



Gefördert durch das
Bundesministerium
für Wirtschaft
und Technologie



Netzwerk Elektronischer
Geschäftsverkehr



Handlungsanleitung für die Praxis

**Sichere Geschäftsprozesse:
Umsetzung im Unternehmen –
Branchenbeispiel Öffentliche Verwaltung**

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

Februar 2008

- 1 Vorwort**
- 2 Ausgangssituation**
- 3 Untersuchungsmodell**
- 4 Datenbestände**
- 5 Computer und Anwendungen**
 - 5.1 Server
 - 5.2 PCs
- 6 Netzanbindungen**
 - 6.1 Extranet
 - 6.2 Internet
- 7 Weitere Komponenten**
 - 7.1 Mobile Geräte
 - 7.2 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 Sicherheitsanalyse zeigen beispielhaft die Relevanz des Themas in der Öffentlichen Verwaltung. Für die individuelle Bewertung der Informationssicherheit in einer konkreten Einrichtung müssen natürlich die dortigen speziellen Rahmenbedingungen mit berücksichtigt werden.

2 Ausgangssituation



Die begutachtete Institution der Öffentlichen Verwaltung liegt in Nordbayern mit einer guten Verkehrsanbindung. Die

Region verfügt über insgesamt ca. 88.000 Einwohner und eine Fläche von knapp 1.000 km². Es sind sowohl touristische als auch wirtschaftliche Schwerpunkte zu finden, so dass von einer ausgewogenen Infrastruktur gesprochen werden kann. Die Kommunalverwaltung verfügt über ca. 300 Mitarbeiter, die an mehreren Standorten angesiedelt sind. Insgesamt finden mehr als 100 Fachverfahren im Rahmen der täglichen Arbeit Anwendung, die teilweise auf Basis des Bundes-, Landesrechts oder durch kommunale Bestimmungen fundiert sind. Die eingehende Analyse der Institution zeigte die folgenden **Gefahrenpotenziale** auf, denen bereits durch gezielte (Gegen-)Maßnahmen entgegengewirkt werden konnte:

- ▶ Die „Dienstanweisung für den Einsatz von informationstechnologischen Systemen und elektronischen Kommunikationseinrichtungen“ war nicht umfassend ausgestaltet.
- ▶ Ein durchgängiges Schulungskonzept für alle Mitarbeiter fehlte.
- ▶ Zwingend notwendig erscheint zudem eine Verteilung der EDV-Systeme, um eine Ausfallsicherheit zu gewährleisten und um im Notfall den täglichen Betrieb aufrecht zu erhalten. Eine krisensichere IT-Anbindung ist z. B. auch im Brandfall zu gewährleisten.

3 Untersuchungsmodell

Auf Basis eines im Vorfeld definierten Betrachtungsgegenstandes erfolgte eine eingehende Analyse der zentralen EDV-Ausstattung. Dabei wurde insbesondere darauf geachtet, dass eine krisensichere Abwicklung der täglichen Aufgaben sichergestellt werden kann. Von der grafischen Erfassung aller Prozesse wurde Abstand genommen, da schnell deutlich wurde, dass in allen Fällen auf die gleiche technische Infrastruktur zurückgegriffen wird. Daher lag der Schwerpunkt dieser Betrachtung in einer garantierten Aufrechterhaltung des Geschäftsbetriebes – unabhängig von der tatsächlichen Umsetzung durch ein einzelnes Fachverfahren.

Abbildung 1: Struktur der Ergebnisdarstellung



Die aufgearbeiteten Erkenntnisse wurden der begleiteten Institution mit konkreten Handlungsempfehlungen zur Verfügung gestellt, die Strukturierung der Ergebnisse ist Abbildung 1 zu entnehmen.

Zweifellos sind die Daten und die damit verbundenen Prozesse und Verfahren die wichtigsten Güter der Institution. Diese liegen sowohl in digitaler als auch in papiergebundener Form vor. Es gilt ein ausgewogenes Konzept zu erarbeiten, mit dem sichergestellt wird, dass zu jedem Zeitpunkt für die Daten Integrität, Vertraulichkeit und Verfügbarkeit gegeben sind.

