KPMG

Bericht

Prüfung der Archivierungslösung Inet-Archiv

deCODEtron Archiv-Service GmbH Steinbach/Taunus

Juni 2008

KPMG Deutsche Treuhand-Gesellschaft
Aktiengesellschaft Wirtschaftsprüfungsgesellschaft

Inhaltsverzeichnis

Anlagenverzeichnis

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
AO	Abgabenordung
ASCII	American Standard Code for Information Interchange
BDSG	Bundesdatenschutzgesetz
BMF	Bundesministerium der Finanzen
EBCDIC	Extended Binary Coded Decimals Interchange Code
FAIT	Fachausschuss für Informationstechnologie des IDW
FTP	File Transfer Protocol
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoB	Grundsätze ordnungsmäßiger Buchführung
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
HGB	Handelsgesetzbuch
http	Hypertext Transfer Protocol
https	http over SSL
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V.
IKS	Internes Kontrollsystem
MD5	Message-Digest Algorithm 5
OTDS	Originäre Tagesdatensicherung
PDF	Portable Document Format
PS	Prüfungsstandard des IDW

PZN	Pharmazentralnummer
RAID	Redundant Array of Inexpensive/Independent Disks
RS	Stellungnahme zur Rechnungslegung des IDW
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
UTF-EBCDIC	Unicode Transformation Format - EBCDIC
VPN	Virtual Private Network
ZIP	Dateiformat für die (komprimierte) Archivierung von Dateien

1 Auftrag und Auftragsdurchführung

1.1 Prüfungsauftrag

Mit Schreiben vom 15. Februar 2007 wurden wir von der

deCODEtron Archiv-Service GmbH, Steinbach/Taunus,
--im Folgenden „deCODEtron GmbH“ oder „Gesellschaft“ genannt--

mit der Prüfung der Lösung für die Übermittlung und (optionale) Archivierung von rechnungslegungsrelevanten Dokumenten in elektronischer Form von der deCODEtron GmbH

deCODEtron Inet-Archiv
--im Folgenden kurz „Archivlösung“ oder „Anwendung“ genannt--

beauftragt.

Ziel der Prüfung war es festzustellen, ob die Software bei sachgerechtem Einsatz eine Übermittlung und Speicherung von rechnungslegungsrelevanten Dokumenten in elektronischer Form im Einklang mit den Grundsätzen ordnungsmäßiger Buchführung (GoB) gewährleistet und damit wesentliche Voraussetzungen für eine spätere Einbindung dieser Dokumente in elektronische Rechnungen erfüllt sind.

Prüfungsgegenstand war die in Abschnitt 3.1.3 detailliert beschriebene Konfiguration einer von der deCODEtron GmbH bereitgestellten Anwendung.

1.2 Maßstab zur Beurteilung der Ordnungsmäßigkeit

Als Maßstab zur Beurteilung der Ordnungsmäßigkeit wurden

- die gesetzlichen Vorschriften des Handels- und Steuerrechts (§§ 238 ff. HGB sowie §§ 140-148 AO),
- die Grundsätze ordnungsmäßiger Buchführung (GoB),
- das BMF-Schreiben vom 7. November 1995 zu den „Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme“ (GoBS),

- das BMF-Schreiben vom 16. Juli 2001 zu den „Grundsätzen des Datenzugriffs und der Prüfbarkeit digitaler Unterlagen“ (GDPdU),

- die Stellungnahme zur Rechnungslegung des Fachausschusses für Informationstechnologie (FAIT) des Instituts der Wirtschaftsprüfer in Deutschland e.V. (IDW) „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ (IDW RS FAIT 1),

- die Stellungnahme zur Rechnungslegung des FAIT des IDW „Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren“ (IDW RS FAIT 3),

- der IDW-Prüfungsstandard „Abschlussprüfung bei Einsatz von Informationstechnologie“ (IDW PS 330),

- der IDW-Prüfungsstandard „Erteilung und Verwendung von Softwarebescheinigungen“ (IDW PS 880) sowie

- die Vorschriften des Bundesdatenschutzgesetzes (BDSG)

zu Grunde gelegt.

1.3 Art und Umfang der Prüfungshandlungen

Unsere Arbeiten führten wir anhand der uns vorgelegten Dokumentation, durch Gespräche mit Mitarbeitern der deCODEtron GmbH sowie durch systemgestützte Prüfungshandlungen durch.

