



Gefördert durch das
Bundesministerium
für Wirtschaft
und Technologie



Netzwerk Elektronischer
Geschäftsverkehr



Handlungsanleitung für die Praxis

Sichere Geschäftsprozesse: Umsetzung im Unternehmen – Branchenbeispiel Finanz- und Versicherungswesen

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

März 2008

1 Vorwort

2 Ausgangssituation

3 Untersuchungsmodell

4 Prozessauswertung

4.1 Netzwerkstatus

4.2 Interner und externer Datenfluss

4.3 Serverarchitektur

4.4 Softwareentwicklungsprozess

4.5 Datenschutz

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 Versicherungs-, Investment- und Finanzbranche bietet seit 2002

mittels Internetportaltechnik vielfältige Vermittlungsdienstleistungen für Endverbraucher und entsprechende Branchenexperten an. Die Website des Unternehmens erlaubt Verbrauchern eine direkte Personensuche untergliedert nach Tätigkeitsschwerpunkten, nach Postleitzahlen oder Namen.

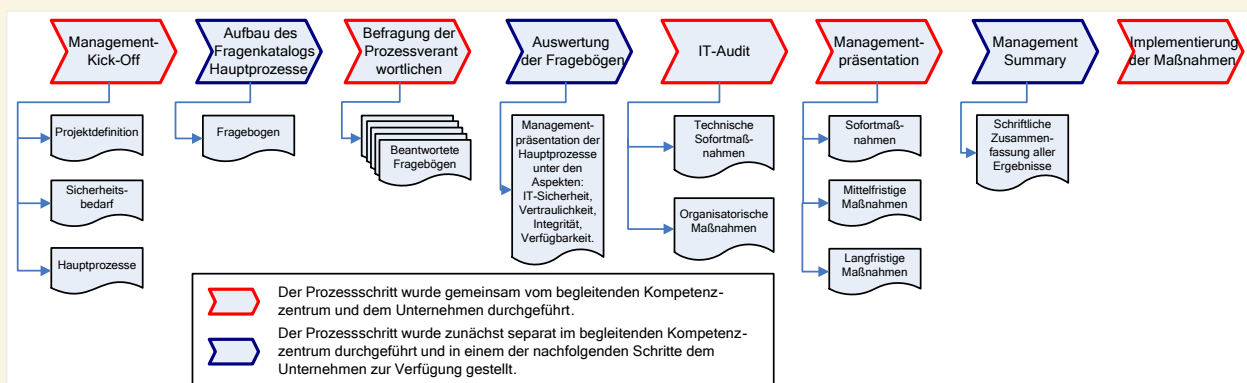
Alle verfügbaren Daten und Informationen der Experten stammen entweder direkt von der jeweiligen Person oder aus dem Handelsregister, von ausgewählten Websites usw. In der Expertenselbstdarstellung besteht für diese die Möglichkeit, sich auf einer eigenen Seite dem Endverbraucher unter Nennung von Ausbildung, Werdegang, Weiterbildung, Fachwissen, Mitgliedschaften, Tätigkeitsschwerpunkten, Referenzen usw. vorzustellen. Eine Verpflichtung zur Veröffentlichung einer Selbstdarstellung

besteht nicht. Endverbrauchern können nach angemeldeten Personen und Unternehmen aus unterschiedlichen Berufsgruppen suchen.

Des Weiteren bietet das Portal für den Endverbraucher den Service eines Vergleichsrechners/Depotmanagers als erste Orientierungshilfe zum Vergleich von Standard-Versicherungsrisiken oder zur individuellen Analyse seines Anlegerprofils. Die komplette Version mit allen Funktionalitäten steht nur registrierten Vermittlern und Beratern zur Verfügung. Im internen Bereich des Portals können bundesweit Ausschreibungen durch die Vermittler an die Fachspezialisten der jeweiligen Unternehmen der Branche weitergeleitet werden. Zusätzlich können die Experten Personen- bzw. Unternehmensinformationen in einem passwortgeschützten Bereich, die für eine Zusammenarbeit erforderlichen Unterlagen (Selbstdarstellung, Werdegang, Führungszeugnis, Handelsregisterauszug, Gewerbeanmeldung usw.) hinterlegen.