Nach eingehender Begutachtung der einzelnen Aspekte konnte eine Risikoanalyse der vorhandenen EDV-Ausstattung durchgeführt werden, auf deren Basis weitere Maßnahmen abgeleitet und Empfehlungen erarbeitet wurden. Dieser Schritt ermöglichte allen Beteiligten einen umfassenden Einblick und führte zu signifikanten Verbesserungen. Die Ergebnisse für alle Schlüsseltechnologien, die im Rahmen dieses Projektes herausgearbeitet worden sind, sind anhand eines „Ampelschemas“ visualisiert worden (siehe Abbildung 2).

Abbildung 2: Bewertung einer Datenbank anhand deren individueller Bedrohungen

Eintrittswahrscheinlichkeit	Extrem hoch						
	Sehr hoch						3,2
	Hoch						
	Mittel		3,3				4,2
	Gering		3,1	5,4			5,5
	Sehr gering	3,5	4,1	4,5	4,3	5,3	4,4
	Unwahrscheinlich		3,4	5,1	5,2		
		Null	Niedrig	Mittel	Hoch	Sehr hoch	Extrem hoch
geschätzter Schaden							

Quelle: in Anlehnung an Kremer, Helmut und Romeike, Frank.

4 Datenbestände



Im Rahmen der aufgezeigten Fachverfahren werden die für sie relevanten Daten durchweg in einer Datenbank abgelegt. Da aufgrund juristischer Vorgaben eine zentrale Datenhaltung über alle Prozesse hinweg nicht zulässig ist, sind die Verantwortlichen dazu verpflichtet, mehrere Datenbanksysteme parallel und unabhängig voneinander zu betreiben. Die jeweiligen Mitarbeiter in den Fachbereichen arbeiten darüber hinaus mit dem Microsoft Office-Paket. Die so erstellten Daten werden auf einem zentralen Datenserver mit einem ausführlichen Rechtssystem abgelegt. Die Sicherung des Datenbestands erfolgt durch eine Spiegelung.

Neben den digitalen Daten liegen zahlreiche Informationen auf Papierbasis vor. Die entsprechenden Räumlichkeiten werden verschlossen gehalten, und der Zutritt ist ausschließlich befugten Mitarbeitern möglich.

Empfehlungen

- ▶ Eine mindestens tagesaktuelle Spiegelung der Daten würde das Ausfallrisiko enorm verringern und eine schnelle Wiederinbetriebnahme im Ernstfall ermöglichen.
- ▶ Ein Ranking auf Basis einer Bewertung der unterschiedlichen Systeme würde den EDV-Verantwortlichen sowie den (politischen) Entscheidungsträgern ein Bild darüber verschaffen, mit welchen Fachverfahren die größte Außenwirkung erzielt wird bzw. welche Relevanz die einzelnen Systeme für das tägliche Arbeiten haben.
- ▶ Eine Dokumentation, welche (Sicherungs-) Maßnahmen für diese Infrastruktur auf welche Art und Weise durchzuführen sind, fehlt und sollte daher eingeführt werden. Diese würde im Krisenfall eine schnelle Reaktionszeit sicherstellen und Arbeitsausfälle reduzieren.

5 Computer und Anwendungen

5.1 Server



Eine Citrix-Serverfarm auf Basis eines RAID-Systems bildet den Kern der verwendeten Serverlandschaft. Es wurden die gängigen Sicherheitsvorkehrungen (Virens Scanner, Firewall etc.) installiert und entsprechend konfiguriert. Über diese Hardware werden alle Dienste, wie z. B. Druck oder E-Mail, abgewickelt, und es besteht ein ausreichend dimensionierter Servicevertrag.