Wir haben die Prüfung im Zeitraum vom 10. April 2007 bis 30. Juni 2008 in unseren Geschäftsräumen und in den Räumen der deCODEtron GmbH in der Siemensstraße 17, Steinbach/ Taunus, durchgeführt. Art und Umfang unserer Prüfungshandlungen haben wir in unseren Arbeitspapieren festgehalten.

Alle zur Prüfung erforderlichen Unterlagen wurden uns zur Verfügung gestellt. Die gewünschten Auskünfte und Erläuterungen wurden uns von den Mitarbeitern der Gesellschaft erteilt. Unsere Feststellungen und Beurteilungen zum Sachverhalt beruhen auf dem zum Prüfungszeitpunkt vorgefundenen Stand des Systems.

Die Geschäftsführung hat uns die Vollständigkeit der erteilten Aufklärungen und Nachweise, der zur Verfügung gestellten Verfahrensdokumentation sowie der Change Requests schriftlich bestätigt.

2 Zusammengefasstes Prüfungsergebnis und Softwarebescheinigung

Wir haben die Lösung für die Übermittlung und (optionale) Archivierung von rechnungslegungsrelevanten Dokumenten in elektronischer Form von der deCODEtron GmbH gemäß den vorstehenden Bedingungen geprüft und die folgende Bescheinigung erteilt:

Softwarebescheinigung

An die deCODEtron Archiv-Service GmbH, Steinbach/Taunus

Sie haben uns den Auftrag erteilt, die Funktionsfähigkeit der deCODEtron-Archivlösung zu prüfen. Die Verantwortung für die Funktionsfähigkeit dieses Systems liegt bei den gesetzlichen Vertretern der deCODEtron GmbH. Unsere Aufgabe ist es, auf der Grundlage der von uns durchgeführten Prüfung eine Beurteilung darüber abzugeben, ob die deCODEtron-Archivlösung bei sachgerechter Anwendung eine den deutschen handels- und steuerrechtlichen Ordnungsmäßigkeitskriterien entsprechende elektronische Übermittlung und (optionale) Archivierung von rechnungslegungsrelevanten Dokumenten in elektronischer Form ermöglicht.

Wir haben unsere Prüfung der Software nach dem vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) veröffentlichten Prüfungsstandard PS 880 „Erteilung und Verwendung von Softwarebescheinigungen“ vorgenommen. Danach ist die Prüfung von Softwareprodukten so zu planen und durchzuführen, dass nach Bestandsaufnahme des Prüfungsobjekts und der Testumgebung die notwendigen Verarbeitungsfunktionen identifiziert und die programmierten Verarbeitungsregeln mit Hilfe der Testfallmethode geprüft werden. Dazu sind sowohl eigene als auch Testfälle des Herstellers zu Grunde zu legen. Des Weiteren sind die Softwaresicherheit und die Dokumentation zu beurteilen. Wir sind der Auffassung, dass unsere Prüfung eine hinreichend sichere Grundlage für unsere Beurteilung bildet.

Auf Grund der von uns durchgeführten Prüfung, über die wir mit Datum vom 30. Juni 2008 gesondert Bericht erstattet haben, kommen wir zu dem Ergebnis, dass die Archivlösung der deCODEtron GmbH --unter Berücksichtigung der nachfolgend aufgeführten Feststellung-- bei sachgerechter Anwendung eine den deutschen Grundsätzen ordnungsmäßiger Buchführung entsprechende Übermittlung und (optionale) Archivierung von rechnungslegungsrelevanten Dokumenten in elektronischer Form ermöglicht.

Klarstellend weisen wir darauf hin, dass die sachgerechte Anwendung insbesondere die Umsetzung der folgenden Maßnahmen beinhalten sollte:

- Um die Wirksamkeit der Kontrollen zur Wahrung der Unveränderlichkeit nachzuweisen, sind seitens der deCODEtron GmbH regelmäßige Prüfungen der intakten Verkettung der Sicherungsmedien durchzuführen und zu dokumentieren.

- Wie generell für solche Systeme üblich, ist durch infrastrukturelle Maßnahmen sicherzustellen, dass nur berechtigte Personen einen kontrollierten Zugang zu der Lösung haben (closed shop), und für eine sachgerechte Vergabe von Benutzer- und Administratorenberechtigungen zu sorgen. Da die Anwendung aus dem Internet erreichbar ist, sollte durch entsprechende Prozesse sichergestellt werden, dass die Sicherheit fortlaufend überprüft und gegebenenfalls angepasst wird, um gegen Bedrohungen aus dem Internet angemessen vorbereitet zu sein.

Im Übrigen verweisen wir auf die Prüfungsergebnisse im Einzelnen.

