvoll aufgezeigt, wie es derzeit um die IT-Sicherheit in Unternehmen bestellt ist. Die Einschätzungen der Geschäftsführer und IT-Verantwortlichen unterstreichen, dass IT-Sicherheit eine ganzheitliche Managementaufgabe darstellt, wenn sie ein Unternehmen zielführend und ökonomisch sinnvoll schützen soll.

Das vom Bundesministerium für Wirtschaft und Technologie (BMWi) geförderte Netzwerk Elektronischer Geschäftsverkehr (NEG) hat es sich zur Aufgabe gemacht, insbesondere kleinen und mittelständischen Unternehmen zur Seite zu stehen und diese auch im Bereich der IT-Sicherheit durch geeignete Informationen praxisnah zu unterstützen. Im Rahmen des Projekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ wurden daher bundesweit 17 Unternehmen aus unterschiedlichen Branchen, Größen und Prozess- bzw. Lieferantenkette bei der Einführung eines IT-Sicherheitsmanagementsystems nach DIN ISO 27001 begleitet. In dieser Handlungsanleitung sind die identifizierten Hindernisse und Problemlösungen detailliert festgehalten und fundiert aufbereitet.

Informieren Sie sich mit dieser Handlungsanleitung über die zielführende Umsetzung von IT-Sicherheit und profitieren Sie davon für Ihr eigenes Unternehmen. Für Ihre Zukunft wünsche ich Ihnen viel Erfolg.

MinR Dr. Rolf Hochreiter
Bundesministerium
für Wirtschaft
und Technologie
Berlin, im Dezember 2007

Hinweis

- ▶ Die folgenden Informationen der IT-Sicherheitsanalyse zeigen beispielhaft die Relevanz des Themas für die Branche auf. Für die individuelle Bewertung der IT-Sicherheit in einem konkreten Unternehmen müssen natürlich die dortigen speziellen Rahmenbedingungen mit berücksichtigt werden.

2 Ausgangssituation



Das begutachtete Unternehmen der Maschinenbau-Branche ist eine Ausgründung einer Hochschule. Das

Unternehmen beschäftigt derzeit 12 Mitarbeiter, die mit der Entwicklung einer neuartigen Produktionstechnik beschäftigt sind. Das Unternehmen konzentriert sich ausschließlich auf die Entwicklung dieser Technik. Prozesse wie die Lohnbuchhaltung sind an einen Dienstleister ausgelagert. In Zukunft soll ein Tochterunternehmen gegründet werden, das die konzipierte Produktionsmaschine fertigt und wartet.

Die Ausgangssituation im IT Bereich

Die IT-Struktur des Unternehmens ist der Größe entsprechend relativ überschaubar. Jedoch werden zur Konstruktion und zum Test des Prototyps der Produktionsmaschine Spezialsysteme eingesetzt, die ein komplexes Umfeld im Bereich des Netzwerks schaffen.

Die **besonderen Problemfelder** der bestehenden IT-Infrastruktur sind folgende, wobei eine Reihe eingeleiteter Maßnahmen deren Risiko bereits zum jetzigen Zeitpunkt minimieren:

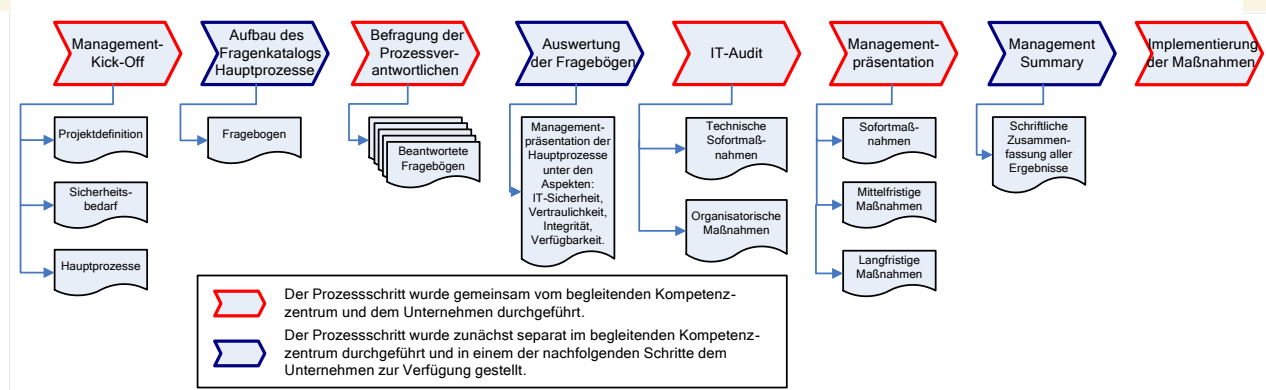
- ▶ Einbindung externer Teile-Datenbanken über das Internet,
- ▶ Absicherung von Informationsrecherche-tätigkeiten über das Internet,
- ▶ Vernetzung der Entwicklungsabteilung mit dem übrigen Unternehmensnetzwerk.

Bei dieser Betrachtung wurden sowohl technische (z. B. Netzwerkstrukturen, Virenschutz) als auch organisatorische Aspekte (z. B. Internetnutzung) untersucht.

3 Untersuchungsmodell

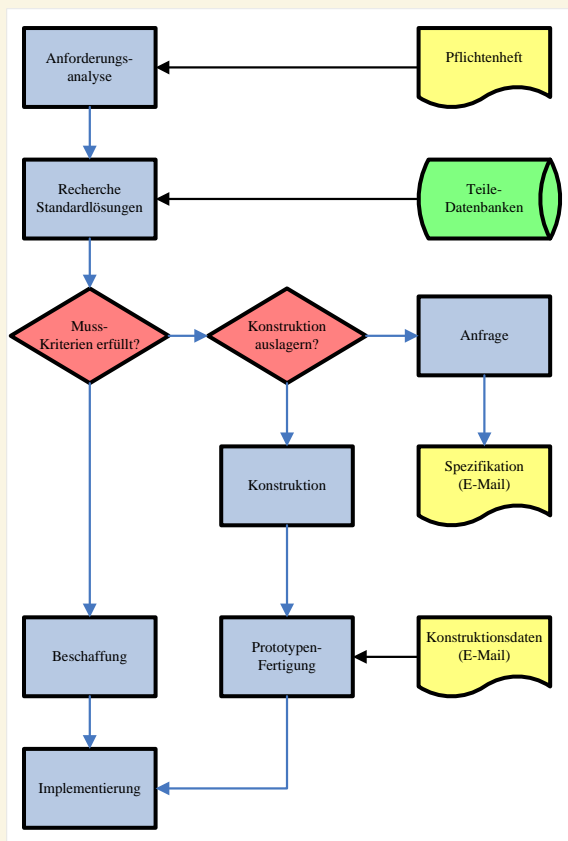
Im Rahmen der Projektaktivitäten wurden die Geschäftsprozesse im Unternehmen analysiert, die im besonderen Maße durch die Informationstechnik geprägt sind. Gemeinsam mit den Mitarbeitern des Unternehmens wurden die Zusammenhänge zwischen den Prozessschritten in

Abbildung 1: Vorgehen der Unternehmensbegleitung



der vorhandenen IT-Infrastruktur und den Anwendern dieser Infrastruktur ermittelt und aufbereitet. Im Besonderen wurden Einzelinterviews durchgeführt (siehe Abbildung 1). Daneben fanden eine begleitete und erläuterte Betriebsbegehung sowie Arbeitsplatzbesuche statt. Eine abschließende Bewertung der Ergebnisse wurde zusammen mit der Geschäftsleitung vorgenommen und es wurden Handlungsfelder identifiziert und konkretisiert.

Abbildung 2: Erfassungsbeispiel eines Prozessausschnitts des internen Projektmanagements



Für den vorliegenden Fall wurden insbesondere die nachfolgenden Prozesse analysiert:

- ▶ Anforderungs-, Anwendungs-, Softwaremanagement,
- ▶ Sicherstellung des laufenden Geschäftsbetriebs (Business Continuity Management),
- ▶ Organisatorisches Sicherheitsmanagement, wie z. B. Internet- und Telefonnutzung,

- ▶ Personalsicherheit,
- ▶ Projektmanagement.