Empfehlungen

- ▶ Eine detaillierte Dokumentation sollte dringend erstellt werden. In dieser sollten die Kontaktpersonen hinterlegt werden, die im Servicefall zu kontaktieren sind. Darüber hinaus sollte festgehalten werden, welche Leistungen von Dienstleistern eingefordert werden können, ohne die vertraglichen Regelungen zu überstrapazieren.
- ▶ Darüber hinaus sollten die Maßnahmen, die regelmäßig von den internen Mitarbeitern getätigt werden, festgehalten werden, damit im Schadensfall ein möglicher Fehler schneller gefunden werden kann.
- ▶ Die Einweisungen und Schulungen für die Mitarbeiter der EDV-Abteilung sollten regelmäßig wiederholt und detailliert festgehalten werden.

5.2 PCs



Es kommt im gesamten Einflussbereich eine Thin Client-Architektur auf Basis von Microsoft-Betriebssystemen zum Einsatz. Ausgewählten Mitarbeitern steht die Möglichkeit offen, sich vom eigenen Rechner zu Hause in die jeweiligen Verfahren einzuwählen. Dieser Zugriff erfolgt verschlüsselt durch einen VPN-Tunnel. Die Arbeitsumgebung am heimischen PC basiert ebenfalls auf einer Thin Client-Architektur.

Empfehlungen

- ▶ Die Mitarbeiter sollten die genannte Dienst-anweisung verinnerlichen. Die darin geforderten Maßnahmen und Verhaltensweisen sollten in Gänze befolgt werden. Dafür empfiehlt es sich, regelmäßige Schulungen bzw. Belehrungen durchzuführen.
- ▶ Es sollte kritisch geprüft werden, inwieweit USB-Schnittstellen sowie CD- und Diskettenlaufwerke allen Mitarbeitern zur Verfügung stehen müssen.
- ▶ Beim Einsatz von Laptops sollten die besonderen Regelungen im Bereich der Verschlüsselung und der Aktualisierung (Virens Scanner/Betriebssystem) erfüllt werden. Für mobile Rechner sollte ein wirksamer Netzwerkschutz sichergestellt werden.

6 Netzanbindungen



6.1 Extranet

Der grundlegende Unterschied zwischen einer Kommune und einem Wirtschaftsbetrieb liegt in der Netzanbindung. Neben einem häufig vorhandenen „regulären“ Internetanschluss verfügen öffentliche Einrichtungen über eine Art Extranet – das Behördennetz. Dieses Kommunikationsmedium stellt eine sichere Datenübertragung zwischen öffentlichen Einrichtungen sicher. Innerhalb zahlreicher Prozesse erfolgt der Datenaustausch jedoch auch über das World Wide Web (WWW), insbesondere dann, wenn der Bürger als Endkunde adressiert wird.

Diese Fälle bedürfen einer gewissenhaften Analyse, da sowohl datenschutzrechtliche als auch sicherheitsrelevante Aspekte zu beleuchten sind.

Empfehlungen

- ▶ Es sollte eine Aufnahme klarer Bestimmungen in die jeweiligen Stellenbeschreibungen erfolgen, welche digitalen Daten in welcher

Art und Weise über das „öffentliche“ Internet versendet werden dürfen.

- ▶ Die schrittweise Implementierung einer Kryptographie- und Signatur-Software für die einzelnen PC-Arbeitsplätze wird empfohlen.

6.2 Internet



Alle PC-Arbeitsplätze verfügen über mindestens einen Netzanschluss – Behördennetz und/oder reguläres WWW. In den meisten Fällen sind beide Netztypen zugänglich. Eine funkbasierte Vernetzung ist nicht installiert.

