



Gefördert durch das
Bundesministerium
für Wirtschaft
und Technologie



Netzwerk Elektronischer
Geschäftsverkehr



Handlungsanleitung für die Praxis

Sichere Geschäftsprozesse: Umsetzung im Unternehmen – Branchenbeispiel Informationstechnik

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

MECK Würzburg – Mainfränkisches Electronic Commerce Kompetenzzentrum

Stand

Mai 2008

- 1 Vorwort**
- 2 Ausgangssituation**
- 3 Untersuchungsmodell**
- 4 Datenbestände**
- 5 Computer und Anwendungen**
 - 5.1 Server
 - 5.2 PCs
- 6 Kommunikation**
- 7 Weitere Komponenten**
 - 7.1 Internet
 - 7.2 Mobile Geräte
 - 7.3 Archiv
- 8 Gebäude und Infrastruktur**
- 9 Organisation und Personal**
- 10 Fazit: Strategische Aufgaben für die künftige Ausrichtung**
- 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 Analyse im Bereich der Informationssicherheit zeigen beispielhaft die Relevanz des Themas für diese Branche auf. Für die individuelle Bewertung der Informationssicherheit in einem konkreten Unternehmen müssen natürlich die dortigen speziellen Rahmenbedingungen mit berücksichtigt werden.

2 Ausgangssituation



Das begutachtete Unternehmen der IT-Dienstleistungsbranche besteht seit 2005 im fränkischen Raum. Die Firma

versteht sich als inländische Alternative zum derzeit im Markt vorherrschenden Trend der Verlagerung von hochspezialisierten Arbeitsplätzen ins osteuropäische und asiatische Niedriglohland.

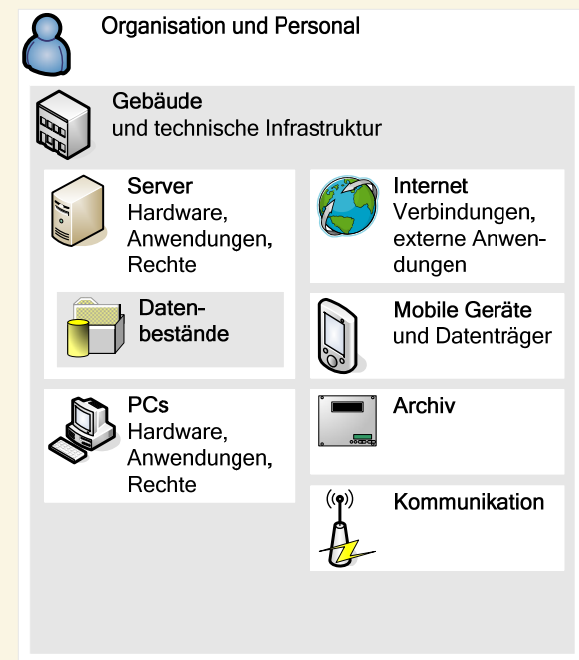
Vom zentralen Standort aus werden die Kunden in den Geschäftsbereichen IT-Consulting, IT-Outtasking und IT-Systembetrieb betreut. Darüber hinaus bietet die Firma individuelle Lösungen im Bereich Datensicherung, Systemmonitoring und in der IT-Notfallvorsorge an.

3 Untersuchungsmodell

Auf Basis eines im Vorfeld definierten Betrachtungsgegenstandes erfolgte eine eingehende Analyse der zentralen IT-Ausstattung und der damit verbundenen Prozesse. Dabei wurde vor allem darauf Wert gelegt, dass eine krisensichere Abwicklung der täglichen Aufgaben in jedem Fall gewährleistet ist. Das betrachtete Unternehmen befindet sich noch in der Marktdurchdringungsphase. Den Verantwortlichen war von entscheidender Bedeutung, dass die bereits etablierten (Beratungs-)Prozesse allzeit krisensicher durchgeführt werden können, denn nur so sind ein stetiges Wachstum und ein zukunftsicherer Fortbestand gewährleistet.

Die folgende Ergebnisbeschreibung basiert auf einem „Schalenmodell“, in dem die unterschiedlichen Bereiche des Unternehmens getrennt voneinander betrachtet werden. Bei der Durchführung dieser Analyse wurden sowohl die Vorgaben der etablierten Sicherheitsstandards ISO und BSI sowie die Wünsche und Pläne der Verantwortlichen vor Ort einbezogen.