Dem Auftrag, in dessen Erfüllung wir vorstehend benannte Leistungen für die deCODEtron GMBH erbracht haben, lag eine Haftungsbeschränkung --auch Dritten gegenüber-- in Höhe von EUR 5 Mio zu Grunde. Durch Kenntnisnahme und Nutzung der in dieser Bescheinigung enthaltenen Informationen bestätigt jeder Empfänger, diese Regelungen zur Kenntnis genommen zu haben, und erkennt deren Geltung im Verhältnis zu uns an.

Berlin, den 30. Juni 2008

KPMG Deutsche Treuhand-Gesellschaft
Aktiengesellschaft
Wirtschaftsprüfungsgesellschaft

Köppe	Hoffmann
Wirtschaftsprüfer	Wirtschaftsprüfer

3 Prüfungsergebnisse im Einzelnen

3.1 Beschreibung des Prüfungsgegenstands

3.1.1 Darstellung der grundlegenden Funktionalität

Die deCODEtron-Archivlösung ist eine kombinierte Hard- und Softwarelösung zur Verwaltung und Archivierung elektronischer Dokumente, die von der deCODEtron GmbH entwickelt wurde und derzeit insbesondere im Pharmagroßhandel und bei Apotheken zum Einsatz kommt.

Die in dieser Lösung archivierten rechnungsrelevanten elektronischen Dokumente (im Folgenden Daten genannt) können mit Indexmerkmalen versehen werden, um über verschiedene Suchkriterien gezielt auf den Datenbestand zugreifen zu können. Eine weitere wesentliche Funktion des Systems ist die Möglichkeit, über ein Web-Portal auf die Daten zuzugreifen sowie die dauerhafte und vor Veränderungen geschützte Archivierung.

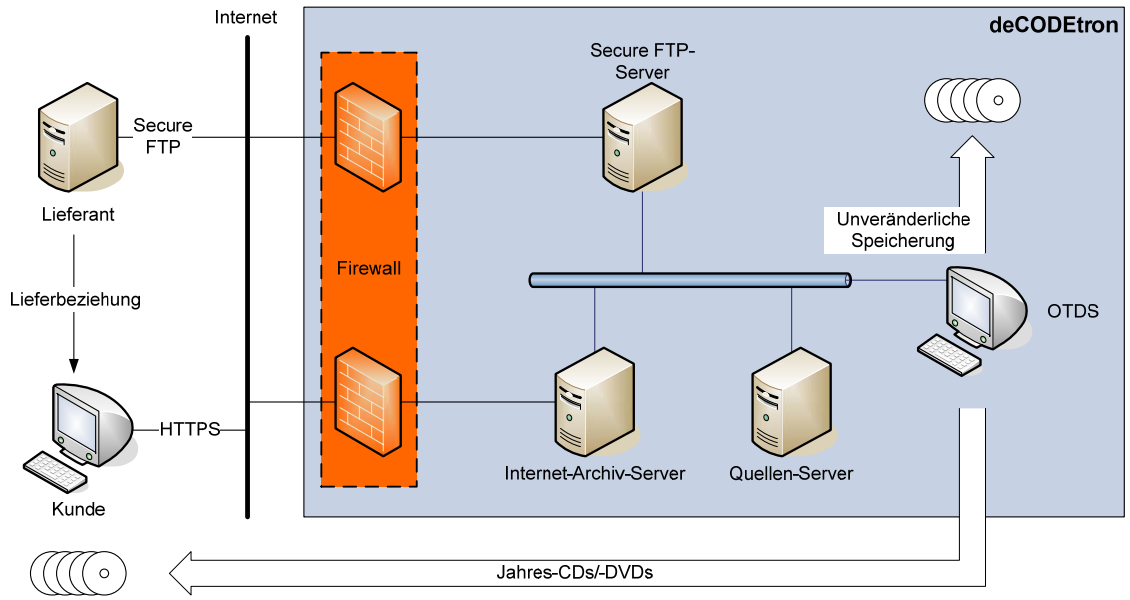
Die Lösung wird von der deCODEtron GmbH eingesetzt, um Daten zu empfangen, aufzubereiten und den Adressaten auf elektronischem Wege zur Verfügung zu stellen. Dem zu Grunde liegen i. d. R. Lieferbeziehungen zwischen den Kunden der deCODEtron GmbH, die die Daten liefern (im Folgenden Lieferanten genannt), und den Adressaten, denen die Dokumente im Auftrag der Lieferanten zur Verfügung gestellt werden (im Folgenden Kunden genannt). Die Kunden haben über individualisierte Zugänge Zugriff auf diese Dokumente und können diese abrufen und bei sich speichern.