Empfehlungen

- ▶ Für die Schlüsselbereiche der hauseigenen Netze sollten tragfähige Notfallpläne erarbeitet werden, um eine kurze Wiederanlaufphase zu gewährleisten.
- ▶ Von der künftigen Installation eines WLAN-Netzwerks wird abgeraten, da die notwendigen Sicherungsmaßnahmen einen enormen Aufwand mit sich bringen und so die möglichen Vorteile amortisieren würden.
- ▶ Durch die Bereitstellung von Heimarbeitsplätzen würde die flexible Anbindung aller Mitarbeiter unterstützt. Dabei sollte bedacht werden, dass die Konfiguration derart sicher gestaltet sein muss, dass Zugriffe über einen korrumpierten Heimarbeitsplatz eines Mitarbeiters ausgeschlossen werden können.
- ▶ Um der aktuellen Entwicklung der deutschen Rechtsprechung Rechnung zu tragen, sollten die Verantwortlichen bei der Auswahl eines Netzwerkanalyseprogramms gewissenhaft darauf achten, dass § 202a bzw. § 303b StGB nicht verletzt wird, da einige Software-Tools nicht mehr ohne weiteres verwendet werden dürfen.

7 Weitere Komponenten



7.1 Mobile Geräte

In dieser Betrachtung sind sowohl PDAs o. ä. als auch Laptops zu berücksichtigen, da auf beiden Gerätearten sensible Daten gespeichert sein können, die aufgrund der geringen Maße dieser Geräte einer erhöhten Gefahr ausgesetzt sind.

Empfehlungen

- ▶ Alle Daten, die auf PDAs o. ä. gespeichert werden, sollten verschlüsselt werden, um einen unberechtigten Zugriff auszuschließen.
- ▶ Eine Benutzerregelung mit eindeutig definierten Rollen sollte bereits vor der Ausgabe in Form eines übergreifenden Rahmenwerkes implementiert werden.
- ▶ Für alle Dienstgeräte sollte gelten, dass ungenutzte Schnittstellen, wie z. B. Bluetooth, von vorne herein deaktiviert sind. Nur so kann einem Missbrauch vorgebeugt werden.
- ▶ Die kleinen, tragbaren Geräte sollten ebenfalls mit speziellen Schutzprogrammen ausgestattet werden (Virenschutz etc.).
- ▶ Wie bereits ausgeführt, sollten tragbare Computer mit ausgewählten Sicherheitsprogrammen ausgestattet werden, da sich Mitarbeiter mit Laptops häufig in fremde Netzwerke einwählen. Nur so kann ein wirksamer Netzwerkschutz gewährleistet werden.
- ▶ Sobald sich diese Mitarbeiter wieder im eigenen Netzwerk anmelden, sollte sichergestellt werden, dass vor einem Programmzugriff ein Update aller sicherheitsrelevanten Programme stattfindet. Dadurch kann verhindert werden, dass schädliche Programme die vorhandenen Schutzmechanismen unterlaufen.

- ▶ Da auf den Laptops häufig sensible Daten abgespeichert werden, sollte mit einer Festplattenverschlüsselung sichergestellt werden, dass bei Verlust oder Diebstahl ein fremder Zugriff ausgeschlossen werden kann.
- ▶ Ein derartiges kryptographisches System sollte auch für andere Speichermedien wie USB-Sticks, CDs etc. angewendet werden.

7.2 Archiv



Da bei mehr als 100 Fachverfahren Unmengen an digitalen und papierbasierten Daten erzeugt werden, muss ein übergreifendes und integriertes Anlagensystem implementiert werden. Da mit der Microsoft Office-Produktfamilie zusätzliche Dokumente generiert werden und zahlreiche Bilddaten dazu kommen, muss eine umfassende Lösung eine redundanzfreie und sichere Speicherung gewährleisten.

Empfehlungen

- ▶ Einführung eines Dokumenten-Management-Systems (DMS), auf das alle Mitarbeiter zugreifen können. Um den Vorgaben des Datenschutzes zu entsprechen, sollte ein eindeutiges Rechtesystem implementiert werden.
- ▶ Im Fall einer (Langzeit-)Archivierung sollten die folgenden Aspekte in jedem Fall berücksichtigt werden:
 - Wahl geeigneter Speichermedien und eines angemessenen Aufbewahrungsorts,
 - Verschlüsselung der Inhalte,
 - Sicherstellung eines einheitlichen und zukunftssicheren Ablageformats.
- ▶ Für die papierbasierte Archivierung sollten folgende Fragen beantwortet werden:
 - Welche Personen dürfen die jeweiligen Räumlichkeiten betreten?