Abbildung 1: Struktur der Ergebnisdarstellung



Die Vorgehensweise innerhalb dieses Projekts erfolgte auf Basis einer abgestimmten Vorgehensbeschreibung, um die Ergebnisse auch branchenübergreifend aufarbeiten und vergleichen zu können.

4 Datenbestände



Die in den vergangenen Projekten erarbeiteten Daten und Informationen stellen einen Großteil des Know-hows des Unternehmens dar. Dieses bildet zusammen mit der mehrjährigen Erfahrung und kombiniert mit aktuellen Weiterbildungsmaßnahmen das Alleinstellungsmerkmal des Unternehmens. Daher sollten die digital gespeicherten Informationen mit besonderer Sorgfalt behandelt werden. Eine unkontrollierte Weitergabe an Dritte oder ein Verlust der Datenbestände können insbesondere in dieser Branche in keinster Weise toleriert werden. Alle Anstrengungen sollten darauf abzielen, diesen Produktionsfaktor (Information) nachhaltig und gewissenhaft zu schützen. Aktuell kommt bereits eine Verschlüsselung und Langzeitarchivierung der Daten zur Anwendung.

Empfehlungen

- ▶ Die bereits eingeführten sicherheitsrelevanten Prozesse und Vorgehensweisen sollten nach einem standardisierten Schema dokumentiert und verwaltet werden. Dadurch ist sicherzustellen, dass:
 - die Prozesse von allen Mitarbeitern auch in kritischen Situationen eingehalten werden, eine Weiterentwicklung und Anpassung an neue Rahmenbedingungen gewährleistet ist, sich neue Mitarbeiter schnell an diese Vorgaben gewöhnen und dadurch die Phase der Eingewöhnung möglichst kurz ist.
- ▶ Die durchgeführte Langzeitarchivierung muss hohen Anforderungen genügen. An dieser Stelle sollte eine krisensichere Lösung erarbeitet werden, bei der auch eine Datensicherung außerhalb der Firmenräume gelagert wird.
- ▶ Obwohl bereits eine Verschlüsselung der Daten erfolgt, sollte ein regelmäßiger Wechsel des verwendeten kryptographischen Verfahrens in Erwägung gezogen werden, da

sowohl die technische Entwicklung als auch die kriminelle Energie immer rasanter voranschreiten.

- ▶ Ein standardisiertes Verfahren, welches die Speicherung dezentral generierter Daten auf der zentralen Serverstruktur ermöglicht bzw. erzwingt, kann den Verbleib der notwendigen Informationen im Unternehmen sicherstellen.

5 Computer und Anwendungen

Wie in der Beratungsbranche üblich, wickelt das begleitete Unternehmen zahlreiche Projekte mit unterschiedlichen Kunden parallel ab. Daher muss bei der nachfolgenden Analyse der bestehenden IT-Infrastruktur berücksichtigt werden, dass sowohl Installationen von Test- als auch Produktivsystemen vorzufinden sind. Trotz der räumlichen Nähe müssen für die produktiven Systeme strikte Regelungen gelten, die konsequent eingehalten werden.

5.1 Server



Zahlreiche (Server-)Dienste und Anwendungen werden von den Verantwortlichen vor Ort betrieben und gewartet. Dadurch können die unterschiedlichen Applikationen – aus dem Bereich der Standardsoftware und Open-Source-Lösungen – genau auf die individuellen Anforderungen und Wünsche der Kunden zugeschnitten werden. Allerdings werden durch dieses Vorgehen auch hohe Anforderungen an das Know-how der Mitarbeiter gestellt, die die regelmäßige und fachkundige Wartung und Pflege der verschiedenen Applikationen sicherstellen. Zur systemimmanenten Vermeidung von Schwachstellen ist eine Verfahrensweise erarbeitet worden, die sicherstellt, dass ein fehlerminimierender Systembetrieb gewährleistet ist.

