



Gefördert durch das  
Bundesministerium  
für Wirtschaft  
und Technologie



Netzwerk Elektronischer  
Geschäftsverkehr



Handlungsanleitung für die Praxis

## Sichere Geschäftsprozesse: Umsetzung im Unternehmen – Branchenbeispiel Handwerk 2

[www.ec-net.de](http://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](http://www.photocase.de)

### **Herausgeber**

SAGeG Chemnitz – Kompetenzzentrum Elektronischer Geschäftsverkehr

### **Stand**

Februar 2008

- 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 zusätzlich die dortigen speziellen Rahmenbedingungen berücksichtigt werden.

## 2 Ausgangssituation



Der 1914 gegründete Familienbetrieb realisiert mit 11 Mitarbeitern das gesamte Spektrum vom Treppenbau aus

Holz, Glas und Edelstahl über die Fertigung von Geländeranlagen im Innen- und Außenbereich, bis zur Sanierung und Restauration von Treppen und Geländern. Alle Produkte werden in dem in Ostsachsen ansässigen Handwerksunternehmen ausschließlich von Fachkräften in handwerklicher Arbeit hergestellt. Dies ermöglicht größte gestalterische Freiräume bei der Planung und garantiert ein Höchstmaß an Qualität.

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

- ▶ Keine Dokumentationen über Passwörter und Regeln der aktiven Elemente (Switches, ISDN-Karten) sowie der Netzwerkbestandteile (PC, Server, Drucker) mit wesentlichen Netzdaten (IP, Administratorpasswort).
- ▶ Keine Programme zum Scannen und Auswerten des Netzwerkverkehrs.
- ▶ Keine zentrale Verwaltung und Aktualisierung von Virensignaturen.
- ▶ Keine ausreichende Dokumentation über die Infrastruktur der Sicherheitskomponenten (Software mit Versionsnummern, Passwörter).

- ▶ Keine Überwachung des Datenverkehrs des Internets.
- ▶ Keine Dokumentation von Informationen über Sicherheits-Updates der genutzten Hard- (Firmware) und Software.
- ▶ Keine durchgängige Verschlüsselung kritischer Daten.
- ▶ Gefährdung der Systembetreuung bei Ausfall des Administrators.
- ▶ Die Archivierung der Daten entspricht noch nicht den Anforderungen aus Compliance und GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen).

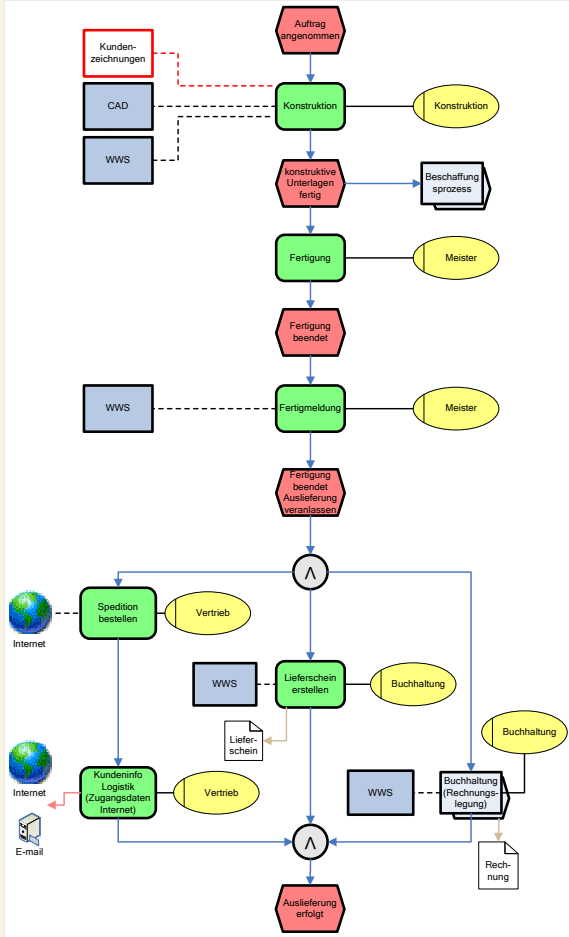
## 3 Untersuchungsmodell

Im Rahmen der Projektaktivitäten wurden die Geschäftsprozesse im Unternehmen analysiert, die im besonderen Maße durch die Informationstechnik geprägt sind. Dazu wurden Befragungen von Mitarbeitern des Unternehmens durchgeführt.

