



Gefördert durch das
Bundesministerium
für Wirtschaft
und Technologie



Netzwerk Elektronischer
Geschäftsverkehr



Handlungsanleitung für die Praxis

Sichere Geschäftsprozesse: Umsetzung im Unternehmen – Branchenbeispiel Umwelt-/Geotechnik

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

Mai 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 seit 1991 erfolgreich am Umweltmarkt tätige mittelständische Unternehmen besteht aus einem Verbund

von fünf selbständig agierenden Ingenieurunternehmen. Dieser wurde 2007 zu einer Ingenieur AG verschmolzen und ist überregional tätig. Die im Unternehmen tätigen über 130 Ingenieure, Naturwissenschaftler und Techniker verfügen über umfangreiche nationale und internationale Erfahrungen und enge Kontakte zu Technischen Universitäten. Diese gewährleisten einen aktiven Zugang zu den neuesten theoretischen und experimentellen Arbeiten auf den Gebieten der Boden- und Gebirgsmechanik sowie Umwelt- und Bautechnik.

Das Unternehmen bietet aus einer Hand eine umfassende, fachübergreifende Bearbeitung von Ingenieurleistungen in allen Phasen der Erkundung, Planung, Bau und Betreuung von Objekten des Ingenieurbaus an. Aufgaben mit komplexem und interdisziplinärem Charakter können fachlich kompetent und kostengünstig innerhalb des Firmenverbundes realisiert werden.

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

- ▶ geringes Wissen aller Mitarbeiter zu aktuellen Sicherheitsgefahren,
- ▶ keine Verschlüsselung von kritischen Daten,

- ▶ unzureichende Zugangsregelung zu Server-Räumen,
- ▶ Archivierung der Daten nicht nach den Anforderungen aus Compliance und GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen),
- ▶ Gefahren bei der Nutzung mobiler Geräte im Einsatz und bei der Wiedereinbindung in das interne Unternehmensnetz,
- ▶ nur Teilauswertung von Protokolldateien.

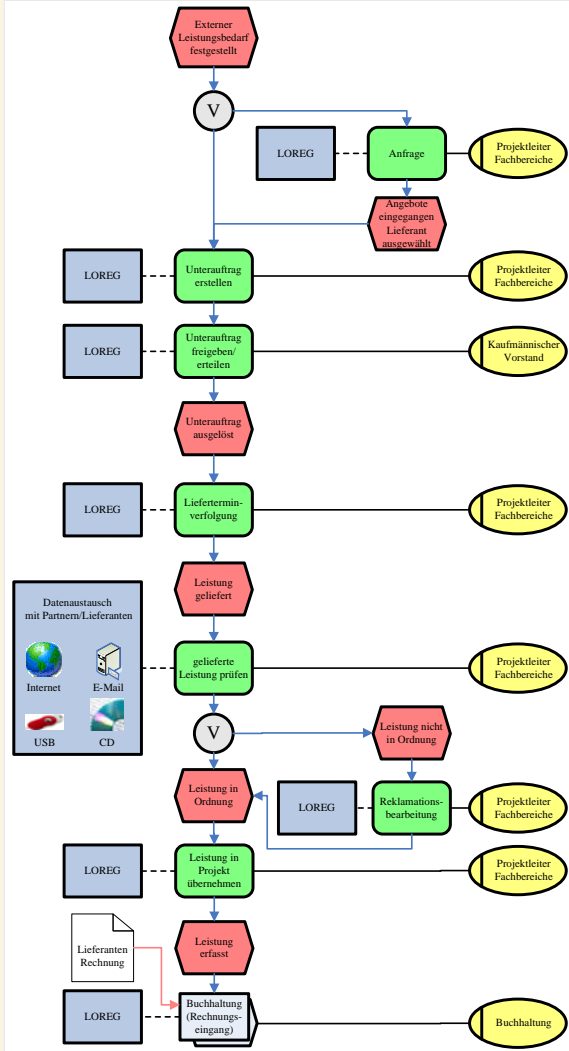
3 Untersuchungsmodell

Die folgenden Empfehlungen beruhen auf einer detaillierten Analyse der Geschäftsprozesse im Unternehmen. Dazu wurden Befragungen von Mitarbeitern des Unternehmens durchgeführt. Zusammenfassend lässt sich festhalten, dass Geschäftsführung und IT-Verantwortliche Fragen der IT-Sicherheit als wichtiges Firmengut betrachten und Maßnahmen zur Verbesserung der IT-Sicherheit kontinuierlich verfolgen. Für den vorliegenden Fall wurden die nachfolgenden Prozesse analysiert:

- ▶ Angebotserstellung,
- ▶ Projektablauf,
- ▶ Rechnungslegung/Rechnungsbegleichung,
- ▶ Beschaffung,
- ▶ IT-Management.