Empfehlungen

- ▶ Mittelfristig sollte eine Fokussierung der aktuellen Infrastruktur auf das zwingend notwendige Maß erfolgen.
- ▶ Die verwendete technische Basis sollte im Hinblick auf mögliche Ausfälle in regelmäßigen Abständen erneuert bzw. durch eine Bevorratung mit Austauschgeräten die Ausfallzeiten entsprechend minimiert werden.
- ▶ Die Laufzeiten der Testsysteme sollten soweit möglich minimiert werden, da diese eine breite Angriffsfläche für mögliche Eindringlinge bzw. Fehler bieten.
- ▶ Um diese Vorgabe zu erfüllen, sollten Handlungsanweisungen erstellt werden, mit denen die zukünftigen Schritte detailliert geregelt werden. Sobald für diese Fälle eine Vorgabe getroffen wurde, können die Risiken in diesem Bereich reduziert werden.
- ▶ Eine grundsätzliche make or buy-Entscheidung in den Bereichen E-Mail-Server etc. wurde getroffen und sollte in regelmäßigen Abständen überprüft werden.
- ▶ Durch die Nutzung von Open-Source-Software können zahlreiche Vorteile realisiert werden. So fallen weniger Lizenzkosten an. Unter Umständen steht das verwendete System nicht im Blickpunkt der Öffentlichkeit, so dass gezielte Attacken und Angriffe von Computerschädlingen nicht so häufig zu verzeichnen sind.

5.2 PCs



In der Beratungsbranche stehen zahlreiche Termine vor Ort bei Kunden auf der Tagesordnung. Daher sind die meisten Mitarbeiter des Unternehmens mit Laptops ausgestattet. So kann die Arbeit beim Kunden effizienter erfolgen und Reisezeiten können mit sinnvollen Tätigkeiten überbrückt werden. Da während dieser Zeit außerhalb des Büros die eigene Erreichbarkeit

erheblich eingeschränkt ist, müssen Vorkehrungen getroffen werden, um auch auf kurzfristige Anfragen zeitnah und über gesicherte Verbindungen reagieren zu können.

Empfehlungen

- ▶ Die Daten auf den tragbaren Computern sollten permanent vor fremdem Zugriff geschützt werden. Diese Vorgabe gilt vor allem auch während der Arbeit an öffentlichen Orten, wie z. B. im Zug.
- ▶ Zum Schutz der Daten auf der Festplatte sollten aktuelle Technologien eingesetzt werden.
- ▶ Der Datenaustausch zwischen mobilen Nutzern und dem Internet sollte nur verschlüsselt und auf Basis der eigenen technischen Infrastruktur erfolgen. Bei der Nutzung öffentlich zugänglicher Einwahlknoten sollten zusätzliche Vorkehrungen getroffen werden, so dass kein unbefugter Dritter an der Kommunikation teilhaben kann.
- ▶ Beim Verlassen des Arbeitsplatzes sollte der Monitor in jedem Fall gesperrt werden und sensible Daten vor fremdem Zugriff geschützt werden.

6 Kommunikation



Die Erreichbarkeit ist entscheidend für den wirtschaftlichen Erfolg eines Beratungsunternehmens. Dies gilt sowohl für digitale Nachrichten als auch allgemein für die persönliche Kommunikation. Wichtige Daten und Informationen, auf die Mitarbeiter im Außendienst mobil zugreifen müssen, werden im begleiteten Unternehmen zentral vorgehalten.

Empfehlungen

- ▶ Sowohl für den Zugriff auf zentrale Datenbestände in den Räumlichkeiten des Unternehmens als auch für die Nutzung von (Tele-)Kommunikationsdienstleistungen sollten mehrere unterschiedliche Kanäle

parallel zur Verfügung stehen, um ein hohes Maß an Ausfallsicherheit zu gewährleisten.