Außerdem wurden die nachfolgenden technischen Systeme im Detail begutachtet:

- ▶ Internetzugang,
- ▶ Netzwerkumgebung,
- ▶ Server und Server-Raum.

Ausgehend von diesen Daten wurde der Status quo der Sicherheitsvorkehrungen im Unternehmen ermittelt und strukturiert aufbereitet. Die aufgearbeiteten Erkenntnisse wurden dem Unternehmen mit konkreten Handlungsempfehlungen zur Verfügung gestellt.

4 Allgemeine Prozessauswertung

4.1 Netzwerkstatus

Alle Bereiche des Unternehmens teilen sich ein gemeinsames Netzwerk. Es ist keine Trennung der einzelnen Bereiche nach Sensitivität oder Funktion vorhanden, auch wenn die eingesetzten Netzwerktechnologien diese Möglichkeit bieten.

Empfehlung

- ▶ Das Netzwerk für die Konstruktions- und Test-Systeme sollte separiert werden. Die eingehenden und auch ausgehenden Kommunikationsmöglichkeiten dieser Teilnetzwerke sollten eingeschränkt werden.

4.2 Firewall-System

Das eingesetzte Firewall-System übernimmt gleichzeitig die Aufgabe des Virenschutzes und bietet die Möglichkeit zur Bildung einer sogenannten demilitarisierten Zone (DMZ; spezielle Zone innerhalb einer Firewall, deren Zugriff geschützt ist und von der Firewall kontrolliert wird). Zurzeit werden Sicherheitsvorkommnisse zwar von dem System protokolliert, jedoch nicht

ausgewertet. Das System ist so konfiguriert, dass jedwede Kommunikation aus den Netzwerken in das Internet erlaubt ist.

Empfehlung

- ▶ Die Firewall-Regeln sollten so präzisiert werden, dass keine unerlaubte Kommunikation aus den zu schützenden Netzwerken in das Internet erfolgen kann.
- ▶ Ein Managementprozess, der regelmäßig die Firewall-Regeln, die anfallenden Protokolle und die Aktualität der Firewall und des Virenschutzes sicherstellt, sollte initiiert werden.

4.3 Anbindung externer Teile-Datenbank

Für den Entwicklungsprozess werden Daten zur Konstruktion in Form von CAD-Dateien für Baugruppen und Datenblätter benötigt. Diese werden über das Internet aus externen Quellen beschafft. Zurzeit werden diese Daten direkt zu den Konstruktionssystemen übertragen.

Empfehlung

- ▶ Eine DMZ der Firewall, in der ein System zur Zwischenprüfung derartiger Daten und anschließenden Übertragung zu dem Konstruktionssystem betrieben wird, sollte eingerichtet werden.
- ▶ In der DMZ sollte ein Client-Server-System für den Transfer der Bilddaten vom Server auf das Konstruktionssystem, sowie für gesicherte Internetrecherchen eingerichtet werden.

4.4 Sicherstellung des laufenden Geschäftsbetriebs

Die Sicherstellung des Geschäftsbetriebs (Business Continuity Management) ist eine gesetzlich reglementierte Aufgabe (KonTraG) der Geschäftsführung. Eine Missachtung dieser Aufgabe hat besondere Haftungsrisiken für die

Geschäftsleitung zur Folge, die nicht durch Versicherungen abgedeckt werden können.

Das im Unternehmen vorhandene Backup-System sichert die Konstruktionsdaten über sieben Datengenerationen hinweg. Ein Test der vollständigen Wiederherstellung der Datenbanken und Systeme wurde bisher nicht durchgeführt.