Im B2B-Bereich des Portals erhalten nur registrierte Personen und Unternehmen Brancheninformationen, Produktinformationen und Informationen zu gesetzlichen Neuregelungen usw. Darüber hinaus erhalten hier die registrier-

Abbildung 1: Vorgehen der Unternehmensbegleitung



ten Experten die von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) herausgegebenen Meldungen über Weisungen, Erlaubnisse oder Einstellungen von Geschäftsbetrieben.

Neben den allgemein zugänglichen Stellenangeboten und Terminen der Versicherungs-, Investment- und Finanzbranche werden für Vollmitglieder Vertriebsvereinbarungen, Courtageszusagen und Provisionsverträge von Produkt- oder Vertriebsgesellschaften zur Verfügung gestellt, deren Veröffentlichung ausdrücklich gewünscht und freigegeben wurde.

Ein Kompetenzbeirat, bestehend aus Rechtsanwälten, Steuerberatern, Wirtschaftsprüfern, Notaren, Hochschulprofessoren, Wirtschaftsjournalisten, Vorständen von Verbänden und öffentlich oder behördlich bestellten Gutachtern, unterstützt das Unternehmen durch richtungweisende Vorschläge und Anregungen beim weiteren Aufbau und Entwicklung des Portals.

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

- ▶ Über Jahrzehnte gewachsene, eher unübersichtliche IT-Struktur,
- ▶ Zusätzliche Nutzung der IT-Infrastruktur durch verbundene Unternehmen der Versicherungswirtschaft,
- ▶ Immer kürzer werdende Programmier-, Test- und Implementierungszeiträume,
- ▶ Steigende Rate kritischer IT-Risiken durch Online-Zugriffe über unsichere Verbindungen.

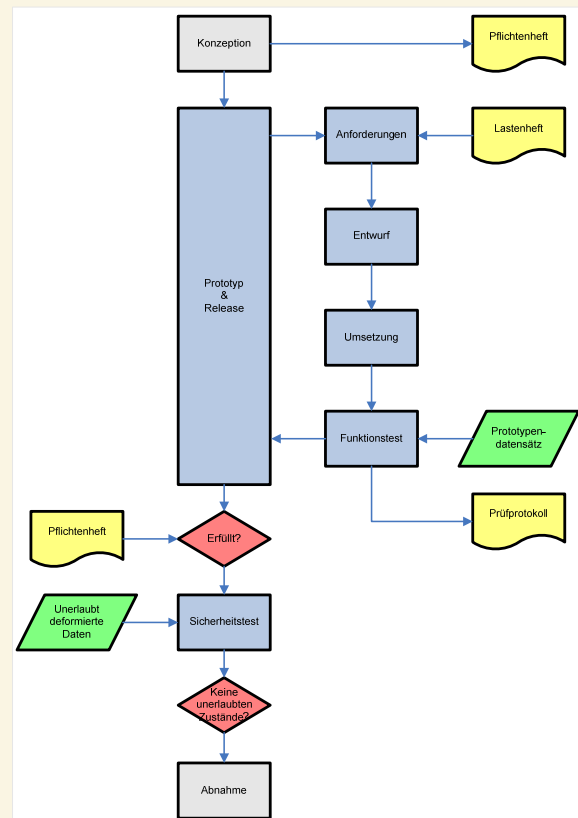
Bei der Unternehmensbegleitung wurden sowohl technische (z. B. Netzwerkstrukturen, Virenschutz) als auch organisatorische Aspekte (z. B. Datenschutz, GDPuD [Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen]) untersucht.

