



Gefördert durch das
Bundesministerium
für Wirtschaft
und Technologie



Netzwerk Elektronischer
Geschäftsverkehr



Handlungsanleitung für die Praxis

Sichere Geschäftsprozesse: Umsetzung im Unternehmen – Branchenbeispiel Maschinenbau 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

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. Lieferantketten 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 in Sachsen ansässige Maschinenbauunternehmen wurde 1991 als Planungs- und Ingenieurbüro gegründet.

Ein klares Firmenkonzept, umfangreiches Wissen aus langjähriger Forschungs- und Entwicklungstätigkeit im Werkzeugmaschinenbau und Enthusiasmus waren die entscheidenden Voraussetzungen für den Weg in eine erfolgreiche Zukunft. Heute ist das Unternehmen mit ca. 140 Mitarbeitern vor allem im innovativen Maschinenbau tätig und bietet neben umfangreichen Ingenieurdienstleistungen, Maschinen und Anlagen als kundenspezifische Einzellösungen oder aus bewährter Serienproduktion an. Ein flexibles ERP-System garantiert Transparenz im Projektmanagement und Fertigungsqualität auf hohem Niveau.

Die **kritischen Gefahrenpotenziale** der bestehenden IT-Infrastruktur sind folgende, wobei eine Reihe eingeleiteter Maßnahmen deren Potenzial bereits jetzt minimieren:

- ▶ Geringes Wissen aller Mitarbeiter über aktuelle Sicherheitsgefahren,
- ▶ Keine Archivierung der Daten nach den Anforderungen aus Compliance und GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen),
- ▶ Keine Verschlüsselung kritischer Daten,
- ▶ Gefahren bei der Nutzung mobiler Geräte im Einsatz und bei Wiedereingliederung in das interne Netzwerk,
- ▶ Nur Teilauswertung von Protokolldateien,

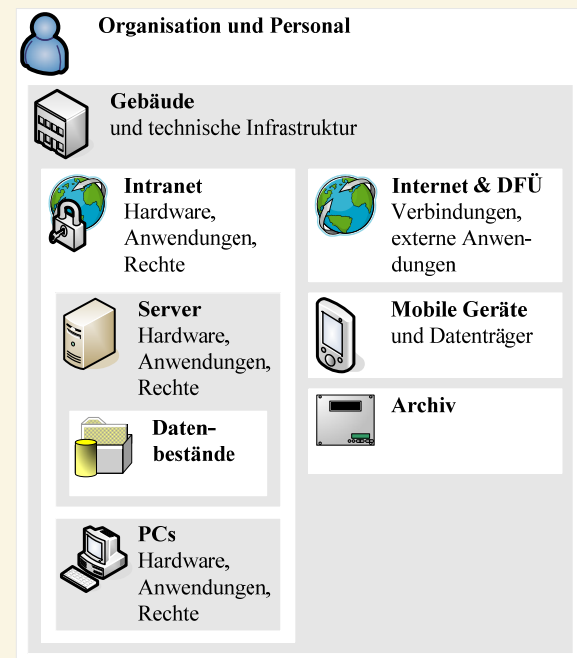
- ▶ Verwendung von ISDN-Verbindungen,
- ▶ Keine aktenkundige Belehrung über unternehmensinterne Verbote zur Nutzung von E-Mail und Internet für private Zwecke.

3 Untersuchungsmodell

Im Rahmen der Projektaktivitäten wurden die Geschäftsprozesse im Unternehmen analysiert, die im besonderen Maße durch die Informationstechnik geprägt sind.

Die Untersuchungsergebnisse werden in den folgenden Abschnitten detailliert dargestellt. Die verwendete Struktur orientiert sich dabei am in Abbildung 1 dargestellten Grundmodell.