Inwieweit kann durch ein spezielles Verfahren festgehalten werden, wer den jeweiligen Raum betreten hat?

Wo ist verankert, welche Mitarbeiter überhaupt dazu befugt sind, sich Zutritt zu den Archivräumen zu verschaffen?

Wie läuft der Genehmigungsprozess für neue Zutrittsgenehmigungen ab?

Werden Zugriffsrechte beim Ausscheiden eines Mitarbeiters auch fristgerecht und endgültig entzogen?

- ▶ Durch eine einheitliche Regelung sollte eindeutig festgelegt werden, wie jeder einzelne Mitarbeiter mit den Dokumenten auf seinem Arbeitsplatz umgehen muss, damit keine datenschutz- und sicherheitsrelevanten Vorgaben verletzt werden.

8 Gebäude und Infrastruktur



Das Gebäude befindet sich in einem sehr guten Zustand. Der zentrale Zugang ist mit einem Empfang ausgestattet. Trotz des Empfangs am Haupteingang bestand allerdings die Möglichkeit, das Gebäude ohne Angabe persönlicher Daten zu betreten. Der EDV-Bereich verfügt über einen eigenen Zutrittsmechanismus, so dass der zentrale Server-Raum nicht ohne weiteres betreten werden kann. Der Server-Raum verfügt aktuell über eine gute Ausstattung. Ein großer Schadensfall könnte jedoch zu einem irreparablen Datenverlust und einem vollkommenen Stillstand der Prozesse führen. Um dem entgegenzuwirken, verfügen alle Räume über entsprechende Vorkehrungen zur Branderkennung.

Empfehlungen

- ▶ Um das Risiko eines Missbrauchs zu reduzieren, sollten die Bereiche, in denen kein Publikumsverkehr vorhanden ist, verschlossen sein.

- ▶ Es wird dringend die Einrichtung eines zweiten Server-Raums in einem anderen Brandabschnitt empfohlen, der im Notfall als Backup-System genutzt werden kann.
- ▶ Für ausgewählte Hardware-Komponenten sollte gewissenhaft abgewogen werden, inwieweit die Bevorratung eines Ersatzgerätes eine schnelle Reaktion im Schadensfall ermöglicht. Es gilt hier, zwischen einem Ausfall im EDV-Bereich sowie der nachgelagerten Prozesse und einer Investition in zusätzliche EDV-Hardware abzuwägen.
- ▶ Es wird empfohlen, durch regelmäßige Brandschutzübungen einen Störfall im EDV-Bereich nachzustellen. Dabei sollte die Zusammenarbeit mit den Löschkraften vor Ort und vor allem deren Reaktionszeiten nach einem Alarm geprüft werden.

9 Organisation und Personal



Im Umfeld der öffentlichen Einrichtung arbeiten zahlreiche Mitarbeiter – auch in angeschlossenen Institutionen oder Eigenbetrieben.

Empfehlungen

- ▶ Für alle Mitarbeiter, die auf die EDV-Infrastruktur zugreifen, sollten einheitliche Regelungen geschaffen werden.
- ▶ Eine (EDV-)Sicherheitsrichtlinie sollte verabschiedet werden, deren Erhalt jeder Mitarbeiter schriftlich bestätigen sollte. Mit dieser Signatur würde er sich dazu verpflichten, die Regelungen in seiner täglichen Arbeit anzuwenden und zu berücksichtigen.
- ▶ Die Kernprozesse der Institution sollten schriftlich erfasst und vor allem mit einem Anlaufplan dokumentiert werden. Nur so kann eine einheitliche Vorgehensweise sichergestellt werden.