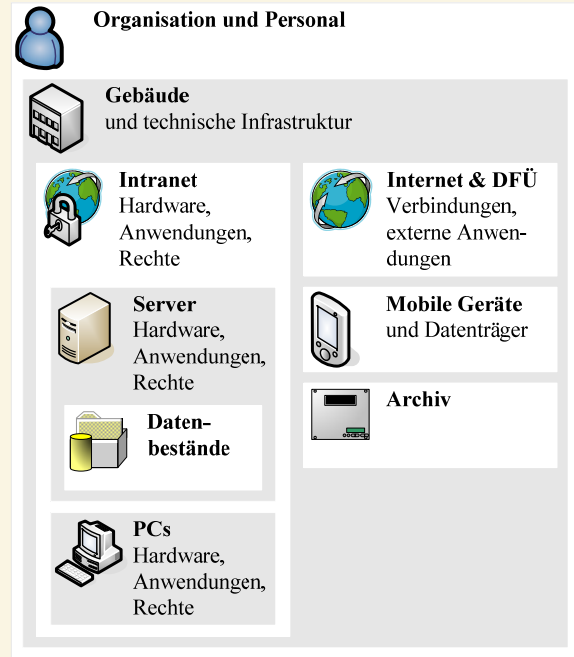
Das Unternehmen ist nach ISO9001 zertifiziert. Damit sind eine Vielzahl der Unternehmensprozesse, die die IT-Sicherheit tangieren, dokumentiert und in Anweisungen umgesetzt.

Abbildung 1: Erfassungsbeispiel für die Prozesse der Abwicklung von Unteraufträgen



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



Geschäftskritische Daten sind zum überwiegenden Teil in einer zentralen Datenbank und auf File-Servern gespeichert. Die Zuordnung der Daten zu verschiedenen Servern für verschiedene Unternehmensbereiche erlaubt im Notfall eine schnelle Wiederherstellung.

Die Daten werden täglich durch Backup gesichert und der Zugriff auf diese Datenbestände ist über Passwort und Gruppenrichtlinien gesichert. Es werden Daten Dritter verarbeitet. Der Zugriff zu Personendaten wurde im Begleitprojekt nicht untersucht. Bislang spielt die Versendung von Geschäftsdaten im Rahmen der E-Mail-Kommunikation nur eine geringe Rolle. Bis auf einen Fall wurden bisher weder von Kunden noch von Partnerunternehmen erhöhte Anforderungen bezüglich der IT-Sicherheit gestellt.

Empfehlung

- ▶ Eine Übersicht der verwendeten Verzeichnisstruktur (Speicherorte der Daten) sollte gemäß den Anforderungen an Compliance und GDPdU erstellt werden.
- ▶ Der Einsatz von Verschlüsselungsverfahren sollte insbesondere für sensible Datenbestände überdacht werden.
- ▶ Da zu erwarten ist, dass die Bedeutung von Geschäftsdaten per 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

Es sind mehrere Windows Server im Einsatz (RAID-Systeme). Die üblichen Sicherheitsvorkehrungen (Zugangskontrolle, Sicherheits-Updates, Virenschutz, Backup) werden beachtet. Auf diesen Servern werden die üblichen Dienste (Netzwerk, Datei, Druck) bedient. Datenbanken und zentrale Anwendungssoftware sind installiert. Die Server sind in einem verschlossenen Schrank klimatisiert angeordnet. Die Möglichkeit zur Wiederbeschaffung der Server-Hardware ist sichergestellt. Der Zugang zum Server-Raum ist, bedingt durch räumliche Beschränkungen, allen Mitarbeitern möglich.