Zusammenfassend bleibt festzuhalten, dass Geschäftsführung und IT-Verantwortliche Fragen der IT-Sicherheit als wichtiges Firmengut betrachten und Maßnahmen zur Verbesserung der IT-Sicherheit kontinuierlich verfolgen. Folgende Prozesse wurden untersucht:

- ▶ Angebotserstellung/Auftragsprüfung,
- ▶ Beschaffung,
- ▶ Fertigung/Auslieferung,
- ▶ Finanzbuchhaltung,
- ▶ IT-Management.

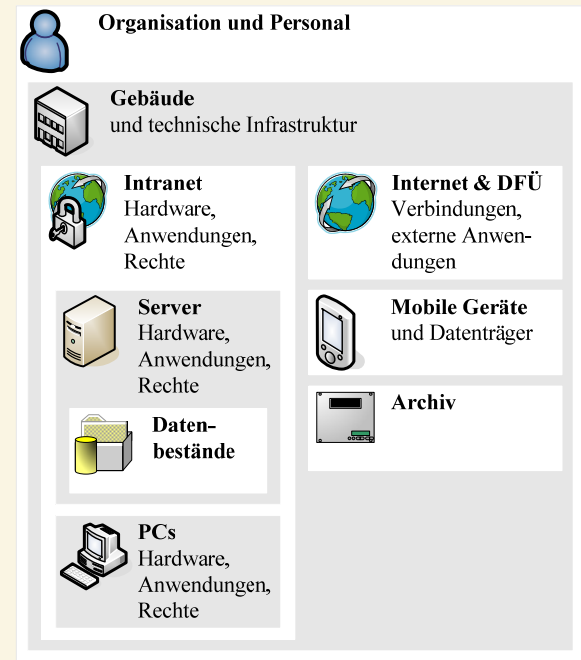
**Abbildung 1: Erfassungsbeispiel für den Prozess der Fertigung und Auslieferung**



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.

In der durchgeführten Analyse wurde die tatsächliche Wirksamkeit der bereits eingesetzten Schutzsysteme, eingestellten Schutzregeln usw. nicht überprüft und dementsprechend nicht ausgewertet. Als eine generelle Maßnahme wird die Überprüfung der Wirksamkeit der Schutzmaßnahmen durch unabhängige Dienstleister empfohlen.

**Abbildung 2: Struktur der Ergebnisdarstellung**



Die Untersuchungsergebnisse werden in den folgenden Abschnitten detailliert dargestellt. Die verwendete Struktur orientiert sich dabei am in Abbildung 2 dargestellten Grundmodell. Als wertvollstes Gut eines Unternehmens werden zu Beginn die 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 (z. B. CAD-Zeichnungen) werden auf einem Fileserver abgelegt. Personendaten werden auf dem PC des Firmeninhabers gespeichert und sind auch nur von diesem einsehbar. Die Daten werden täglich gespiegelt und durch ein Band-Backup gesichert. Daten Dritter fallen in geringem Umfang als CAD-Dateien an. In E-Mails fallen gelegentlich Geschäftsdaten an. Für die Finanzbuchhaltung steht ein spezielles Programm zur Verfügung.

