



Gefördert durch das
Bundesministerium
für Wirtschaft
und Technologie



Netzwerk Elektronischer
Geschäftsverkehr



Handlungsanleitung für die Praxis

Sichere Geschäftsprozesse: Umsetzung im Unternehmen – Branchenbeispiel Sondermaschinenbau

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

März 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 natürlich die dortigen speziellen Rahmenbedingungen mit berücksichtigt werden.

2 Ausgangssituation



Das begutachtete Unternehmen der Sondermaschinenbaubranche stellt Fluid-Befüllanlagen für die unterschiedlichen Medien in Fahrzeugen sowie zugehörige Prüftechnik (inkl. Steuergerätekommunikation, Automatisierung, Versorgungseinrichtungen etc.) zum Einsatz in Montagelinien, im Nacharbeitsbereich und im Versuchsfeld her. Im Bereich Montagetechnik bietet das Unternehmen kundenspezifische Systemlösungen zum Einbau von Fahrzeugmodulen, Glasdächern und Scheiben sowie zur Herstellung von Fahrzeugkomponenten. Das Unternehmen verfügt über ein weltweites Service- und Vertriebsnetz und beschäftigt 170 Mitarbeiter.

Da die IT alle Firmenprozesse durchdringt, ist im Unternehmen ein Administrator angestellt, der die IT-Prozesse kontinuierlich plant und realisiert. Die vorhandenen Lösungen zur IT-Sicherheit werden von übergeordneten Anforderungen des Konzerns bestimmt. Hieraus resultiert insbesondere eine sehr hohe Sicherheitsrichtlinie bezüglich des abgesicherten externen Zugangs zum Unternehmensnetzwerk. Die EDV-Struktur wird durch SAP-Software bestimmt, die bei einem Provider betrieben wird.

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,
- ▶ Keine Verschlüsselung kritischer Daten,
- ▶ Nur Teilauswertung von Protokolldateien,
- ▶ Keine Dokumentationen zur Behebung kritischer Situationen,
- ▶ Keine aktenkundige Belehrung über das unternehmensinterne Verbot zur Nutzung von E-Mail und Internet für private Zwecke.

3 Untersuchungsmodell

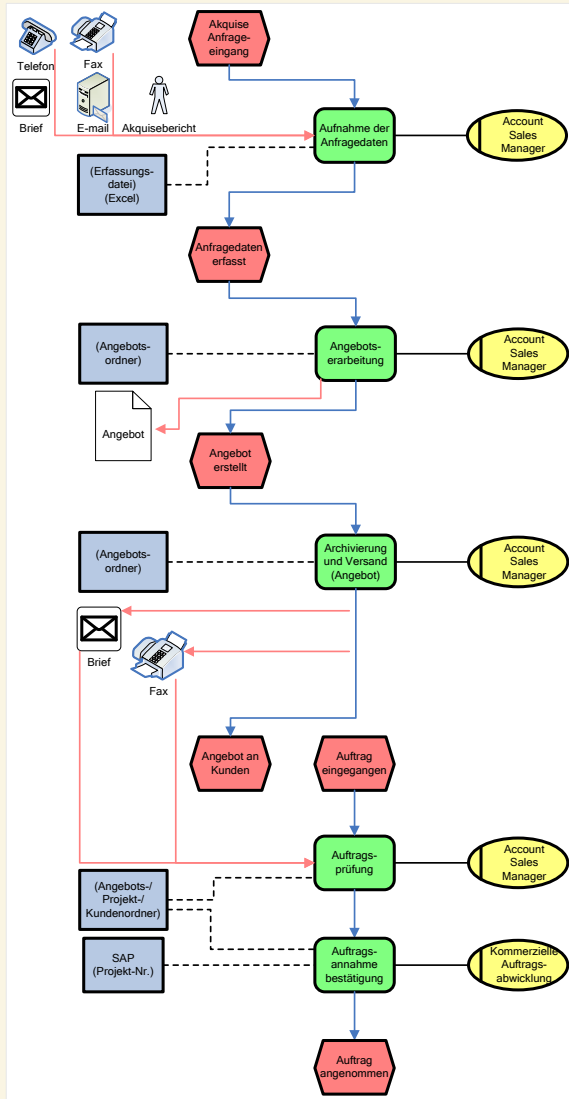
Im Rahmen der Projektaktivitäten wurden die Geschäftsprozesse im Unternehmen analysiert, die im besonderen Maße durch die Informationstechnik geprägt sind. Gemeinsam mit den Mitarbeitern des Unternehmens wurden die Zusammenhänge zwischen den Prozessschritten in der vorhandenen IT-Infrastruktur und den Anwendern dieser Infrastruktur ermittelt und aufbereitet.

