



Gefördert durch das
Bundesministerium
für Wirtschaft
und Technologie



Netzwerk Elektronischer
Geschäftsverkehr



Handlungsanleitung für die Praxis

Sichere Geschäftsprozesse: Umsetzung im Unternehmen – Branchenbeispiel Handwerk 1

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

SAGeG Chemnitz – Kompetenzzentrum Elektronischer Geschäftsverkehr

Stand

Dezember 2007

- 1 Vorwort**
- 2 Ausgangssituation**
- 3 Untersuchungsmodell**
- 4 Datenbestände**
- 5 Computer und Anwendungen**
 - 5.1 Server
 - 5.2 PCs
- 6 Intranet**
- 7 Weitere Komponenten**
 - 7.1 Internet
 - 7.2 Mobile Geräte
 - 7.3 Archiv
- 8 Gebäude und Infrastruktur**
- 9 Organisation und Personal**
- 10 Fazit: Aufgaben für die Unternehmensführung**
 - 10.1 Reaktives Verhalten
 - 10.2 Strategisches Verhalten
- 11 Anhang**
 - 11.1 Das Netzwerk Elektronischer Geschäftsverkehr
 - 11.2 Verbundprojekt „Sichere E-Geschäftsprozesse in KMU und Handwerk“
 - 11.3 Kompetenzzentren vor Ort
- 12 Weiterführende Literatur**
 - 12.1 Die Reihe „Sichere Geschäftsprozesse: Umsetzung im Unternehmen“
 - 12.2 Fachzeitschriften
 - 12.3 Fachbücher
 - 12.4 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 Handwerksbranche besteht seit dem Jahr 1980 mit Firmensitz im sächsischen

Raum. Mit insgesamt 50 Mitarbeitern ist das Unternehmen im stahlverarbeitenden Gewerbe tätig. Auf einer Produktionsfläche von 3.500 m² werden jährlich über 150 Tonnen Edelstahl verarbeitet. Für Serienproduktionen und Einzelanfertigungen nach Kundenwunsch steht ein moderner Maschinenpark zur Verfügung.

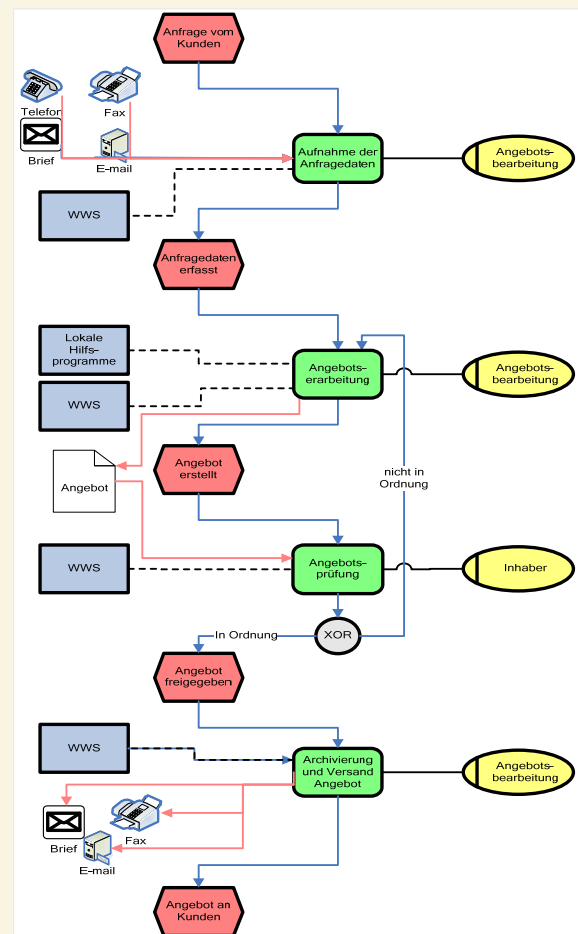
Die **kritischen Gefahrenpotenziale** der bestehenden IT-Infrastruktur sind Folgende, wobei eine Reihe eingeleiteter Maßnahmen deren Risiko bereits zum jetzigen Zeitpunkt minimieren:

- ▶ Geringes Wissen aller Mitarbeiter zu aktuellen Sicherheitsgefahren,
- ▶ Archivierung der Daten erfolgt noch nicht nach den Anforderungen aus Compliance und GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen),
- ▶ Keine Verschlüsselung kritischer Daten,
- ▶ Nur teilweise Auswertung von Protokolldateien,
- ▶ Verwendung von ISDN-Verbindungen,
- ▶ Keine aktenkundige Belehrung über das unternehmensinterne Verbot zur Nutzung von E-Mail und Internet für private Zwecke.