Empfehlung

- ▶ Erstellung von Monatsdatenträgern für das Backup-System und Dokumentation des Alters der verwendeten Backup-Medien,
- ▶ Test einer vollständigen Wiederherstellung der Datenbanken und Systeme,
- ▶ mittelfristiger Aufbau eines detaillierten Business-Continuity-Plans unter Berücksichtigung zeitkritischer Faktoren, wie z. B. E-Mail, Telefon, Hauptlogistikanwendungen,
- ▶ regelmäßige Überprüfung und Anpassung des Business-Continuity-Plans.

4.5 Organisatorisches Sicherheitsmanagement

Die private Nutzung des Internetzugangs und des dienstlichen E-Mail-Kontos ist im Unternehmen nicht reglementiert. Gleiches gilt für die private Telefon- und Mobiltelefonnutzung. Weitere Sicherheitsrisiken entstehen im Zusammenhang mit dem physischen Zugang von Lieferanten und Kunden, externen Dienstleistern der Gebäudereinigung und der Dokumentenbeseitigung.

Empfehlung

- ▶ Es sollte ein Sicherheitsleitfaden eingeführt werden, aus dem Sicherheitsrichtlinien und entsprechende Arbeitsanweisungen für die Mitarbeiter hervorgehen. Deren Umsetzung und Einhaltung sollte kontinuierlich geprüft werden.

4.6 Personalsicherheit

Im Hinblick auf IT-Sicherheitsaspekte besteht ein regelmäßiger Schulungsbedarf der Mitarbeiter. Derzeit sind die Mitarbeiter zu Aspekten der unternehmerischen Gefahren und Risiken der freien Nutzung von Internet und E-Mail nicht ausreichend sensibilisiert.

Empfehlung

- ▶ Weiterbildungen sollten innerhalb eines Schulungs- und Sensibilisierungsplans angeboten werden, die alle Mitarbeiter der Verwaltung regelmäßig durchlaufen sollten.

5 Fazit: Aufgaben für die Unternehmensführung

Die Unternehmensführung hat die Sicherheit der IT-Ressourcen als wichtiges Element in den Unternehmensprozessen erkannt. Eine Verbesserung der Sicherheit der IT-Prozesse stellt künftig eine wichtige Aufgabe dar.

Empfehlung

- ▶ Für den Schadens- und Notfall sollten die aufgeführten Dokumentationen entwickelt und in Papierform gesichert abgelegt werden. Diese sollten auch solche Unterlagen umfassen, die eventuell durch Dienstleister bereitgestellt werden müssen.
- ▶ Schulungen der Mitarbeiter zu Fragen der IT-Sicherheit sollten wiederkehrend durchgeführt werden.
- ▶ Eine schriftliche Regelung der privaten Nutzung der IT-Infrastruktur und des Internets sollte getroffen werden.
- ▶ Die nachfolgenden administrativen Aufgaben sollten kontinuierlich umgesetzt werden: Nutzerverwaltung, tägliche Netzüberwachung, Sicherheit der IT-Struktur (Updates, Sicherheits-Patches einpflegen), arbeitsplatzbezogene Schulung der Mitarbeiter bei

neuen Anforderungen, Planung der Ressourcen (Hardware und Software), ständige eigene Weiterbildung, Durchführung der Backup- und Archivierungsprozesse. Die zeitlichen Ressourcen sollten entsprechend bereitgestellt werden.

- ▶ Es sollten separate Netzwerke für die Konstruktions- und Testsysteme eingerichtet werden.
- ▶ Das Firewall-System sollte hinsichtlich der Firewall-Regeln, der Protokolle, der Aktualität sowie des Virenschutzes regelmäßig überprüft werden.
- ▶ Für die Anbindung externer Teile-Datenbanken sollten eine DMZ und ein Server-Client-System eingerichtet werden.
- ▶ Die bereits erfüllten und die weiteren genannten Empfehlungen sollten als wesentliche Bausteine auf dem Weg der IT-Zertifizierung (Selbstzertifizierung) verstanden werden.
- ▶ Zielführende, ökonomisch tragfähige IT-Sicherheit stellt eine ganzheitliche Managementaufgabe dar. Hier sollte eine kontinuierliche Kommunikation von Zielen und Veränderungsprozessen zwischen Geschäftsführung, IT-Mitarbeitern und Anwendern erfolgen.
- ▶ Bei der Analyse der IT-relevanten Prozesse im Unternehmen wurde kein Belastungstest an der vorhandenen IT-Infrastruktur vorgenommen. Aus diesem Grund kann keine Einschätzung der Wirksamkeit der installierten Sicherheitsmaßnahmen (Firewall, Virenschutz, Zugangsschutz, Verschlüsselung usw.) vorgenommen werden. Es wird empfohlen, die Wirksamkeit der Schutzmaßnahmen durch einen unabhängigen Dienstleister in regelmäßigen Abständen überprüfen zu lassen.