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 der vorhandenen IT-Infrastruktur und den Anwendern dieser Infrastruktur ermittelt und aufbereitet. Im Besonderen wurden Einzelinterviews mit ausgewählten Abteilungsleitern, Führungskräften und Mitarbeitern der IT durchgeführt (siehe Abbildung 1).

Daneben fanden eine begleitete und erläuterte Betriebsbegehung sowie stichprobenartige Arbeitsplatzbesuche statt. Netzwerkstrukturplan, Netz und Server-Landschaft wurden unter technischen Gesichtspunkten beurteilt.

Abbildung 2: Erfassungsbeispiel eines Prozessausschnitts der Softwareentwicklung



Eine abschließende Bewertung der Ergebnisse wurde zusammen mit der Geschäftsleitung vorgenommen und es wurden Handlungsfelder identifiziert und konkretisiert.

Für den vorliegenden Fall wurde der interne und externe Datenfluss analysiert (Fokus: sicherer externer Zugang für Mitarbeiter, sichere Anwendungsprogrammierung).

Darüber hinaus wurden Art und Ort der Vorhaltung von Nutzerkontendaten diskutiert. Unter Berücksichtigung des Bundesdatenschutzgesetzes wurden Maßnahmen vorgeschlagen und es wurde abschließend die Durchführung eines Penetrationstests dringend empfohlen.

4 Prozessauswertung

4.1 Netzwerkstatus

Aktuell wird die IT-Infrastruktur gemeinsam mit anderen Unternehmen aus der Versicherungswirtschaft genutzt.

Empfehlung

- ▶ Die gemeinsame Nutzung mit anderen Unternehmen stellt grundsätzlich ein potenzielles Sicherheitsrisiko dar. Es sollte daher über eine strikte Trennung der Systeme nachgedacht werden.

4.2 Interner und externer Datenfluss

Bei der Überprüfung des internen und externen Datenflusses konnte festgestellt werden, dass der E-Mail-Abruf durch Mitarbeiter über das World Wide Web (WWW) mitunter über unsichere Verbindungen erfolgt. Zudem sind die zugehörigen Ports für Internetdienste wie VoIP über Skype, Chat, ICQ geöffnet.

Datenbestände, auch geschäftskritischen Informationen, werden teilweise unverschlüsselt abgelegt. Kontendaten der Kunden und Experten

werden in einer unverschlüsselten MS-Access-Datenbank aufbewahrt.

Insgesamt muss der Datenfluss als „zu offen“ bezeichnet werden. Dies birgt erhebliche Sicherheitsrisiken, wie z. B. die Gefahr der Verbreitung von Schad-Software über E-Mail oder durch sogenannte „Man-In-The-Middle“-Attacken, bei denen der Datenverkehr eingesehen und manipuliert wird.

Empfehlung

- ▶ Der Mitarbeiterzugang sollte nur über einen getunnelten Verbindungsaufbau per VPN (Virtual Private Network) erfolgen.
- ▶ Die Ports für Internetdienste wie VoIP, Chat und ICQ sollten gesperrt werden, um eventuellen Angriffen über diese Kanäle vorzubeugen.
- ▶ Alle geschäftskritischen und personenbezogenen Daten sollten nur verschlüsselt aufbewahrt werden.
- ▶ Insbesondere die Kontendaten der Kunden und Experten sollten in einer verschlüsselten Datenbank hinterlegt werden.

4.3 Server-Architektur

Die Betriebssystemsituation der Server ist uneinheitlich. Es werden viele MS-Access-Komponenten eingesetzt. Es findet eine gemeinsame Nutzung des Internetzugangs von mehreren Unternehmen statt.

Empfehlung

- ▶ Die Betriebssystemsituation der Server sollte vereinheitlicht werden.
- ▶ Es sollten in regelmäßigen Abständen Penetrationstests durchgeführt werden, um eventuelle Lücken aufzudecken und entsprechende Maßnahmen ergreifen zu können.