Für den vorliegenden Fall wurden die nachfolgenden Prozesse analysiert:

- ▶ Angebotserstellung,
- ▶ Projektablauf,
- ▶ Service,
- ▶ Rechnungslegung/Rechnungsbegleichung.

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.

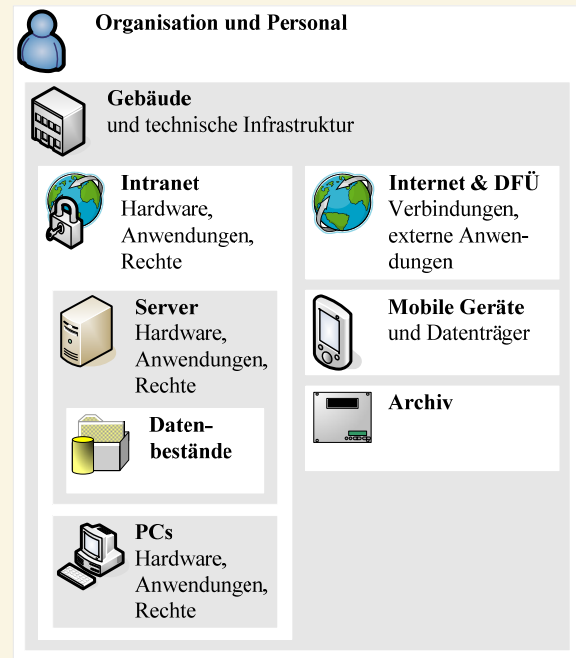
Abbildung 1: Erfassungsbeispiel für die Prozesse der Angebotserstellung und Auftragsprüfung



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 gespeicherten Daten (Datenbestände) näher betrachtet.

Abbildung 2: Struktur der Ergebnisdarstellung



4 Datenbestände



Der Großteil der geschäftskritischen Daten wird im begleiteten Unternehmen in einer Datenbank des SAP-Systems und auf File-Servern gespeichert. Das SAP-System wird durch einen externen Dienstleister gewartet und wird als sehr zuverlässig eingeschätzt. Die Datensicherung erfolgt täglich durch ein Voll-Backup. Der Speicherumfang der Daten liegt im Terabyte-Bereich. Das Backup wird über Festplatten realisiert und erfüllt damit einen hohen Sicherheitsstandard. Eine zusätzliche Archivierung erfolgt monatlich. Der Zugriff auf diese Datenbestände ist durch ein Passwort und Gruppenrichtlinien gesichert.

Weiterhin werden Daten Dritter (z. B. CAD-Dateien) verarbeitet. Der Zugriff zu Personendaten wurde im Rahmen des Projekts nicht untersucht. Es ist ein wachsender Anteil von Geschäftsdaten zu verzeichnen, die über die E-Mail-Kommunikation des Unternehmens erzeugt werden.

Empfehlung

- ▶ Eine Übersicht der verwendeten Verzeichnisstruktur (Speicherorte der Daten) sollte gemäß den Anforderungen an Compliance und GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen) erstellt werden.
- ▶ Der Einsatz von Verschlüsselungsverfahren sollte insbesondere für sensible Datenbestände überdacht werden.
- ▶ Da zu erwarten ist, dass die Bedeutung von Geschäftsdaten im Rahmen der E-Mail-Kommunikation weiter zunehmen wird, 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-System), und die gängigen Sicherheitsvorkehrungen (Zugangskontrolle, Sicherheits-Updates, Virenschutz, Band-Backup) werden beachtet. Der Server bedient zum einen die üblichen Dienste (Netzwerk, Datei, Druck), zum anderen sind auf ihm Datenbanken und zentrale Anwendungssoftware installiert. Da die Wiederbeschaffung der Server-Komponenten nicht mehr gesichert ist, wird derzeit eine neue Ausstattung der IT-Technik vorbereitet. Hierfür werden Betriebssystem, Datenbanken und Anwendungssoftware manuell sowie Virensignaturen automatisch aktualisiert.

Empfehlung

- ▶ Eine Wiederanlaufdokumentation des Servers (Hardware, Anwendungen, Daten, Einstellungen, Virenschutz) sollte für einen

möglichen Ausfall des Servers vorgehalten werden, um eine zeitnahe Reaktion zu ermöglichen.

- ▶ Die relevanten log-Dateien (Betriebssystem, E-Mail) sollten täglich ausgewertet werden.