6 Anhang

6.1 Das Netzwerk Elektronischer Geschäftsverkehr

Das Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt seit Mitte 1998 das NEG. Mit heute insgesamt 25 regionalen Kompetenzzentren sowie einem Branchenzentrum (Handel) für den elektronischen Geschäftsverkehr ist es seine Aufgabe, Mittelstand und Handwerk zum Thema E-Business neutral zu informieren und beim Einsatz von Lösungen zu beraten.

Die Internetplattform www.ec-net.de stellt alle Zentren im Netzwerk und deren Kooperationspartner vor. Sie bietet einen Überblick über das Leistungsangebot für kleine und mittlere Unternehmen. Zudem werden zahlreiche Informationsmaterialien zum kostenfreien Download angeboten.

Das Angebot für Mittelstand und Handwerk umfasst:

- ▶ Neutrale Beratung und Informationen für den Einstieg ins E-Business,
- ▶ Kompetenz in Spezialthemen für die individuelle Anwendung von E-Business-Lösungen,
- ▶ Seminare, Workshops und Schulungen für die Qualifikation von Unternehmen,
- ▶ Leitfäden, Checklisten und Best-Practice-Beispiele als Hilfe zur Selbsthilfe,
- ▶ Marktbeobachtungen, Dienstleisterdatenbanken und regionale Websites für Unternehmen in deren Region.
- ▶ Das Netzwerk arbeitet eng mit der Initiative PROZEUS – Prozesse und Standards (www.prozeus.de) zusammen, die ebenfalls durch das BMWi gefördert wird.



6.2 Verbundprojekt „Sichere E-Geschäftsprozesse in KMU und Handwerk“

Im Projekt „Sichere E-Geschäftsprozesse in KMU und Handwerk“ fand eine Begleitung von bundesweit 17 Unternehmen aus unterschiedlichen Branchen, Größen und Prozess- bzw. Lieferantenketten bei der Einführung eines IT-Sicherheitsmanagementsystems nach DIN ISO 27001 statt. Hindernisse und Problemlösungen wurden detailliert festgehalten, aufbereitet und mit Zustimmung der Unternehmen in der Handlungsanleitungsreihe „Sichere Geschäftsprozesse: Umsetzung im Unternehmen“ veröffentlicht. Neben der Unternehmensbegleitung und der Dokumentation in den Handlungsanleitungen setzt sich das Gesamtprojekt aus den nachfolgenden Tätigkeiten zusammen:

- ▶ Die im August 2007 veröffentlichte Studie „IT-Sicherheit in Unternehmen 2007“ zeigt auf, wie es um die IT-Sicherheit in Unternehmen bestellt ist und welche Folgen ein IT-Ausfall aus Sicht der Befragten haben kann. An der zugrunde liegenden Online-

Befragung beteiligten sich von Dezember 2006 bis April 2007 bundesweit 275 Unternehmen. Den kompletten Berichtsband finden Sie zum kostenlosen Download unter: http://www.ecc-handel.de/it-sicherheit_in_unternehmen_2007.php

- ▶ Die bundesweite NEG-Roadshow „Brennpunkt IT-Sicherheit“ begleitet das Verbundprojekt im ersten und zweiten Halbjahr 2007 mit insgesamt 20 Veranstaltungen. Eine Veranstaltungsübersicht finden Sie auf [ec-net.de](http://www.ec-net.de/EC-Net/Navigation/root,did=205394.html) unter: <http://www.ec-net.de/EC-Net/Navigation/root,did=205394.html>
- ▶ Aktuelle und neutrale Informationen zur IT-Sicherheit werden Ihnen im Internet auf der Informationsplattform des NEG unter der Rubrik „Netz- und Informationssicherheit“ angeboten: <http://www.ec-net.de/EC-Net/Navigation/netz-informationssicherheit.html>