Abbildung 1: Struktur der Ergebnisdarstellung



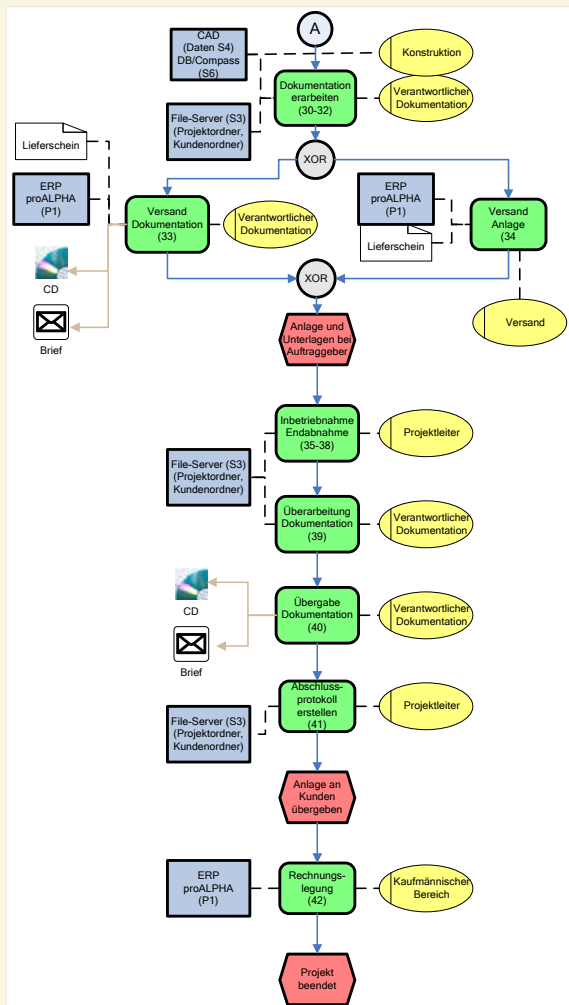
Gemeinsam mit den Mitarbeitern des Unternehmens wurden die Zusammenhänge zwischen den Prozessschritten in der vorhandenen IT-

Infrastruktur und den Anwendern dieser Infrastruktur ermittelt und aufbereitet. Für den vorliegenden Fall wurden die nachfolgenden Prozesse analysiert:

- ▶ Angebotserstellung/Auftragsprüfung,
- ▶ Projektablauf,
- ▶ 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.

Abbildung 2: Erfassungsbeispiel für den Prozess eines Projektablaufs



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

4 Datenbestände



Geschäftskritische Daten werden zum überwiegenden Teil in der Datenbank des ERP-Systems und auf Fileservern gespeichert. Die Zuordnung der Daten zu verschiedenen Servern erlaubt im Notfall eine schnelle Wiederherstellung. Die Daten werden täglich durch ein Band-Backup gesichert. Der Zugriff auf diese Datenbestände ist über Passwort und Gruppenrichtlinien gesichert. Es werden Daten Dritter (CAD-Zeichnungen) verarbeitet. Der Zugriff auf Personen-daten wurde in diesem Fall nicht untersucht. Per E-Mail fallen bislang lediglich wenige Geschäftsdaten an.

Empfehlung

- ▶ Es sollte eine Übersicht über die Speicherorte aller Daten geschaffen werden, die den Anforderungen an Compliance und GDPdU entsprechen müssen.
- ▶ Für die Zukunft sollte über Verschlüsselungsverfahren nachgedacht werden (sensible Datenbestände, Kommunikation mit Servicemitarbeitern).
- ▶ Es ist zu erwarten, dass die Geschäftsdatenübermittlung per E-Mail an Bedeutung gewinnt. Ein Konzept für die Nutzung von E-Mail (Speicherung, Backup, Archivierung) sollte vorbereitet werden.

5 Computer und Anwendungen

5.1 Server



Es sind sechs Windows Server im Einsatz. Die üblichen Sicherheitsvorkehrungen (Zugangskon-

trolle, Sicherheits-Updates, Virenschutz, Backup) werden beachtet.

Auf diesen Servern werden die üblichen Dienste (Netzwerk, Datei, Druck) bedient. Datenbanken und zentrale Anwendungs-Software sind installiert. Die Server sind mit RAID-Systemen ausgerüstet. Die Wiederbeschaffbarkeit der Server-Komponenten ist gesichert.

Empfehlung

- ▶ Eine Dokumentation der Server (Hardware, Anwendungen, Daten, Einstellungen, Virenschutz) wird für den Fall eines Server-Ausfalls empfohlen.
- ▶ Eine tägliche Auswertung der log-Dateien (Betriebssystem, ERP, E-Mail) wird empfohlen.
- ▶ Als Informationsquelle für Sicherheitslöcher in Betriebssystem und Anwendungen können 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 PCs sind in der Regel austauschbar, so dass bei Ausfall Ersatz vorhanden ist. Spezifische PCs sind bei Ausfall in einem Zeitrahmen ersetzbar, der keine für den Betriebsablauf gefährlichen Zustände erwarten lässt.

Auf den PCs werden keine Daten gespeichert, die für den Betriebsablauf kritisch sind.

Empfehlung

- ▶ Da die Verwendung von externen Datenträgern (USB-Sticks, CDs) betriebsbedingt nicht ausgeschlossen werden kann, sollten die 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. Aufgrund der Unternehmensgröße werden mehrere aktive Komponenten (Switches) zur Verteilung der Datenströme verwendet. In der Fertigungshalle werden WLAN-Komponenten eingesetzt.