- ▶ Durch die Erstellung von (Prozess-)Dokumentationen könnte in allen Bereichen dieser Institution eine präzisere und qualitativ hochwertigere Durchführung aller (Fach-)Verfahren erzielt werden.
- ▶ Bei der Erstellung papierbasierter Regelungen sollte ein Mechanismus etabliert werden, mit dem eine Aktualisierung und Verbreitung der Dokumente an alle Mitarbeiter sichergestellt werden kann. Dies könnte z. B. mit einem speziell konfigurierten Intranet sowie einer E-Mail-Benachrichtigung erfolgen, die verbindlich zu bestätigen ist.
- ▶ Alle Mitarbeiter, die mit EDV am Arbeitsplatz in Berührung kommen, sollten regelmäßig durch Schulungsmaßnahmen oder Workshops für aktuelle Probleme sensibilisiert werden. Um den Aufwand dieser Vorgabe in einem überschaubaren Rahmen zu halten, könnte dieses Thema zu Beginn anderer Veranstaltungen, wie z. B. einer Betriebsversammlung, auf die Tagesordnung genommen werden. In jedem Fall sollte gewissenhaft protokolliert werden, welche Mitarbeiter welche Schulungsveranstaltungen besucht haben.

10 Fazit: Strategische Aufgaben für die künftige Ausrichtung

Auch die Öffentliche Verwaltung ist mittlerweile zu einem Dienstleistungsunternehmen geworden und konkurriert mit den jeweiligen Nachbarregionen um Einwohner und Gewerbetreibende. Die Ausrichtung der eigenen Prozesse an den Wünschen der „Kunden“ ist dadurch vermehrt in den Vordergrund getreten und bestimmt das Handeln der Verantwortungsträger. Dieses hohe Ziel kann durch den stringenten Einsatz von EDV gezielt unterstützt und voran-

getrieben werden. Die zukünftige Entwicklung und insbesondere die flächendeckende Verbreitung der digitalen Signatur wird zweifellos die Abwicklung von Verwaltungsprozessen dramatisch verändern. Die digitale Abwicklung von Verwaltungsaufgaben birgt ein sehr hohes Einsparpotenzial in sich. Obwohl der Begriff „E-Government“ in den vergangenen Jahren scheinbar etwas von seiner Bedeutung verloren hat, sind die Errungenschaften in diesem Bereich unbestritten. Die PC-basierte Abwicklung von Verfahren in Ämtern und Behörden mit einer noch intensiveren Vernetzung zwischen den einzelnen Institutionen wird in den kommenden Jahren weiter zunehmen.

Empfehlungen

- ▶ Um abschätzen zu können, welche Fachverfahren die höchste Relevanz besitzen, sollte eine umfassende Prozessanalyse durchgeführt werden, die von sicherheitstechnischen Rahmenbedingungen flankiert wird.
- ▶ Anhand eines jährlich durchzuführenden Sicherheitstests vor Ort durch einen neutralen Fachmann könnte die Qualität der eigenen Sicherheitsmaßnahmen kontrolliert werden.
- ▶ Gerade kleinere Kommunen sollten sich dem Trend der digitalen Signatur nicht verschließen, da sie sonst einen nicht mehr einzuholenden Rückstand beklagen werden.
- ▶ Dieser Entwicklung sollte die Öffentliche Verwaltung Rechnung tragen. Dazu sollten die eigenen Strukturen und Vorgaben kritisch hinterfragt 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, 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.

Schneider, Bruce: Secrets and Lies, IT-Sicherheit in einer vernetzten Welt, 2004.

Witt, Bernhard Carsten: IT-Sicherheit kompakt und verständlich. Eine praxisorientierte Einführung, 2006.

12.4 Websites

<http://www.bsi.de>

Website des Bundesamts für Sicherheit in der Informationstechnik; kostenfrei.