4.4 Software-Entwicklungsprozess

Bei der Analyse des Software-Entwicklungsprozesses wurden einige Schwachstellen identifiziert. So erfolgen Software-Tests derzeit ausschließlich mit Live-Daten, d. h. mit tatsächlich genutzten Daten und nicht mit Testdaten. Zudem ist die Testumgebung bereits während der Entwicklung im Internet verfügbar. Weiterhin erfolgen Migrationsprozesse der Datenbank ohne vorhergehende Tests.

Empfehlung

- ▶ Software-Tests sollten nur mit speziellen Testdaten erfolgen.
- ▶ Die Testumgebung sollte während der Entwicklungsphase nicht im Internet verfügbar sein.
- ▶ Die Datenbankmigration sollte ausführlich getestet werden.

4.5 Datenschutz

Die derzeitige gemeinsame Nutzung einer Datenbank für mehrere Unternehmen stellt ein Sicherheitsrisiko in Bezug auf schützenswerte Daten dar. Weitere Kritikpunkte in diesem Bereich sind:

- ▶ Es existiert keine schriftliche Bestellung eines Datenschutzbeauftragten.
- ▶ Ebenso fehlt ein Verzeichnis, in dem die Verfahren der automatisierten Datenverarbeitung dokumentiert werden.
- ▶ Die Nutzer der Plattform werden nicht zur Einwilligung der Verarbeitung ihrer Daten aufgefordert.
- ▶ Es erfolgte keine Vorabkontrolle bzgl. der automatisierten Datenverarbeitung.

Empfehlung

- ▶ Es sollte eine Trennung der Datenbanken nach Unternehmen erfolgen.

- ▶ Nutzer des Portals sollten zu Beginn online zu einer Einwilligungserklärung aufgefordert werden.
- ▶ Eine Datenschutzerklärung sollte grundsätzlich auf der Website einsehbar sein.
- ▶ Ein Schulungs- und Sensibilisierungsplan, den alle Mitarbeiter der Verwaltung regelmäßig durchlaufen müssen, sollte eingerichtet werden.
- ▶ Es empfiehlt sich der Aufbau eines GDPdU- bzw. GoBS-konformen Verzeichnisverfahrens parallel zum datenschutzrechtlichen Verzeichnis.
- ▶ Die Aufnahme eines digitalen Archivsystems in die mittelfristige Investitionsplanung im Rahmen des IT-Budgets und der Aufbau eines reversionssicheren Archivs sollten in Erwägung gezogen werden.

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 werden und in Papierform gesichert abgelegt werden. Diese sollten auch solche Unterlagen umfassen, die eventuell durch Dienstleister bereitgestellt werden müssen.
- ▶ Schulungen der Mitarbeiter (einschließlich Außendienstmitarbeiter) zu Fragen der IT-Sicherheit sollten wiederkehrend durchgeführt werden.
- ▶ Im Hinblick auf den Datenschutz müssen Mitarbeiter regelmäßig geschult werden. Zudem sind unter dem Aspekt der Verarbei-

tung geschäftskritischer und personenbezogener Daten alle Anwender ausreichend für die Gefahren und Risiken der EDV-Nutzung zu sensibilisieren.

- ▶ Unabhängig davon, ob eine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht, ist das gesetzlich vorgeschriebene Verzeichnis nach BDSG und GDPdU sowie GoBS zu erstellen. Mitarbeiter sollten entsprechend geschult und Verschwiegenheitserklärungen unterzeichnet 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.
- ▶ 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, Viren-

schutz, 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:

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

Legend:
 ● Regionales Kompetenzzentrum
 ● Branchen-Kompetenzzentrum
 ● externer Netzwerkpartner

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“)