Zur Wiederbeschaffung der Hardware-Komponenten bestehen geschäftliche Beziehungen.

Empfehlung

- ▶ Eine Dokumentation über Passwörter und Regeln der aktiven Elemente (Switches, ISDN-Karten) sollte angelegt sein.
- ▶ Programme zum Scannen des internen Netzverkehrs sollten als zukünftige Maßnahme vorgesehen werden.
- ▶ Auf sicheren WLAN-Betrieb, insbesondere bei Veränderung der Komponenten, sollte geachtet werden.

7 Weitere Komponenten

7.1 Internet



Das Unternehmen hat Zugang vom Intranet zu außen liegenden Komponenten über Internet und ISDN-Verbindungen.

Die sicherheitsüblichen Hardware- und Softwarekomponenten sind vorhanden.

Für den Zugang ist ein von den Datenservern unabhängiger Gateway-Server einschließlich Firewall vorhanden. Sicherheitsregeln wurden eingerichtet und die Werkseinstellungen für Passwörter wurden verändert.

Empfehlung

- ▶ Es sollte eine Dokumentation der Infrastruktur der Sicherheitskomponenten (Software mit Versionsnummern, Passwörter) vorgenommen werden.
- ▶ Zusätzlich sollten die eingestellten Regeln der Firewall dokumentiert werden.
- ▶ Diese Unterlagen sollten sicher verwahrt werden.
- ▶ Es sollte eine tägliche Überwachung des Datenverkehrs zum Internet stattfinden, um schnell auf unbekannte Ereignisse reagieren zu können. Die entsprechende Software könnte bei der Auswertung behilflich sein.
- ▶ Es sollte sich über Sicherheits-Updates der genutzten Hard- (Firmware) und Softwarekomponenten informiert werden. Eine zeitnahe Installation der Aktualisierungen wird dabei empfohlen.
- ▶ Fragen zur IT-Sicherheit sollten mit einem Dienstleister schriftlich geklärt und festgehalten werden.

7.2 Mobile Geräte



Laptops werden u. a. durch Servicemitarbeiter verwendet. Mobile Datenträger (USB-Speichermedien, CDs, Disketten) werden genutzt und können ohne Beschränkungen an den PCs verwendet werden.

Empfehlung

- ▶ Laptops, die nach Nutzung im Außendienst wieder an das Firmennetz angeschlossen werden, sollten über einen vom Firmennetz getrennten PC mit Sicherheits-Updates und Virenschutzkomponenten ausgerüstet werden, bevor eine Verbindung zum Firmennetz hergestellt wird.
- ▶ Unternehmenssensible Daten sollten auf allen mobilen Geräten verschlüsselt abgelegt

werden (Laptops der Servicemitarbeiter, USB-Speichersticks).

- ▶ Servicemitarbeiter sollten über die Gefahren bei der Nutzung mobiler Datenträger außerhalb der Firma geschult und aktenkundig belehrt werden.
- ▶ Für den Administrator wird eine ständige Weiterbildung zu den Themen Verschlüsselung, WLAN und Bluetooth empfohlen.
- ▶ Die Verwendung von PDAs in Verbindung mit Bluetooth stellt eine neuartige Sicherheitslücke dar. Die Nutzer sollten hierzu im Vorfeld geschult werden.

7.3 Archiv



Die Archivierung von Daten erfolgt auf Magnetbändern, welche in einem Datenschränk des Unternehmens in einem anderen Gebäude gelagert werden. Zugang haben nur ausgewählte Mitarbeiter.

Empfehlung

- ▶ Im Unternehmen sollten schriftliche Vorschriften für die Archivierung festgelegt werden.
- ▶ Für die Auswahl der zu archivierenden Daten sollten die Anforderungen an Compliance und insbesondere GDPdU beachtet werden.
- ▶ Bei Versionswechseln von Anwendungen und der notwendigen Migration der Daten sollten auch die archivierten Daten miteinbezogen werden, damit eine reibungslose Wiederherstellung und Integration gewährleistet ist.

8 Gebäude und Infrastruktur



Das Firmengebäude ist in einem sicherheitstechnisch guten Zustand. Die Lage in einem

Gewerbegebiet schließt allerdings Vandalismus nicht aus. Besucherverkehr in den Büroräumen findet nicht statt. In der Fertigungshalle kann zeitweise Fremdpersonal anwesend sein.

9 Organisation und Personal



Im Unternehmen sind nach Aussage der Unternehmensleitung pflichtbewusste Mitarbeiter eingestellt. Die Anwesenheit von Studenten und Praktikanten ist üblich.