Das Projektteam IT-Sicherheit:

The image shows a map of Germany with several cities circled in red, indicating project locations. Red lines connect these locations to the names of team members. The cities circled are Köln, Chemnitz, Würzburg, and Heidenheim. The team members and their associated logos are:

- ECC** (E-Commerce-Center Handel): Dr. Kai Hudetz, Andreas Duscha
- KECoS** (Kompetenz-Zentrum Electronic Commerce Schwaben): Prof. Dr. Hans-Jürgen Ott, Markus Wirth, Stephan Rogge
- SAGeG** (Kompetenzzentrum Elektronischer Geschäftsverkehr): Dagmar Lange (Projektleiterin), Prof. Dr. Günther Neef
- m/e/c/k** (Sicherheit im Internet): Andreas Gabriel

The map also includes a legend for the locations:

- Regionales Kompetenzzentrum (yellow dot)
- Branchen-Kompetenzzentrum (orange dot)
- externe Netzwerkpartner (green dot)

6.3 Kompetenzzentren vor Ort

Wir hoffen, dass Ihnen diese Handlungsanleitung als wertvolle erste Hilfestellung bei der Planung und Durchführung Ihres IT-Sicherheitsprojekts dient.

Für entsprechende Fragen stehen wir Ihnen gerne zur Verfügung:

Kompetenzzentrum

SAGeG Chemnitz

Strasse der Nationen 25

09111 Chemnitz



Ansprechpartner:

Dagmar Lange

Telefon: 0371 690012-11

Fax: 0371 69001912-11

E-Mail: langed@chemnitz.ihk.de

Kompetenzzentrum

KECoS Schwaben

Schmelzofenvorstadt 33

89520 Heidenheim



Ansprechpartner:

Markus Wirth

Telefon: 07321 38-1828

Fax: 07321 38-1829

E-Mail: wirth@kecos.de

Kompetenzzentrum

MECK Würzburg

Neubaustraße 66

97070 Würzburg



Ansprechpartner:

Andreas Gabriel

Telefon: 0931 3501-231

Fax: 0931 31-2955

E-Mail: gabriel@meck-online.de

7 Weiterführende Literatur

Nachfolgend finden Sie eine Auswahl an Literatur und Internetadressen zum Einstieg bzw. zur Vertiefung des Themas (jeweils in alphabetischer Reihenfolge).

7.1 Die Reihe „Sichere Geschäftsprozesse: Umsetzung im Unternehmen“

In dieser Reihe von Handlungsanleitungen erscheinen die nachfolgenden, branchenspezifischen Broschüren zur Umsetzung von IT-Sicherheit im Unternehmen:

- ▶ Branchenbeispiel Handwerk 1
- ▶ Branchenbeispiel Handwerk 2
- ▶ Branchenbeispiel Einzelhandel
- ▶ Branchenbeispiel Produktion/Großhandel
- ▶ Branchenbeispiel Maschinenbau 1
- ▶ Branchenbeispiel Maschinenbau 2
- ▶ Branchenbeispiel Maschinenbau 3
- ▶ Branchenbeispiel Sondermaschinenbau
- ▶ Branchenbeispiel Textilindustrie
- ▶ Branchenbeispiel Logistik
- ▶ Branchenbeispiel Öffentliche Verwaltung
- ▶ Branchenbeispiel Finanzwesen/Versicherung
- ▶ Branchenbeispiel Gesundheitswesen
- ▶ Branchenbeispiel Automatisierungs-/Wartungstechnik
- ▶ Branchenbeispiel Informationstechnik
- ▶ Branchenbeispiel Anlagenbau
- ▶ Branchenbeispiel Umwelt-/Geotechnik

7.2 Fachzeitschriften

„<kes> – Die Zeitschrift für Informations-Sicherheit“ der SecuMedia-Verlags-GmbH, Fachmagazin für IT-Sicherheitsmanager und Rechenzentrumsleiter.