- ▶ Wenn eine mobile Erreichbarkeit nicht gewährleistet werden kann, sollten tragbare Alternativen installiert werden, die dem Kunden eine erste Rückmeldung geben. Hier könnten z. B. Lösungen von einer einfachen Mailbox bis hin zu einem Voice over IP-Netzwerk zum Einsatz kommen.
- ▶ Sobald eine Kundennachricht eingetroffen ist, sollten Eskalationsmechanismen greifen, mit denen sichergestellt wird, dass diese Anfrage zeitnah bearbeitet wird.
- ▶ Verschiedene Zugriffsmöglichkeiten auf zentral gelagerte Daten helfen, Kunden schnell und kompetent zu antworten. Allerdings stellt jede zusätzliche Methode, eine externe Datenabfrage durchzuführen, ein weiteres Sicherheitsrisiko dar. Daher sollte bereits im Vorfeld gewissenhaft abgewogen werden, inwieweit die Vorteile für das tägliche Arbeiten die Nachteile erhöhter Sicherheitsmaßnahmen aufwiegen.
- ▶ Die zentrale Bereitstellung der Daten sollte den hohen Anforderungen und der flexiblen Arbeitsweise der Mitarbeiter genügen. Gerade weil das „Wissen“ der Mitarbeiter, das in diesen Systemen hinterlegt ist, für den Geschäftserfolg entscheidend ist, sollten exakte Vorgaben getroffen werden, wie und wann eine Datenaktualisierung erfolgen sollte.
- ▶ Die E-Mail-Kommunikation mit Kunden sollte ausschließlich verschlüsselt erfolgen.
- ▶ Die Verwaltung der eigenen Schlüssel sollte durch den Zugriff auf einen zentralen Adress-Server gemanagt werden.
- ▶ Die verwendeten Verschlüsselungsverfahren sollten in regelmäßigen Abständen aktualisiert werden, um potenzielle Sicherheitslücken kontinuierlich zu schließen.

- ▶ Der Umgang mit den Schlüsseln der verschiedenen Geschäftspartner sollten im Unternehmen durch ein Ablagesystem unterstützt werden, das Redundanzen vermeidet und einen größtmöglichen Sicherheitsstand garantiert.

7 Weitere Komponenten

7.1 Internet



Der Zugriff auf das Internet wird sowohl von den Räumlichkeiten des Unternehmens als auch von unterwegs zwingend benötigt. Da zahlreiche (Kunden-)Daten unternehmenssensible Informationen enthalten, muss ein sicherer Datentransfer zu jeder Zeit gewährleistet sein.

Für alle Aspekte der Internetnutzung ist eine entsprechende Vorgabe/Richtlinie erstellt worden, die für alle Mitarbeiter bindend ist.

Empfehlungen

- ▶ Sobald mit Passwörtern gearbeitet wird, sollten diese nur über eine sichere Verbindung eingegeben werden. Dies ist über einen getunnelten Verbindungsaufbau per VPN (Virtual Private Network) erreicht worden.
- ▶ Die Mitarbeiter sollten bei der täglichen Arbeit eine fest vorgegebene Verbindungsart erhalten, damit gewährleistet wird, dass keine unsichere Verbindung verwendet wird.
- ▶ Da zahlreiche Laptops zum Einsatz kommen, sollte deren Schutz bei der Arbeit in einem unternehmensfremden Netzwerk sichergestellt werden.

7.2 Mobile Geräte



Die Daten und Informationen auf mobilen Endgeräten sind in den letzten Monaten vermehrt Gegenstand von Angriffen geworden. Daher müssen die Verantwortlichen geeignete Maß-

nahmen wählen, um diesen Bedrohungen angemessen zu begegnen.

Empfehlungen

- ▶ Die Verantwortungsträger sollten eine grundsätzliche Entscheidung darüber treffen, ob Firmendaten bzw. Informationen der Kunden auf USB-Sticks oder PDAs übertragen werden dürfen. Die Vor- und Nachteile sollten hierbei gewissenhaft abgewogen werden.
- ▶ Sobald derartige Infrastruktur zum Einsatz kommt, sollten Daten ausschließlich verschlüsselt auf den Datenträgern abgelegt werden. Damit verbunden sollte ein Schlüsselmanagement implementiert werden, das den aktuellen Anforderungen genügt.
- ▶ Bei Verlust dieser Geräte sollten unverzüglich entsprechende Maßnahmen eingeleitet werden. Für diesen Fall sollte ein Maßnahmenkatalog erstellt werden, der dann schnell und unkompliziert abgearbeitet werden kann.
- ▶ Es sollte eine grundsätzliche Entscheidung darüber getroffen werden, inwieweit an den zentralen Servern die USB-Schnittstellen überhaupt aktiviert werden, da eine generelle Aktivierung zu Komplikationen und vorsätzlichen Datenverlusten führen kann.
- ▶ Bei Handys, Blackberrys etc. sollten der Dienst „Bluetooth“ und die Infrarotschnittstelle nur punktuell aktiviert werden, wenn diese unbedingt verwendet werden müssen.