5.2 PCs

Es werden Windows-Betriebssysteme eingesetzt. Hier werden ebenfalls die gängigen Sicherheitsvorkehrungen (Zugangskontrolle, Passwortgebrauch, Sicherheits-Updates, Virenschutz) beachtet. Die einzelnen PCs sind in der Regel austauschbar, so dass bei einem möglichen Ausfall Ersatz vorhanden ist. Spezifische PCs, die nicht ohne weiteres ausgetauscht werden können, lassen sich bei einem Ausfall in einem Zeitrahmen ersetzen, der keine den Betriebsablauf gefährdenden Zustände erwarten lässt. Auf den PCs werden keine Daten gespeichert, die kritisch für den Betriebsablauf sind.

Empfehlung

- ▶ Da die Verwendung von externen Datenträgern (USB-Sticks, CDs) an bestimmten Arbeitsplätzen betriebsbedingt notwendig ist, 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. Durch die Unternehmensgröße bedingt werden mehrere aktive Komponenten (z. B. Switches) verwendet. WLAN-Komponenten werden ausschließlich entkoppelt von der übrigen produktiven Netzwerkstruktur eingesetzt. Zur zeitnahen Wieder-

beschaffung der Hardware-Komponenten im Schadensfall bestehen geschäftliche Beziehungen zu Dienstleistungsunternehmen.

Die Netzstruktur ist in einer Datenbank ausführlich dokumentiert, wird kontinuierlich aktualisiert und ermöglicht es dem Administrator, von jeder Stelle des Unternehmens aus relevante Informationen zu erhalten.

Empfehlung

- ▶ Eine Dokumentation über Passwörter und Regeln aller aktiven Elemente (z. B. Switches) sollte angelegt werden.
- ▶ Programme zum Scannen und Auswerten des Netzverkehrs sollten in zukünftigen Maßnahmen zur Vorsorge gegen Störungen, Überbelastungen etc. vorgesehen werden.

7 Weitere Komponenten

7.1 Internet



Vom Intranet aus besteht ein Zugang zu extern liegenden Komponenten mittels Internetverbindungen, die dem Unternehmen über VPN von der Konzernzentrale zur Verfügung gestellt werden. Die sicherheitsüblichen Hard- und Software-Komponenten sind vorhanden. Die zugehörigen Sicherheitsregeln sind eingerichtet. Die Werkseinstellungen für Passwörter wurden verändert. Die Firewall wird durch einen Dienstleister administriert. Über einen FTP-Server werden Unterlagen für Außendienstmitarbeiter und Geschäftskunden bereitgestellt, wobei der Zugang bei längerer Nichtnutzung automatisch gesperrt wird. Redundanzen für externe Verbindungskanäle sind nicht vorhanden.

Empfehlung

- ▶ Da das betriebsbestimmende SAP-System extern vorgehalten wird, sollte die Einrichtung eines redundanten Verbindungskanals für den Störfall erwogen werden.

- ▶ Die Infrastruktur der Sicherheitskomponenten (Software mit Versionsnummer, Passwörter) sollte dokumentiert werden.
- ▶ Die eingestellten Regeln sollten dokumentiert werden.
- ▶ Die erstellten Unterlagen sollten sicher verwahrt werden und im Bedarfsfall schnell auffindbar sein.
- ▶ Der Datenverkehr zum Internet sollte mittels entsprechender Software täglich überwacht werden, um schnell auf unbekanntere Ereignisse reagieren zu können.
- ▶ Sicherheits-Updates der genutzten Hard- (Firmware) und Software sollten zeitnah installiert werden.
- ▶ Fragen zur IT-Sicherheit sollten mit den Dienstleistern schriftlich geregelt werden.

7.2 Mobile Geräte



Laptops und mobile Datenträger (USB-Speichermedien, CD, Disketten) werden von den Mitarbeitern genutzt und können an Computern verwendet werden.

Empfehlung

- ▶ Laptops, die nach der Nutzung im Außendienst wieder an das Firmennetz angeschlossen werden, sollten über einen vom Firmennetz getrennten PC mit Sicherheits-Updates und Virenschutzkomponenten ausgerüstet werden, bevor die eigentliche Verbindung zum Firmennetz hergestellt wird.
- ▶ Für das Unternehmen sensible Daten sollten (zukünftig) auf allen mobilen Geräten verschlüsselt abgelegt werden (z. B. Laptops der Servicemitarbeiter, USB-Sticks etc.).
- ▶ Servicemitarbeiter sollten über die Gefahren der Nutzung mobiler Geräte außerhalb der Firma geschult und aktenkundig belehrt werden.