### Empfehlung

- ▶ Es sollte eine Übersicht der verwendeten Verzeichnisstruktur (Speicherorte der Daten) gemäß den Anforderungen an Compliance und GDPdU erstellt werden.
- ▶ Verschlüsselungsverfahren sollten insbesondere für sensible Datenbestände auf Einsatzmöglichkeiten überprüft werden.
- ▶ Ein ganzheitliches Konzept für eine geregelte E-Mail-Nutzung sollte erstellt und umgesetzt werden, da zu erwarten ist, dass die Geschäftsdatenübermittlung im Rahmen der E-Mail-Kommunikation an Bedeutung gewinnen wird. Das Konzept umfasst insbesondere die Speicherung, Backup und Archivierung.

## 5 Computer und Anwendungen

### 5.1 Server



Ein Windows Server ist im Einsatz (RAID 5-System). Dabei werden die gängigen Sicherheitsvorkehrungen (Zugangskontrolle, Sicherheits-Updates, Virenschutz, Band-Backup) beachtet. Dieser Server bedient die üblichen Dienste (Netzwerk, Datei, Druck). Darüber hinaus ist auf ihm das zentrale Warenwirtschaftssystem des Unternehmens mit der zugehörigen Datenbank installiert.

### Empfehlung

- ▶ Eine Wiederanlauf-Dokumentation des Servers (Hardware, Anwendungen, Daten, Einstellungen, Virenschutz) sollte für den Fall eines Server-Ausfalls vorgehalten werden.
- ▶ Eine tägliche Auswertung der relevanten log-Dateien (Betriebssystem, Warenwirtschaftssystem, E-Mail) sollte erfolgen.
- ▶ Als Informationsquelle für Sicherheitslöcher in Betriebssystem und Anwendungen kön-

nen gängige Internetportale zum Thema Sicherheit verwendet werden.



### 5.2 PCs

Es sind Windows Betriebssysteme im Einsatz. Die üblichen Sicherheitsvorkehrungen (Zugangskontrolle, Passwortgebrauch, Sicherheits-Updates, Virenschutz) werden beachtet. Die eingesetzten PCs sind im Notfall ersetzbar. Auch spezifische PCs sind bei einem Ausfall kurzfristig ersetzbar, so dass der Betriebsablauf nicht gefährdet wird.

### Empfehlung

- ▶ Sensible Daten des Unternehmens sollten in das vorhandene Backup-System einbezogen werden.
- ▶ Für diese Daten sollten Dokumentationen entwickeln werden.
- ▶ 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 sollte gleichermaßen für E-Mail- und Internetnutzung gelten.
- ▶ Um den sicheren Zustand der einzelnen PCs zu garantieren, sollte die Verwaltung von Sicherheits-Updates (Betriebssystem, Anwendungen) zentral gesteuert werden.

## 6 Intranet



Das Intranet ist durch ein verkabeltes Netzwerk realisiert. WLAN- und Bluetooth-Geräte kommen nicht zum Einsatz. Es werden Hardware-Komponenten eingesetzt, die im Notfall schnell wiederbeschafft werden können.

### Empfehlung

- ▶ Über Passwörter und Regeln der aktiven Elemente (Switch, ISDN-Karten) sollte eine Dokumentation angelegt werden. Eine

Dokumentation der Netzwerkbestandteile (PC, Server, Drucker) mit wesentlichen Netzdaten (z. B. IP-Adressen, Administratorpasswort) sollte ebenfalls sicher hinterlegt werden.

- ▶ Künftig sollten zur Kontrolle Programme zum Scannen und Auswerten des Netzwerkverkehrs eingesetzt 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 über eine Internet-Verbindung. Die sicherheitsüblichen Hard- und Software-Komponenten sind vorhanden. Eine Firewall ist vorhanden, Sicherheitsregeln sind eingerichtet. Die Werkseinstellungen für Passwörter wurden verändert.