7.3 Archiv



Da das Wissen der Mitarbeiter den entscheidenden Produktionsfaktor darstellt und aus diesem Grund umfassend digitalisiert wird, müssen Vorkehrungen getroffen werden, um diese Informationen zu schützen.

Durch den Einsatz technisch innovativer Lösungen in diesem Segment versucht das Unterneh-

men, die eigenen Prozesskosten zu reduzieren und eine positive Außenwirkung zu erzeugen.

Empfehlungen

- ▶ In Zusammenarbeit mit einem spezialisierten Juristen sollte die eigene Vorgehensweise in Bezug auf GOB (Grundsätze ordnungsgemäßer Buchführung) und GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen) geprüft werden.
- ▶ Das Ablagesystem sollte gewährleisten, dass auf Basis einer Verschlagwortung alle Informationen schnell gefunden werden können.
- ▶ Das Einspielen der Daten sollte vom System derart unterstützt werden, dass Arbeitsschritte, wie z. B. die Indizierung von neuen Dateien, automatisiert durchgeführt werden. Dieses Vorgehen stellt eine einheitliche und krisensichere Abwicklung sicher.
- ▶ Die Ablage der Daten sollte so konzipiert werden, dass eine langfristige Nutzung sowie eine schrittweise Erweiterung sichergestellt werden.
- ▶ Für die archivierten Daten gelten unter Umständen besondere Vorgaben des jeweiligen Kooperationsvertrages mit den Kunden. Daher sollte durch ein DRM (Digital Rights Management) gewährleistet werden, dass nur die Personen auf diese Informationen zugreifen können, die dazu berechtigt und befugt sind.

8 Gebäude und Infrastruktur



Die aktuellen Räumlichkeiten entsprechen den Markterfordernissen, die zentrale EDV ist in einem abgetrennten Bereich zu den Geschäftsräumen im gleichen Gebäude untergebracht. Die strukturellen Rahmenbedingungen werden durch den Vermieter vorgegeben.

Empfehlungen

- ▶ Sobald die Abhängigkeit des Unternehmens in Bezug auf die zentrale Serverlandschaft weiter zunimmt, sollten die vorhandenen Räumlichkeiten gezielt erweitert werden. Dies gilt vor allem für die bereitzustellenden Funktionalitäten bezüglich Ausfallsicherheit, autarker Stromversorgung, Zutrittskontrolle und Schutz vor externen Schäden durch Sturm, Wasser, Unwetter etc.
- ▶ Diesbezüglich sollte in Anbetracht der erhöhten Anforderungen eine make or buy-Entscheidung getroffen bzw. eine entsprechende Analyse vorbereitet werden. Die notwendigen Investitionen könnten unter Umständen durch eine Auslagerung (z. B. Outsourcing) erheblich reduziert werden.
- ▶ Im Bereich der Zutrittskontrolle kann nur bedingt auf die Leistungen eines zentralen Empfangs zurückgegriffen werden. Aus diesem Grund sollten strikte Vorgaben erstellt werden, wie die eigenen Büroräume zu verlassen sind. (Dies gilt gerade auch für kurze Botengänge). Denn auch kurze Abwesenheitszeiten können ein erhebliches Sicherheitsrisiko darstellen. Eine strikte Richtlinie, die von allen Mitarbeitern konsequent umgesetzt werden muss, sollte an dieser Stelle eine angemessene Lösung darstellen.
- ▶ Eine zusätzliche Sicherung der entscheidenden digitalen Daten und papierbasierten Informationen sollte durch die Anschaffung eines entsprechenden Mobiliars geschaffen werden. So könnten verschließbare Schränke für Ordner o. ä und ein Safe für die Archivierung digitaler Speichermedien verwendet werden.

9 Organisation und Personal



In Beratungsunternehmen arbeiten in der Regel viele Mitarbeiter, die mit den unterschiedlichen Facetten der Informationssicherheit vertraut sind. Eine Sensibilisierung dieser Personengruppe ist häufig nur eingeschränkt notwendig. Allerdings können sich auch bei derartigen Experten gewisse Arbeitsweisen einschleichen, die nicht den aktuellen Sicherheitsvorgaben entsprechen und dadurch eine Bedrohung für das ganze Unternehmen darstellen. Aus diesem Grund darf das Thema der Mitarbeiterschulung auch für „Profis“ nicht völlig aus den Augen gelassen werden.