Da die Daten für die Kunden in der Regel zu den für sie aufbewahrungspflichtigen Unterlagen gehören, bietet die deCODEtron GmbH den Kunden als optionale Zusatzleistung an, diese Aufbewahrungspflicht im Auftrag der Kunden zu übernehmen. Bei Inanspruchnahme dieser Zusatzleistung müssen die Kunden die Daten nicht aus dem Portal abrufen und selbst für die ordnungsmäßige Aufbewahrung sorgen, sondern können die Daten im Inet-Archiv belassen und dort jederzeit darauf zugreifen. Nach Ablauf eines Jahres werden die Daten den Kunden dann gesammelt auf optischen Medien in auswertbarer Form („Jahres-CD/DVD“) übergeben.

Die Umsetzung der Aufbewahrungspflichten und die entsprechenden Prozesse bei den Kunden waren nicht Gegenstand unserer Prüfung.

3.1.2 Darstellung der Komponenten

Die folgende Abbildung stellt den Aufbau einer minimalen Konfiguration schematisch dar:



Secure FTP-Server

Die Lieferanten übertragen ihren Druckstrom als ZIP-Datei unter Nutzung eines verschlüsselten Protokolls (Secure FTP) an die deCODEtron GmbH und legen diesen auf dem entsprechenden Server in einem für sie vorbereiteten Verzeichnis ab. Der FTP-Server wird ferner für die Protokollierung des Dateneingangs verwendet.

OTDS (Originäre Tagesdatensicherung)

Zunächst werden die übermittelten Daten auf den OTDS-Server kopiert und anhand einer Prüfsumme auf Unversehrtheit geprüft. Ist der Druckstrom unverändert, wird er anschließend auf CD/DVD archiviert. Monatlich werden die zugehörigen Dokumente zusammengefasst und am Ende des Jahres zu einer so genannten Jahres-CD/DVD zusammengefasst, die den Kunden zur Verfügung gestellt werden kann.

Quellen-Server

Nach Abschluss der Sicherung werden die Daten auf den Quellen-Server kopiert, um die Originaldruckströme zu speichern und weiterzuverarbeiten. Danach wird der FTP-Server bereinigt, da er ausschließlich für die Datenübertragung und den Dateneingang zum Einsatz kommt.

Internet-Archiv-Server (Inet-Server bzw. -Archiv)

Schließlich wird der Druckstrom vom Quellenserver auf den Inet-Server des jeweiligen Lieferanten kopiert und dort aufbereitet. Die einzelnen Schritte der Aufbereitung umfassen das Dekomprimieren der Datenströme, die Indizierung und Erstellung einer Indexdatenbank sowie die Bereitstellung im Internet. Ist die Aufbereitung der Daten abgeschlossen, können Lieferanten und Kunden im Internet unter Nutzung einer verschlüsselten Kommunikationsverbindung (https) auf ihre Daten zugreifen.

Indexdatenbank

Für den gezielten Zugriff erzeugt die deCODEtron GmbH eine Indexdatenbank auf dem jeweiligen Inet-Server, über die der Zugriff auf die Daten erfolgt. Diese Indexdatenbank wird täglich auf Basis der vorhandenen Druckströme neu erstellt. Der Druckstrom bleibt dabei unangetastet und dient lediglich als Datenquelle.

Jahres-CDs/DVDs

Am Ende eines Geschäftsjahres haben die Kunden die Möglichkeit, eine so genannte Jahres-CD bzw. -DVD zu erwerben. Darauf sind sämtliche Daten des vergangenen Geschäftsjahres enthalten. Der entsprechende Datenträger ist als autarkes Archiv konzipiert. Enthalten sind daher sowohl die eigentlichen Daten als auch Werkzeuge zum gezielten Zugriff und zur Lesbarmachung.

3.1.3 Darstellung der verwendeten Testumgebung

Für den Zeitraum der Prüfung wurde uns von der deCODEtron GmbH eine Testumgebung zur Verfügung gestellt. Die Konfiguration der Hard- und Software haben wir in Anlage 1 zusammengestellt.

3.2 Verarbeitungsfunktionen

3.2.1 Produktalternativen des Inet-Archivs

Das Inet-Archiv basiert auf dem Angebot einiger Lieferanten ihren belieferten Kunden gegenüber, papierbasierte Dokumente (z. B. Lieferscheine) durch elektronisch über die deCODEtron

GmbH zur Verfügung gestellte Daten zu ersetzen und papierbasierte Informationen nur noch in Kopie zu versenden.