#### Empfehlung

- ▶ Die Infrastruktur der Sicherheitskomponenten (Software mit Versionsnummer, Passwörter) sollte dokumentiert werden.
- ▶ Eingestellte Regeln (z. B. Firewall) sollten ebenfalls dokumentiert werden.
- ▶ Die erstellten Unterlagen sollten sicher verwahrt werden.
- ▶ Eine tägliche Überwachung des Datenverkehrs zum Internet sollte erfolgen, um schnell auf unbekannte Ereignisse reagieren zu können. Zu diesem Zweck sollte eine entsprechende Überwachungs-Software eingesetzt werden.
- ▶ Informationen über Sicherheits-Updates der genutzten Hard- (Firmware) und Software sollten regelmäßig eingeholt werden. Eine Installation sollte zeitnah erfolgen.

- ▶ Die Aufgabenstellungen zur IT-Sicherheit sollten mit externen Dienstleister schriftlich vereinbart werden.
- ▶ Die Browsersoftware sollte regelmäßig, möglichst automatisch, aktualisiert werden.

### 7.2 Mobile Geräte



Laptops werden genutzt, die Verwendung mobiler Datenträger, wie z. B. USB-Speichermedien, ist möglich.

#### Empfehlung

- ▶ Bevor die Verbindung zum Firmennetz hergestellt wird, sollten Laptops nach der Nutzung im Außendienst zuerst an einen vom Firmennetz getrennten PC angeschlossen und mit Sicherheits-Updates und Virenschutzkomponenten ausgestattet werden.
- ▶ Sensible Daten für das Unternehmen sollten zukünftig auf allen mobilen Geräten verschlüsselt abgelegt werden (z. B. Laptops, USB-Speichermedien).
- ▶ Über die Gefahren bei der Nutzung mobiler Geräte außerhalb der Firma sollten Außendienstmitarbeiter geschult und aktenkundig belehrt werden.
- ▶ Administratoren sollten regelmäßig an Weiterbildungen zu den Themen Verschlüsselung, WLAN und Bluetooth teilnehmen.

### 7.3 Archiv



Die Archivierung von Daten erfolgt auf DVDs. Die Lagerung erfolgt außerhalb des Firmengebäudes, wobei nur der Inhaber Zugang zu den Archivmedien hat.

#### Empfehlung

- ▶ Da die Archivierung mittels selbst gebrannter DVDs, bedingt durch chemische Prozesse und weitere Bedingungen, in einigen Fällen nur ein Jahr betragen kann, erscheint

eine Archivierung auf einer externen Festplatte empfehlenswert. DVDs sollten zyklisch erneuert werden.

- ▶ Vorschriften für die Archivierung sollten schriftlich im Unternehmen festgelegt werden.
- ▶ Für die Auswahl der zu archivierenden Daten sollten die Anforderungen an Compliance und insbesondere an die GDPdU beachtet werden.
- ▶ Digitale Daten, die der „Digitalen Betriebsprüfung“ (GDPdU) unterliegen, müssen über die gesetzliche Frist auswertbar bleiben. Dies sollte bei einem Versionswechsel der Software beachtet werden.

- ▶ Belehrung über die Geheimhaltung betrieblicher Daten bereits bei Eintritt in das Unternehmen (insbesondere Praktikanten).
- ▶ Verbot der privaten Nutzung von E-Mail und Internet (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.
- ▶ Zukünftig sollten Schulungen zu Erstellung und Umgang mit verschlüsselten Daten durchgeführt werden.

## 8 Gebäude und Infrastruktur



Das Firmengebäude ist unter sicherheitstechnischen Gesichtspunkten in einem guten Zustand. Die Lage schließt jedoch die Gefahr von Vandalismus nicht aus. In den Büroräumen findet Besucherverkehr statt. In den Produktions- und Verkaufsräumen kann zeitweise Fremdpersonal anwesend sein. Die Computertechnik ist in einem üblicherweise unzugänglichen Teil untergebracht.

## 9 Organisation und Personal



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

### Empfehlung

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

## 10 Fazit: Aufgaben für die Unternehmensführung

### 10.1 Reaktives Verhalten

Durch die Unternehmensgröße bedingt, kennen die Mitarbeiter die richtigen Ansprechpartner bei betriebsbedingten Störungen.