Empfehlungen

- ▶ Für alle Mitarbeiter – im Innen- und Außendienst – sollte eine einheitliche Vorgehensweise für die Verwendung von Richtlinien und sonstigen Vorgaben geschaffen werden.
- ▶ Eine Plattform, auf der alle Richtlinien, Dokumentationen etc. abgespeichert werden, sollte eingerichtet werden. Diese sollte neben einer Versionierung weitere Funktionalitäten enthalten, die eine Workflow-Unterstützung ermöglichen und sicherstellen, dass aktuelle Informationen von allen Mitarbeitern, die diese betrifft, zur Kenntnis genommen werden.
- ▶ Die gestellten Vorgaben sollten regelmäßig unter Beachtung des Datenschutzes kontrolliert werden, um deren Nachhaltigkeit und Aktualität sicherzustellen.
- ▶ Diese dazu notwendigen Aufgaben sollten schriftlich an den verantwortlichen Mitarbeiter delegiert werden, der im Jahreszyklus eine Zielerreichung mit seinem Vorgesetzten abspricht, um das Arbeitspensum zu fixieren.
- ▶ Es ist zu prüfen, inwieweit ein Datenschutzbeauftragter nach Vorgaben des Bundesda-

tenschutzgesetzes (BDSG) benannt werden muss. Gerade weil der Bereich des Datenschutzes in der Öffentlichkeit einen immer höheren Stellenwert einnimmt, sollten frühzeitig entsprechende Schritte eingeleitet werden.

10 Fazit: Strategische Aufgaben für die künftige Ausrichtung

Insbesondere in der Branche der Unternehmensberatungen müssen die einzelnen Know-how-Träger im Unternehmen gewissenhaft darauf achten, dass Sie auf Kundenfragen unverzüglich und seriös reagieren. Diese, scheinbar grundsätzlichen Anforderungen, bedingen ein hohes Maß an organisatorischen und technischen Maßnahmen. In jedem Fall müssen die Verantwortungsträger im Unternehmen dafür Sorge tragen, dass eine schnelle Reaktionszeit auf Basis einer sicheren und ausfallarmen Technologie aufgebaut wird. Insbesondere im Bereich des Consultings herrscht für mittelständische Unternehmen ein intensiver Konkurrenzkampf. Es sollte zwingend im täglichen Geschäftsleben gewissenhaft darauf geachtet werden, dass nicht aufgrund technischen Versagens oder Fehlverhaltens der Mitarbeiter Kunden falsch beraten werden oder der Kundenkontakt leichtfertig verspielt wird.

Empfehlungen

- ▶ Um dem organischen Wachstum des Unternehmens Rechnung zu tragen, empfiehlt es sich, die vorhandenen Prozessdokumentationen so zu erweitern, dass sich neue Mitarbeiter schnell und fehlerarm in die vorhandenen Strukturen einfinden können.
- ▶ Alle Daten sollten auf Basis einer verbindlichen Vertriebsvereinbarung mindestens mittelfristig einer zentralen Speicherung zugeführt werden, um deren stringente Sicherung

zu gewährleisten (Backup) und diese Informationen allen Mitarbeitern zugänglich zu machen (evtl. mit einer Kopplung an ein CRM-System).

- ▶ Gerade weil bei der Kooperation mit Unternehmen vermehrt auf extern vorhandene, sensible Daten zugegriffen wird, sollte eine strikte Datenschutzrichtlinie verabschiedet werden, um sicherzustellen, dass nicht durch Fehlverhalten der Mitarbeiter Kooperationsverträge in ihrer Gültigkeit verletzt werden bzw. die Reputation des Unternehmens Schaden erleidet.
- ▶ Für den Beratungsbereich werden für kleine und mittelständische Unternehmen enorme Wachstumspotentiale prognostiziert. Es kann daher davon ausgegangen werden, dass sich mittelfristig die Personalsituation positiv verändert wird. Um dieser Entwicklung Rechnung zu tragen, sollte ein Vorgehensleitfaden erstellt werden, der darauf abzielt, neuen Mitarbeitern die Einarbeitung in die Regelungen und Prozesse des Unternehmens zu erleichtern.
- ▶ Derartige Dokumente bzw. Dokumentationen sollten so aufgebaut, abgelegt und weitergeführt werden, dass in jedem Fall sichergestellt wird, dass eine dauerhafte Aktualität erhalten bleibt.
- ▶ 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