„c't magazin für computertechnik“ der Heise Zeitschriften Verlag GmbH & Co. KG, IT-Fachliteratur für ambitionierte Anwender und Computer-Profis.

„iX Magazin für professionelle Informationstechnik“ der Heise Zeitschriften Verlag GmbH & Co. KG, IT-Profimagazin für IT-Fachleute, Berater, Softwareentwickler, System- und Netzwerkverwalter.

„eCommerce Magazin“ des WIN-Verlags, Magazin für Entscheider, das IT-Sicherheits-Fragestellungen aufgreift.

„IT-Sicherheit – Fachmagazin für Informationstechnik und Compliance“ der DATAKONTEXT GmbH, Fachzeitschrift für CIO's, das Security- und IT-Management, die IT-Revision und die IT-Administration.

7.3 Fachbücher

- Aebi, Daniel: Praxishandbuch Sicherer IT-Betrieb, 2004.
- Bundesamt für Sicherheit in der Informationstechnik: IT-Sicherheitsmanagement und IT-Grundschutz, BSI-Standards zur IT-Sicherheit, 2006.
- Bursch, Daniel: IT-Security im Unternehmen, Grundlagen, Strategien, Check-up, 2005.
- Eckert, Claudia: IT-Sicherheit, Konzepte – Verfahren – Protokolle, 2006.
- Gründer, Torsten/Schrey, Joachim: Managementhandbuch IT-Sicherheit, Risiken, Basel II, Recht, 2007.
- Kersten, Heinrich/Klett, Gerhard/Wolfenstetter, Klaus-Dieter (Hrsg.): Der IT Security Manager, Expertenwissen für jeden IT Security Manager – Von namhaften Autoren praxisnah vermittelt, 2005.
- Pohlmann, Norbert/Blumberg, Hartmut: Der IT-Sicherheitsleitfaden, 2006.
- Reinhard, Tim/Pohl, Lorenz/Capellaro, Hans-Christoph: IT-Sicherheit und Recht, 2007.
- Schmidt, Klaus: Der IT Security Manager, 2006.
- Schneier, Bruce: Secrets and Lies, IT-Sicherheit in einer vernetzten Welt, 2004.
- Witt, Bernhard Carsten: IT-Sicherheit kompakt und verständlich. Eine praxisorientierte Einführung, 2006.

7.4 Websites

- <http://www.bsi.de>
Website des Bundesamts für Sicherheit in der Informationstechnik; kostenfrei.
- <http://www.competence-site.de/it-sicherheit>
Online-Wissensportal der NetSkill AG, Düsseldorf; kostenfrei.
- http://www.computerwoche.de/knowledge_center/it_security
Online-Portal der Computerwoche; kostenfrei.
- <http://www.ecc-handel.de/sicherheit.php>
Themenspezifische Informationen des E-Commerce-Center Handel, Köln; kostenfrei.
- <http://www.ec-net.de> („Themenbereich Netz- und Informationssicherheit“)
Online-Portal des Netzwerks Elektronischer Geschäftsverkehr; kostenfrei.
- <http://www.heise.de>
Online-Informationsportal der Heise Zeitschriften Verlag GmbH & Co. KG; kostenfrei.
- <http://www.kes.de>
Online-Portal zur Zeitschrift <kes> – Die Zeitschrift für Informations-Sicherheit; teilweise kostenfrei.



Netzwerk Elektronischer Geschäftsverkehr



KECoS
Kompetenz-Zentrum
Electronic Commerce
Schwaben

Diese Broschüre wird vom regionalen Kompetenzzentrum KECoS Schwaben im Rahmen des Begleitprojektes „Sichere E-Geschäftsprozesse in KMU und Handwerk“ als Teil der BMWi-Förderinitiative „Netzwerk Elektronischer Geschäftsverkehr“ herausgegeben.