- ▶ Für Administratoren werden regelmäßige Weiterbildungen zu den Themen Verschlüsselung, WLAN und Bluetooth empfohlen.
- ▶ Da die Verwendung von PDAs in Verbindung mit Bluetooth eine neuartige Sicherheitslücke darstellt, sollten die Nutzer entsprechend geschult werden.

7.3 Archiv



Die Archivierung von Daten erfolgt auf Festplatten, zu denen nur ausgewählte Mitarbeiter Zugang haben. Die Archivmedien werden in einem unabhängigen Brandabschnitt in einem Schutzschrank gelagert. Der Speicherbedarf der Daten liegt im Terabyte-Bereich.

E-Mails sind in die Archivierung eingeschlossen. Es ist jedoch keine separate Software zur geordneten Ablage von E-Mails vorhanden.

Empfehlung

- ▶ Vorschriften für die Archivierung sollten im Unternehmen schriftlich festgelegt werden.
- ▶ Für die Auswahl der zu archivierenden Daten sollten die Anforderungen an Compliance und insbesondere an die GDPdU beachtet werden.
- ▶ Bei einem Versionswechsel von Anwendungen und einer notwendiger Migration der Daten sollten auch die archivierten Daten migriert werden, damit diese bei Bedarf weiterhin verwendet werden können.

8 Gebäude und Infrastruktur



Das Firmengebäude ist unter sicherheitstechnischen Gesichtspunkten in einem guten Zustand. Die Lage in einem Gewerbegebiet schließt Vandalismus jedoch nicht aus. Besucherverkehr in den Büroräumen findet kontrolliert statt. In der Fertigungshalle kann zeitweise Fremdpersonal

anwesend sein. Der Server-Raum ist brand-schutztechnisch hochwertig gesichert.

Empfehlung

- ▶ Die Mitarbeiter sollten bezüglich des Umgangs mit Fremdpersonal vor dem Hintergrund der IT-Sicherheit belehrt werden.

9 Organisation und Personal



Im Unternehmen sind nach Aussage der Unternehmensleitung pflichtbewusste Mitarbeiter eingestellt. Neben den Angestellten sind Studenten und Praktikanten anwesend.

Empfehlung

Im Unternehmen sollten Schulungen und aktienkundige Belehrungen zu den nachfolgenden 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. Es besteht jedoch eine Verantwortung des Unternehmens, sich gegen die Spionage von Passwörtern etc. zu schützen),
- ▶ Belehrungen zum Virenschutz bei der Nutzung des Internets (einschließlich E-Mail) und der Nutzung mobiler Geräte und Datenträger,
- ▶ Belehrungen zum Umgang mit Daten Dritter (CAD-Dateien, Programme, Betriebsmitteldaten von Kunden, Messprotokolle etc.) und Daten und Programmen entsprechend der Copyright-Richtlinien,
- ▶ Für die Zukunft: 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. Bedingt durch die Unternehmensgröße kennen die Mitarbeiter die richtigen Ansprechpartner bei betriebsbedingten Störungen. Bei akuten Störungen sind ausreichende Ressourcen vorhanden, um diese schnellstmöglich zu beheben.

10.2 Strategisches Verhalten

Der im Unternehmen eingesetzte Administrator sorgt auch für die Belange der IT-Sicherheit. Die Unternehmensführung hat die Sicherheit der IT-Ressourcen als wichtiges Element in den Unternehmensprozessen erkannt und fördert diese. Darüber hinaus wurde die Verbesserung der Sicherheit der IT-Prozesse als wichtige Aufgabe definiert.

Empfehlung

- ▶ Für den Schadens- und Notfall sollten die genannten Dokumentationen entwickelt und in Papierform gesichert abgelegt werden. Dies bezieht sich auch auf Unterlagen, die eventuell durch Dienstleister bereitgestellt werden müssen.
- ▶ Mitarbeiter (einschließlich Servicemitarbeiter) sollten zu Fragen der IT-Sicherheit geschult werden.
- ▶ Die private Nutzung der IT-Infrastruktur und des Internets 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 hierfür sollten bereitgestellt werden.
- ▶ Die bereits erfüllten, zuzüglich der hier benannten Empfehlungen stellen wesentliche Bausteine auf dem Weg der IT-Zertifizierung (Selbstzertifizierung) dar.
- ▶ Die Anforderungen an die sichere Speicherung von Daten, die durch Compliance gestellt sind, sollten über die Anforderungen durch die GDPdU hinaus zukünftig besonders beachtet werden. (Die Prozesse, in denen betriebswirtschaftliche Daten verarbeitet werden, wurden in diesem Projekt nicht speziell berücksichtigt. Deshalb wird keine Aussage zum Stand der GDPdU vorgenommen.)
- ▶ 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.
- 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.