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.

Abbildung 1: Erfassungsbeispiel für den Prozess der Angebotserstellung



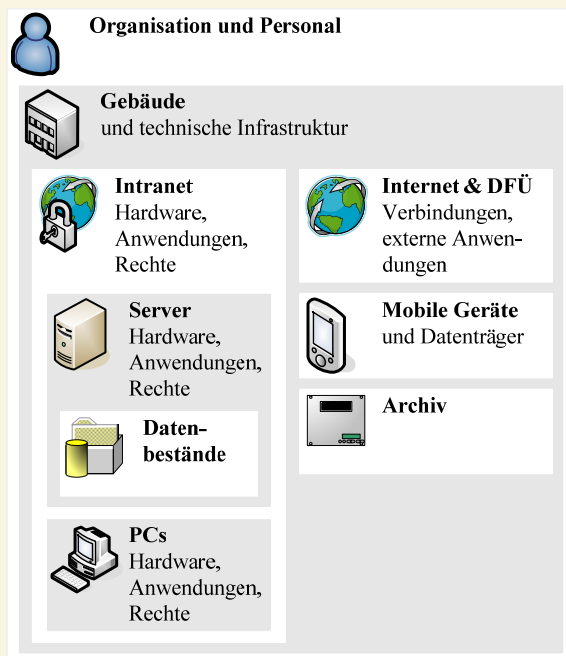
Für den vorliegenden Fall wurden die nachfolgenden Prozesse analysiert:

- ▶ Angebotserstellung,
- ▶ Auftragsprüfung/Fertigungsvorbereitung,
- ▶ Beschaffung,
- ▶ Fertigung,
- ▶ Finanzbuchhaltung,
- ▶ Lohnbuchhaltung,
- ▶ Service,
- ▶ IT-Management.

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.

Die Untersuchungsergebnisse werden in den folgenden Abschnitten detailliert dargestellt. Die verwendete Struktur orientiert sich dabei am in Abbildung 2 dargestellten Grundmodell.

Abbildung 2: Struktur der Ergebnisdarstellung



Als wertvollstes Gut eines Unternehmens werden zu Beginn die gespeicherten Daten (Datenbestände) näher betrachtet.

4 Datenbestände

Im begleiteten Unternehmen wird ein Großteil der geschäftskritischen Daten in der Datenbank des Warenwirtschaftssystems gespeichert. Diese Daten sind besonders schutzwürdig. Weitere Daten, beispielsweise technische Zeichnungen aus CAD-Anwendungen, werden auf einem Fileserver abgelegt. Die Datensicherung erfolgt täglich mittels Speicherung auf einem Bandlaufwerk. Ein Rechtesystem erlaubt nur dem Inhaber den Zugriff auf personenbezogene Daten.

Empfehlung

- ▶ Eine Übersicht der verwendeten Verzeichnisstruktur (Speicherorte der Daten) sollte gemäß der Anforderungen an Compliance und GDPdU erstellt werden.
- ▶ Die Einsatzmöglichkeit von Verschlüsselungsverfahren insbesondere für sensible Datenbestände sollte überdacht werden.
- ▶ Da zu erwarten ist, dass die Geschäftsdaten im Rahmen der E-Mail-Kommunikation an Bedeutung gewinnen, sollte ein ganzheitliches Konzept für eine geregelte E-Mail-Nutzung erstellt und umgesetzt werden. Dieses umfasst insbesondere die Aspekte Speicherung, Backup und Archivierung.

5 Computer und Anwendungen

5.1 Server

Ein Windows Server ist im Einsatz (RAID), so dass die gängigen Sicherheitsvorkehrungen (Zugangskontrolle, Sicherheits-Updates, Virenschutz, Band-Backup) zu beachten sind. Dieser

Server bedient zum einen die üblichen Dienste (Netzwerk, Datei, Print) und zum anderen ist auf ihm das zentrale Warenwirtschaftssystem des Unternehmens, mit seiner Datenbank installiert.

Empfehlung

- ▶ Eine Wiederanlaufdokumentation des Servers (Hardware, Anwendungen, Daten, Einstellungen, Virenschutz) sollte für den Fall vorgehalten werden, dass er ausfallen sollte.
- ▶ Die relevanten log-Dateien (Betriebssystem, Warenwirtschaftssystem, E-Mail) sollten täglich ausgewertet werden.
- ▶ Als Informationsquellen für Sicherheitslöcher in Betriebssystemen und Anwendungen kann z. B. www.heise.de genutzt werden.