Andreas Gabriel
m/e/c/k
Sicherheit im Internet

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“)

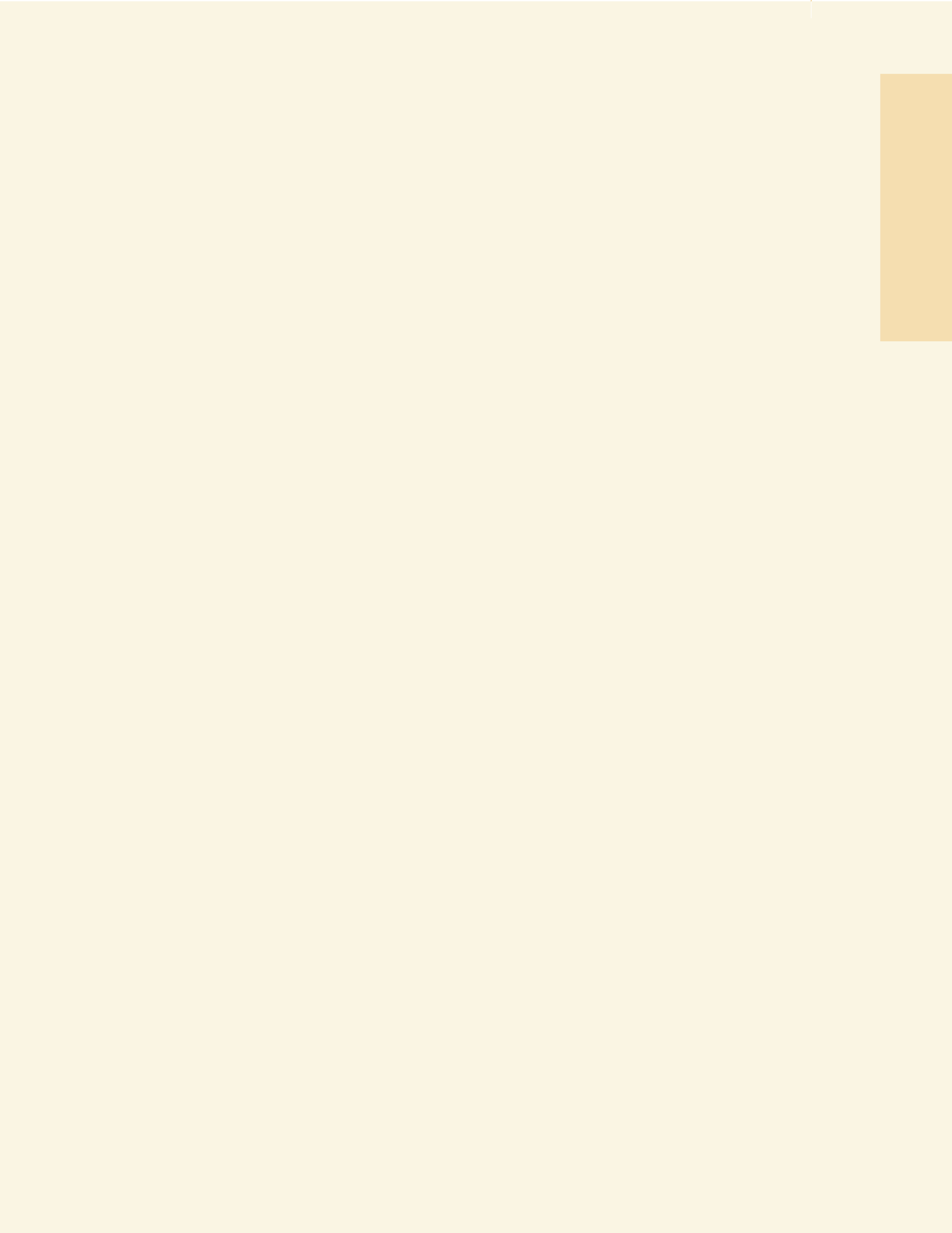
Online-Portal des Netzwerks Elektronischer Geschäftsverkehr; kostenfrei.

<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 MECK Würzburg im Rahmen des Begleitprojektes „Sichere E-Geschäftsprozesse in KMU und Handwerk“ als Teil der BMWi-Förderinitiative „Netzwerk Elektronischer Geschäftsverkehr“ herausgegeben.