### 10.2 Strategisches Verhalten

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

### Empfehlung

- ▶ Kritisch ist der mögliche Ausfall des Administrators. Es sollte ein Dienstleister für Notfallsituationen eingebunden werden.

- ▶ Für den Schadens- und Notfall sollten die aufgeführten Dokumentationen entwickelt werden und in Papierform gesichert abgelegt werden. Diese sollten auch Unterlagen umfassen, die eventuell durch Dienstleister bereitgestellt werden müssen.
- ▶ Regelmäßige Schulungen der Mitarbeiter (einschließlich Außendienstmitarbeiter) zu Fragen der IT-Sicherheit sollten eingeführt werden.
- ▶ Eine schriftliche Regelung der privaten Nutzung der IT-Infrastruktur und des Internets sollte insbesondere für nicht zur Unternehmerfamilie gehörende Mitarbeiter getroffen 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 sowie Durchführung der Backup- und Archivierungsprozesse. Die zeitlichen Ressourcen sind entsprechend bereitzustellen.
- ▶ Die bereits erfüllten und die hier benannten Empfehlungen sollten als wesentliche Bausteine auf dem Weg der IT-Zertifizierung (Selbstzertifizierung) verstanden werden.
- ▶ Bei der Analyse der IT-relevanten Prozesse im Unternehmen wurde kein Belastungstest an der vorhandenen IT-Infrastruktur vorgenommen. Eine Einschätzung der Wirksamkeit der installierten Sicherheitsmaßnahmen (Firewall, Virenschutz, Zugangsschutz, Verschlüsselung usw.) kann aus diesem Grund nicht vorgenommen werden. Die Wirksamkeit der Schutzmaßnahmen sollte durch einen unabhängigen Dienstleister in regelmäßigen Abständen überprüft werden.

## 11 Anhang

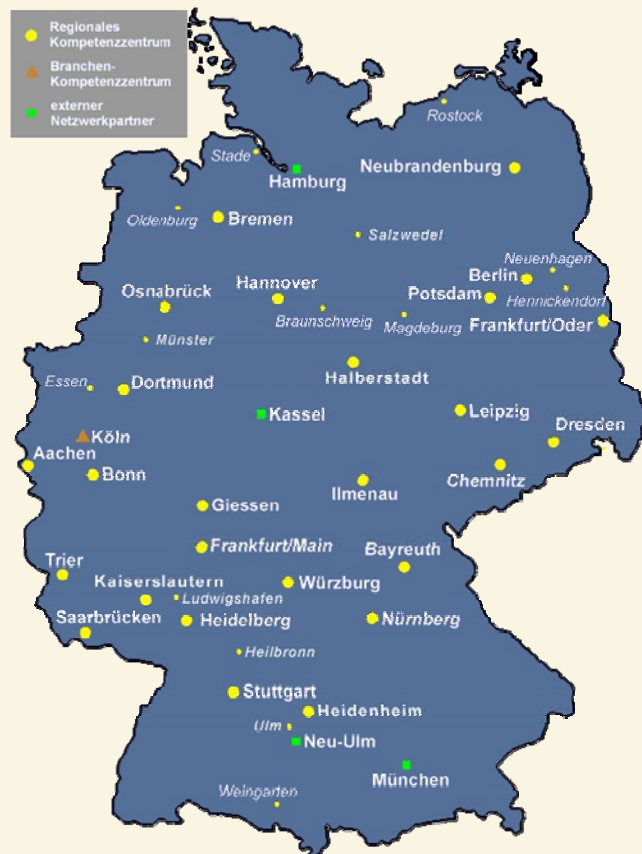
### 11.1 Das Netzwerk Elektronischer Geschäftsverkehr

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](http://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](http://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](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](mailto: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](mailto: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](mailto: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](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.