5.2 PCs



Da Windows Betriebssysteme zum Einsatz kommen, sind auch hier die gängigen Sicherheitsvorkehrungen (Zugangskontrolle, Passwortgebrauch, Sicherheits-Updates, Virenschutz) zu beachten. Spezifische PCs, die nicht ohne weiteres austauschbar sind, sollten sich bei Ausfall in einem Zeitrahmen ersetzen lassen, der sich nicht kritisch auf den regulären Betriebsablauf auswirkt.

Empfehlung

- ▶ Sensible Daten des Unternehmens sind in das Backup-System einzubeziehen.
- ▶ Für diese Daten sind Dokumentationen zu entwickeln.
- ▶ Da die Verwendung von externen Datenträgern (USB-Sticks, CDs) nicht ausgeschlossen werden kann, sollte der Nutzer über die Gefahren und den notwendigen Virenschutz aktenkundig belehrt werden. Dies gilt gleichermaßen für E-Mail- und Internetnutzung.
- ▶ Die Verwaltung von Sicherheits-Updates (Betriebssystem, Anwendungen) sollte zentral gesteuert werden, um den sicheren Zustand der einzelnen PCs zu garantieren.

6 Intranet



Das Intranet ist verkabelt, wobei WLAN und Bluetooth hier nicht zum Einsatz kommen. Darüber hinaus werden schnell wiederbeschaffbare Hardwarekomponenten eingesetzt.

Empfehlung

- ▶ Eine Dokumentation über Passworte und Regeln der aktiven Elemente (Switch, ISDN-Karten) sollte angelegt werden. Eine Dokumentation der Netzbestandteile (PC, Server, Drucker) mit wesentlichen Netzdaten (z. B. IP-Adressen, Administratorpasswort) sollte sicher hinterlegt werden.
- ▶ Programme zum Scannen und Auswerten des Netzverkehrs sollten in zukünftigen Maßnahmen vorgesehen werden.
- ▶ Virensignaturen sollten zentral verwaltet und automatisch verteilt werden.

7 Weitere Komponenten

7.1 Internet



Vom Intranet aus besteht ein Zugang zu extern liegenden Komponenten mittels einer Internet- und ISDN-Verbindung. Die sicherheitsüblichen Hard- und Softwarekomponenten sind vorhanden und für den Zugang sind eine Firewall und Sicherheitsregeln eingerichtet. Die Werkseinstellungen für Passworte wurden verändert.

Empfehlung

- ▶ Dokumentieren Sie die Infrastruktur der Sicherheitskomponenten (Software mit Versionsnummer, Passwörter).
- ▶ Dokumentieren Sie die eingestellten Regeln (z. B. Firewall).
- ▶ Verwahren Sie die Unterlagen sicher.
- ▶ Überwachen Sie den Datenverkehr zum Internet täglich, um schnell auf unbekannte

Ereignisse reagieren zu können. Nutzen Sie entsprechende Software.

- ▶ Informieren Sie sich über Sicherheits-Updates der genutzten Hard- (Firmware) und Software. Installieren Sie diese zeitnah.
- ▶ Regeln Sie die Aufgabenstellungen zur IT-Sicherheit mit Dienstleistern schriftlich.
- ▶ Die ISDN-Verbindung sollte dokumentiert sein und wenn möglich nur während der Nutzung physisch verbunden werden.
- ▶ Aktualisieren Sie (möglichst automatisch) Ihre Browsersoftware regelmäßig.

7.2 Mobile Geräte



Mobile Datenträger, z. B. Laptops, USB-Speichermedien, werden häufig genutzt.

Empfehlung

- ▶ Laptops, die nach Nutzung im Außendienst wieder an das Firmennetz angeschlossen werden, sollten mit Sicherheits-Updates und Virenschutzkomponenten ausgerüstet werden, bevor die Verbindung zum Firmennetz hergestellt wird.
- ▶ Sensible Daten für das Unternehmen sollten (zukünftig) auf allen mobilen Geräten verschlüsselt abgelegt werden (z. B. Laptops im Außendienst, USB-Sticks).
- ▶ Außendienstmitarbeiter sollten über die Gefahren bei der Nutzung außerhalb der Firma geschult und aktenkundig belehrt werden.
- ▶ Administratoren sollten an regelmäßige Weiterbildungen zu den Themen Verschlüsselung, WLAN und Bluetooth teilnehmen.