Empfehlung

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

- ▶ Belehrung beim Eintritt in das Unternehmen (auch Praktikanten, Diplomanten) über die Geheimhaltung betrieblicher Daten.
- ▶ Verbot der privaten Nutzung von E-Mail und Internet im Allgemeinen (Die deutsche Rechtsprechung lässt aus datenschutzrechtlichen Gründen den Betrieb eines sicheren Datenverkehrs nicht zu, der bestimmte Monitoring-Funktionen erfordert).
- ▶ Belehrung zum Virenschutz etc. bei der Nutzung des Internets (einschließlich E-Mail) und bei der Nutzung mobiler Geräte und Datenträger.
- ▶ Belehrung zum Umgang mit Daten Dritter (CAD, Programme, Betriebsmitteldaten von Kunden, Messprotokolle usw.) und zum Umgang mit Daten und Programmen entsprechend der Copyright-Richtlinien.
- ▶ Schulungen zu Erstellung und Umgang mit verschlüsselten Daten.

10 Fazit: Aufgaben für die Unternehmensführung

10.1 Reaktives Verhalten

Das Unternehmen beschäftigt einen IT-Administrator und eine Vertretung. Durch die Unternehmensgröße bedingt kennen die Mitarbeiter die notwendigen Ansprechpartner bei betriebsbedingten Störungen. Bei akuten Störungen sind Ressourcen vorhanden, um diese schnellstmöglich zu beheben.

10.2 Strategisches Verhalten

Die Unternehmensführung hat die Sicherheit der IT-Ressourcen als wichtiges Element in den Unternehmensprozessen erkannt und fördert diese. Zudem hat die Unternehmensführung die Verbesserung der IT-Sicherheit als wichtige Aufgabe definiert. Dabei stellen die bereits erfüllten, zuzüglich der im Folgenden benannten Empfehlungen, wesentliche Bausteine auf dem Weg der IT-Zertifizierung (Selbstzertifizierung) dar. Bei der Analyse der IT-relevanten Prozesse im Unternehmen wurden keine Belastungstests an der vorhandenen IT-Infrastruktur vorgenommen. Aus diesem Grund konnte keine Einschätzung der tatsächlichen Wirksamkeit der installierten Sicherheitsmaßnahmen (Firewall, Virenschutz, Zugangschutz, Verschlüsselung usw.) vorgenommen werden.

Im Unternehmen werden ein Administrator und ein Stellvertreter beschäftigt, die auch für die Belange der IT-Sicherheit sorgen. In dieser Unternehmensbegleitung wurden die Prozesse, in denen betriebswirtschaftliche Daten verarbeitet werden, nicht berücksichtigt. Deshalb wird keine Aussage zum Stand der GDPdU-Umsetzung vorgenommen.

Empfehlung

- ▶ Als generelle Maßnahme wird die regelmäßige Überprüfung der Wirksamkeit der bereits im Unternehmen bestehenden Schutzmaßnahmen, Schutzregeln usw. durch unabhängige Dienstleister empfohlen.
- ▶ Für den Schadens- und Notfall sollten die genannten Dokumentationen entwickelt und in Papierform gesichert abgelegt werden. Das bezieht sich auch auf Unterlagen, die eventuell durch Dienstleister bereitgestellt werden müssen.
- ▶ Mitarbeiter (einschließlich Servicemitarbeiter) sollten regelmäßig zu Fragen der IT-Sicherheit geschult werden.
- ▶ Die private Nutzung der IT-Infrastruktur und des Internets sollte schriftlich geregelt werden. Es wird empfohlen, diese mit Verbotscharakter zu formulieren.
- ▶ Durch den Administrator sollten folgende ständigen Aufgaben erfüllt werden: Nutzerverwaltung, Netzüberwachung, Sicherheit der IT-Infrastruktur (Updates, Sicherheits-Patches pflegen), 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 dafür bereitgestellt werden.
- ▶ Es wird empfohlen, die Wirksamkeit der Schutzmaßnahmen durch einen unabhängigen Dienstleister in regelmäßigen Abständen überprüfen zu lassen.
- ▶ Die aus Compliance und GDPdU resultierenden Anforderungen an die sichere Speicherung von Daten sollten künftig besonders beachtet 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 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:

The image shows a map of Germany with various cities marked. Red circles highlight specific locations: Köln, Chemnitz, Würzburg, and Heidenheim. Red lines connect these locations to the names of team members listed around the map. The map also includes a legend for regional and branch competence centers, and logos for ECC, SAGeG, KECoS, and m/e/c/k.

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

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.
- Schneier, 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.