Aufgrund des hohen Speicherplatzbedarfs einiger Dateien werden relevante Dokumente parallel in den Außenstellen des Unternehmens vorgehalten. Die Synchronisation der Arbeitsstände erfolgt manuell durch die Mitarbeiter.

Empfehlung

- ▶ Eine Wiederanlaufdokumentation der Server (Hardware, Anwendungen, Daten, Einstellungen, Virenschutz) sollte für einen möglichen Ausfall vorgehalten werden, um eine zeitnahe Reaktion zu ermöglichen.
- ▶ Die relevanten log-Dateien (Betriebssystem, E-Mail) sollten täglich ausgewertet werden.
- ▶ Der Zugang zum Server-Raum sollte neu geregelt werden.
- ▶ Notfallkonzepte sollten entwickelt werden.

5.2 PCs



Auf den PCs werden Windows-Betriebssysteme eingesetzt. Die gängigen Sicherheitsvorkehrungen (Zugangskontrolle, Passwortverwendung, Sicherheits-Updates, Virenschutz) werden beachtet. Die einzelnen PCs sind in der Regel austauschbar, so dass bei einem möglichen Ausfall direkt 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 selbst werden keine Daten gespeichert, deren Verlust sich kritisch auf den Betriebsablauf auswirken könnte.

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.

- ▶ Ein Teil der PCs besitzt einen eigenen Internetanschluss via ISDN. Die Nutzung dieser Verbindungen sollte restriktiv erfolgen.

6 Intranet



Das Intranet des Unternehmens ist verkabelt. Durch die Unternehmensgröße bedingt werden mehrere aktive Komponenten (Switches) verwendet. WLAN-Komponenten sind nicht im Einsatz. Zur zeitnahen Wiederbeschaffung der Hardware-Komponenten im Schadensfall bestehen geschäftliche Beziehungen zu Dienstleistungsunternehmen.

Empfehlung

- ▶ Eine Dokumentation über Passwörter und Regeln aller aktiven Elemente (Switches, ISDN-Karten) sollte angelegt werden.
- ▶ Programme zum Scannen und Auswerten des internen Netzwerkverkehrs sollten für zukünftige Maßnahmen zur Vorsorge gegen Störungen, Überbelastungen etc. vorgesehen werden.

7 Weitere Komponenten

7.1 Internet



Der Zugang zum Internet erfolgt mittels einer gesicherten ISDN-Verbindung. Der Datenverkehr zu und zwischen den Außenstellen des Unternehmens erfolgt über VPN-Verbindungen. Die sicherheitsüblichen Hardware- und Software-Komponenten sind vorhanden und für den Zugang ist ein von den Datenservern unabhängiger Gateway-Server einschließlich Firewall und Sicherheitsregeln eingerichtet.

Die E-Mail-Kommunikation aller Zweigstellen wird über einen zentralen Knoten realisiert.

Die Werkeinstellungen für Passwörter sind verändert. Für DATEV-Dienste des Unternehmens besteht eine eigene ISDN-Verbindung.

Empfehlung

- ▶ Die Infrastruktur der Sicherheitskomponenten (Software mit Versionsnummer, Passwörter) sowie die eingestellten Regeln (z. B. die Regeln der Firewall) sollten dokumentiert werden.
- ▶ Eine sichere Verwahrung der Unterlagen und Dokumente sollte sichergestellt sein.
- ▶ Der Datenverkehr zum Internet sollte täglich überwacht und mit entsprechender Software analysiert werden, um schnell auf Unregelmäßigkeiten reagieren zu können.
- ▶ Sicherheits-Updates der genutzten Hard- und Firmware sollten zeitnah installiert werden.
- ▶ Fragen zur IT-Sicherheit sollten mit Dienstleistern schriftlich geregelt werden.
- ▶ Die Internetverbindungen der einzelnen Zweigstellen stellen eine potenzielle Sicherheitslücke zur Einschleusung von Schad-Software dar. Die dezentralen lokalen Netzwerke sollten mittels geeigneter Monitoring-Anwendungen überwacht werden.

7.2 Mobile Geräte



Firmen-Laptops werden von den Mitarbeitern auch im Außendienst genutzt. Sie enthalten selbst jedoch keine sicherheitsrelevanten Informationen. Mobile Datenträger (USB-Speichermedien, CD, Disketten) werden genutzt und können an Computern verwendet werden.