7.3 Archiv



Die Archivierung von Daten erfolgt auf DVD. Die Lagerung sollte in Räumen außerhalb des

Firmengebäudes erfolgen, zu denen nur der Inhaber Zugang hat.

Empfehlung

- ▶ Da die Archivierung mittels selbst gebrannter DVDs, bedingt durch chemische Prozesse und bestimmte anderer Bedingungen nur ein Jahr betragen kann, ist eine Archivierung auf einer externen Festplatte notwendig.
- ▶ Im Unternehmen sollten schriftliche Vorschriften für die Archivierung festgelegt werden.
- ▶ Für die Auswahl der zu archivierenden Daten sollen die Anforderungen an Compliance und insbesondere an die GDPdU beachtet werden.
- ▶ Digitale Daten, die der „Digitalen Betriebsprüfung“ (GDPdU) unterliegen, müssen während der gesetzlichen Frist auswertbar bleiben. Dies muss bei einem Versionswechsel der Software beachtet werden.
- ▶ Geschäftsrelevante E-Mails sollten in die Archivierung einbezogen werden. Zukünftig sollte ein Organisationssystem für E-Mails genutzt werden.

8 Gebäude und Infrastruktur



Das Firmengebäude ist unter sicherheitstechnischen Gesichtspunkten in einem guten Zustand. Der Besucherverkehr unterbleibt in den Büroräumen, ist in den Produktions- und Verkaufsräumen jedoch temporär gestattet. Die Computertechnik ist in einem üblicherweise eher unzugänglichen Teil untergebracht.

9 Organisation und Personal



Im Unternehmen sind nach Aussage der Unternehmensleitung pflichtbewusste Mitarbeiter eingestellt. In der überwiegenden Mehrheit werden Programme ausschließlich für die zu erledigenden Aufgaben genutzt.

Empfehlung

Im Unternehmen sollten Schulungen und aktienkundige Belehrungen zu folgenden Themen erfolgen:

- ▶ Belehrung über die Geheimhaltung betrieblicher Daten bei Eintritt in das Unternehmen (auch Praktikanten, Diplomanden),
- ▶ Verbot der privaten Nutzung von E-Mail und Internet allgemein (die deutsche Rechtsprechung lässt aus datenschutzrechtlichen Gründen den Betrieb eines sicheren Datenverkehrs, der bestimmte Monitoring-Funktionen erfordert, nicht zu),
- ▶ Belehrungen zum Virenschutz im Internet und zur Nutzung mobiler Geräte und Datenträger,
- ▶ Für die Zukunft: Schulungen zum Erstellen und Umgang mit verschlüsselten Daten.

10 Fazit: Aufgaben für die Unternehmensführung

10.1 Reaktives Verhalten

Bedingt durch die Unternehmensgröße kennen die Mitarbeiter die richtigen Ansprechpartner bei betriebsbedingten Störungen. Zusätzlich hat die Unternehmensleitung Dienstleister verpflichtet, die bei akuten Störungen der IT-Infrastruktur beauftragt werden können.

10.2 Strategisches Verhalten

Die Unternehmensführung hat die Sicherheit der IT-Ressourcen als wichtiges Element in den Unternehmensprozessen erkannt und fördert diese. Im Unternehmen ist ein Administrator eingesetzt, der auch für die Belange der IT-Sicherheit sorgt.

Empfehlung

- ▶ Für den Schadens- und Notfall sollten die genannten Dokumentationen entwickelt werden und in Papierform gesichert abgelegt werden. Das bezieht sich auch auf Unterlagen, die eventuell durch Dienstleister bereitgestellt werden müssen.
- ▶ Mitarbeiter (einschließlich Außendienstmitarbeiter) sollten zu Fragen der IT-Sicherheit geschult werden.
- ▶ Die private Nutzung der IT-Infrastruktur und des Internet sollte schriftlich geregelt werden.
- ▶ Durch den Administrator sollten folgende Aufgaben kontinuierlich erfüllt 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 sind bereitzustellen.
- ▶ Die bereits erfüllten, zuzüglich der hier benannten Empfehlungen stellen wesentliche Bausteine auf dem Weg der IT-Zertifizierung (Selbstzertifizierung) dar.

- ▶ 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.

11 Anhang

11.1 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.



11.2 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

11.3 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

12 Weiterführende Literatur

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

12.1 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

12.2 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.

12.3 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.
- Schneider, Bruce: Secrets and Lies, IT-Sicherheit in einer vernetzten Welt, 2004.
- Witt, Bernhard Carsten: IT-Sicherheit kompakt und verständlich. Eine praxisorientierte Einführung, 2006.

12.4 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



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