<http://www.competence-site.de/it-sicherheit>

Online-Wissensportal der NetSkill AG, Düsseldorf; kostenfrei.

http://www.computerwoche.de/knowledge_center/it_security

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“)

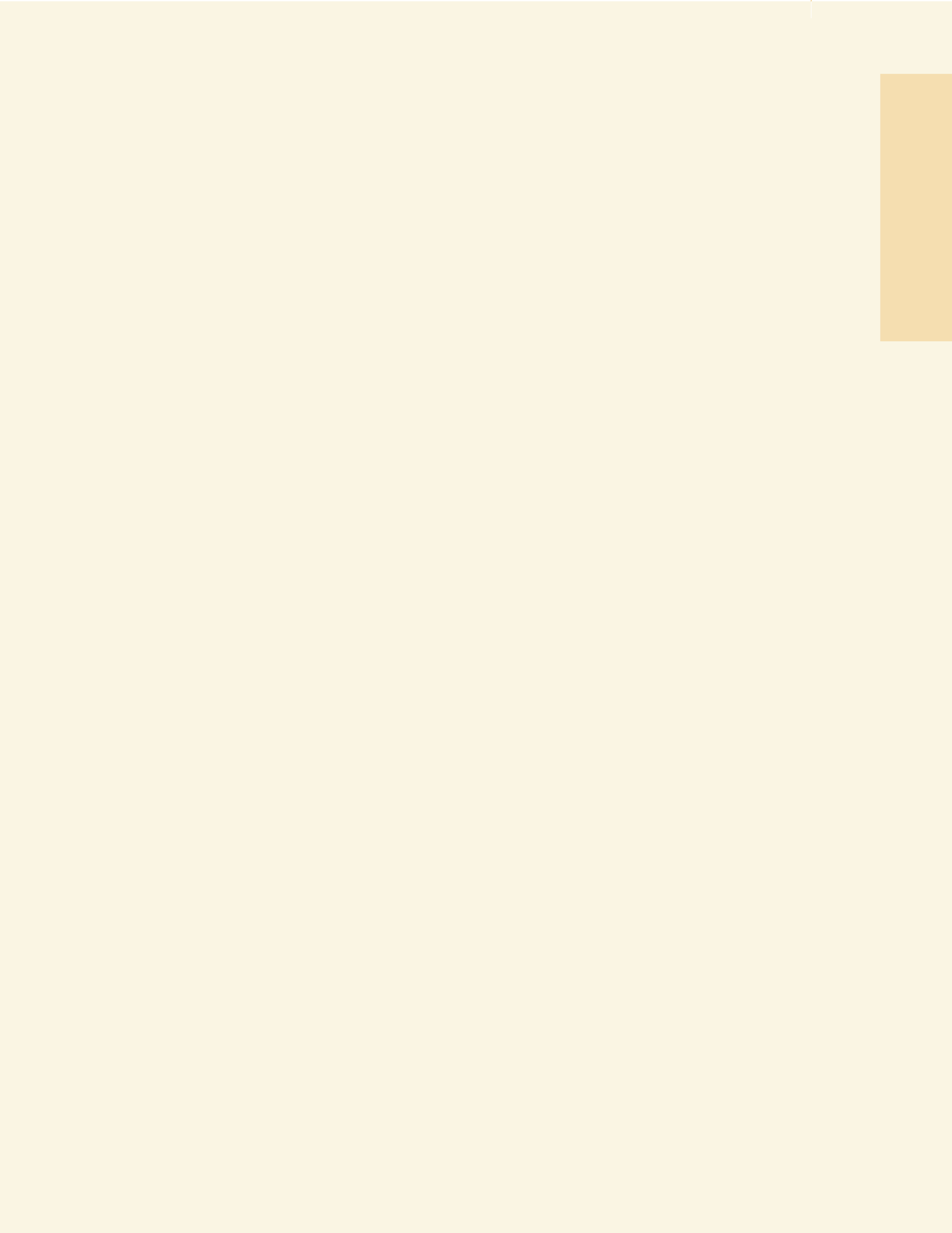
Online-Portal des Netzwerks Elektronischer Geschäftsverkehr; kostenfrei.

<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

m/e/c/k
Sicherheit im Internet

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.