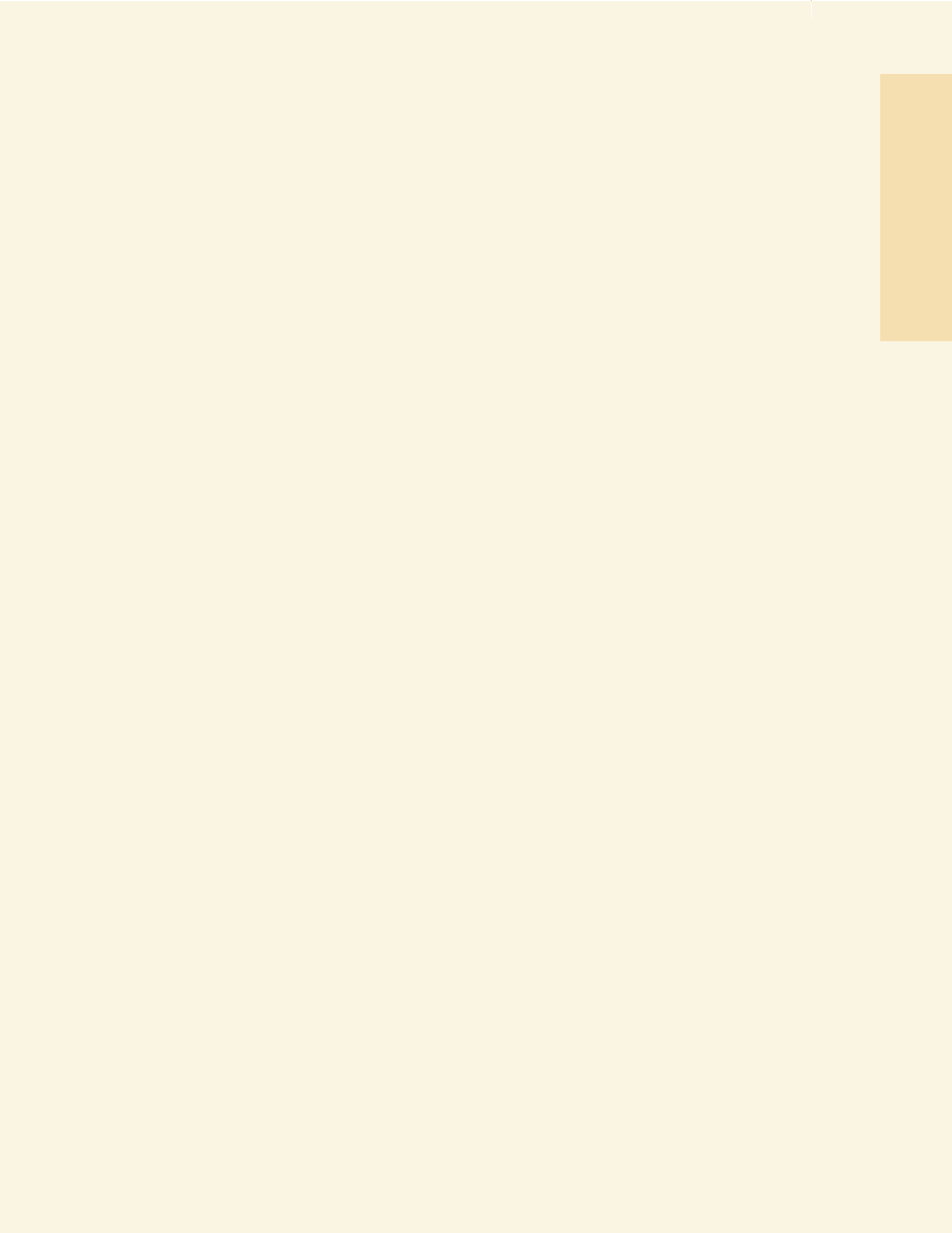
Online-Portal des Netzwerks Elektronischer Geschäftsverkehr; kostenfrei.

<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.