Empfehlung

- ▶ Laptops, die nach der Nutzung im Außendienst wieder an das Firmennetz angeschlossen werden, sollten erst nach einem Sicherheitscheck und Sicherheits-Updates,

die eigentliche Verbindung zum Firmennetz herstellen dürfen.

- ▶ Unternehmenssensible 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 Netzwerk-Monitoring empfohlen.
- ▶ Da die Verwendung von PDAs in Verbindung mit der Bluetooth-Technologie eine neuartige Sicherheitslücke darstellt, sollten die Nutzer entsprechend geschult werden.

7.3 Archiv



Die Archivierung von Daten erfolgt auf CDs, DVDs und Magnetfestplatten. Die Lagerung erfolgt in einem Datenschränk des Unternehmens. Ein zusätzliches Backup wird außerhalb des Unternehmens aufbewahrt.

Eine spezielle Archivierungs-Software wird nicht genutzt, es wurden jedoch Vorschriften für die Archivierung festgelegt.

Empfehlung

- ▶ Für die Auswahl der zu archivierenden Daten sollen die Anforderungen an die Compliance und insbesondere an die GDPdU beachtet werden.
- ▶ Die Archivierung mittels WORM-Speicher (Write Once Read Many) ist zu untersuchen.
- ▶ Bei einem Versionswechsel von Anwendungen und notwendiger Migration der Daten, sind auch die archivierten Daten zu migrieren.

8 Gebäude und Infrastruktur



Das Firmengebäude ist sicherheitstechnisch in einem guten Zustand. Die Lage in einem öffentlich zugänglichen Gebäude schließt Vandalismus jedoch nicht aus. Besucherverkehr in den Büroräumen ist zugelassen.

Empfehlung

- ▶ Die Zugangskontrolle in die Firmenräume sollte verschärft werden.
- ▶ Die Mitarbeiter sollten bezüglich der Risiken durch Besucherverkehr belehrt werden.

9 Organisation und Personal



Im Unternehmen sind nach Aussage der Unternehmensleitung pflichtbewusste Mitarbeiter eingestellt. Neben den Angestellten sind zeitweise Studenten und Praktikanten anwesend. Es existieren Arbeitsanweisungen zur Nutzung der IT-Infrastruktur und insbesondere zur Nutzung von E-Mail und Internet. Deren Nutzung für private Zwecke ist verboten.

Empfehlung

Im Unternehmen sollten die Schulungen und aktenkundige Belehrungen um nachfolgende Themen erweitert werden:

- ▶ Belehrungen zum Virenschutz bei der Nutzung des Internets (einschließlich E-Mail) sowie 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.

10 Fazit: Aufgaben für die Unternehmensführung

10.1 Reaktives Verhalten

Durch die Unternehmensgröße bedingt kennen die Mitarbeiter notwendige 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. Die Unternehmensführung hat die Verbesserung der Sicherheit der IT-Prozesse als wichtige Aufgabe definiert.

Das Unternehmen beschäftigt einen Administrator und einen Stellvertreter, die auch für die Belange der IT-Sicherheit sorgen.

Empfehlung

- ▶ 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) sollen zu Fragen der IT-Sicherheit geschult werden.
- ▶ Die private Nutzung der IT-Infrastruktur und des Internet oder deren Verbot sollten schriftlich geregelt werden.

- ▶ Durch den Administrator sollen folgende Aufgaben kontinuierlich 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 dafür sind bereitzustellen.
- ▶ 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 im Rahmen der Compliance sollten zukünftig über die Anforderungen der GDPdU besonders beachtet werden. Im vorliegenden Projekt wurden die Prozesse, in denen betriebswirtschaftliche Daten verarbeitet werden, nicht berücksichtigt. Eine Aussage zum Stand der GDPdU kann unter diesen Bedingungen nicht vorgenommen werden.
- ▶ 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, Zugangschutz, 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:

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 team members and their associated logos are:

- 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

A legend in the top left of the map area identifies symbols: a yellow dot for 'Regionales Kompetenzzentrum', an orange triangle for 'Branchen-Kompetenzzentrum', a green square for 'externer Netzwerkpartner', and a blue circle for 'Rüstköche'.

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.