Die Kunden haben dabei darüber hinaus die Wahl, die so zur Verfügung gestellten Daten im Folgenden in eigener Verantwortung aufzubewahren (Variante A) oder --als zusätzliche Dienstleistung-- für die Aufbewahrung das Inet-Archiv und die Jahres-CDs von der deCODEtron GmbH einzusetzen (Variante B).

Bei der ausschließlichen Nutzung der Daten (Variante A) besteht keinerlei vertragliche Beziehung zwischen den Kunden und der deCODEtron GmbH. Die Aufgabe von der deCODEtron GmbH besteht auskunftsgemäß in diesem Fall ausschließlich darin, die Daten aufbereitet für die Kunden zugänglich zu machen. Die daraus ableitbaren Anforderungen an die deCODEtron GmbH haben wir in Abschnitt „3.2.2 Nutzung der Daten“ untersucht. Im Wesentlichen betrifft dies

- die Übermittlung der Daten vom Lieferanten an die deCODEtron GmbH sowie
- die Bereitstellung der Daten für die Kunden.

Alle weiteren Verpflichtungen, insbesondere hinsichtlich der Erfüllung weiterer Aufbewahrungspflichten seitens der Kunden, sind --nicht zuletzt durch die fehlende vertragliche Vereinbarung zwischen der deCODEtron GmbH und Kunden-- durch diese selbst zu erfüllen. Dazu gehören das zeitnahe Abrufen der Informationen aus dem Inet-Archiv und die ordnungsmäßige Speicherung unter Berücksichtigung der entsprechenden Anforderungen hinsichtlich der GoBS und GDPdU.

Bei Nutzung des Inet-Archivs und der Jahres-CD (Variante B) übernimmt die deCODEtron GmbH auf vertraglicher Grundlage weitere Pflichten für die Kunden. Die Erfüllung der daraus abzuleitenden Anforderungen haben wir in Abschnitt „3.2.3 Nutzung des Inet-Archivs und der Jahres-CD“ untersucht.

3.2.2 Nutzung der Daten

3.2.2.1 Übermittlung der Daten an die deCODEtron GmbH

Anforderung

Zur Vermeidung von Datenverlusten und Manipulationsmöglichkeiten ist die Übermittlung der Daten ausreichend abzusichern. Durch angemessene Kontrollen ist die zeitnahe, korrekte und vollständige Verarbeitung der übermittelten Daten sicherzustellen.

Sachverhalt

Die Übertragung der Daten von den Lieferanten zur deCODEtron GmbH wird über zwei Mechanismen abgesichert:

- Die Datenübertragung wird per Secure FTP durchgeführt. Dadurch erfolgt die Datenkommunikation, die über das Internet erfolgt, durchgängig verschlüsselt.

- Zusätzlich kommt ein asymmetrisches Kryptographieverfahren auf Open-Source-Basis zum Einsatz (GPG), um die Integrität der Daten zu gewährleisten. Die Lieferanten signieren die zu verschickenden Daten, diese Signatur wird beim Empfang der Daten durch die deCO-DEtron GmbH verifiziert. Die dazu notwendigen öffentlichen Schlüssel der Lieferanten werden dazu auf ausreichend sicheren Wegen ausgetauscht.

Nachdem die Daten bei der deCODEtron GmbH weiterverarbeitet wurden, erfolgt die Signaturprüfung im Rahmen der originären Tagesdatensicherung. Der gesamte Prozess läuft über eine Stapelverarbeitungsdatei automatisiert ab. Ist die Signaturprüfung nicht erfolgreich, erfolgt automatisch eine entsprechende Meldung an die Administratoren.

Beginnend mit der Einwahl der Lieferanten auf dem FTP-Server der deCODEtron GmbH wird der Zugriff protokolliert. Die Informationstiefe des Protokolls umfasst die IP-Adresse des Lieferanten, die Zugriffszeit, die Dauer des Zugriffs sowie das verwendete Zugriffsprotokoll.

Ergebnis

Durch Tests haben wir uns von der Wirksamkeit des verschlüsselten Datenübertragung sowie der Signaturprüfung überzeugt. Wir halten die ergriffenen Maßnahmen --inklusive der Protokollierung-- für angemessen, die Integrität, Vertraulichkeit und Vollständigkeit der Datenübertragung sowie die Nachvollziehbarkeit des Verfahrens zu gewährleisten.

3.2.2.2 Bereitstellung der Daten für die Kunden

Anforderung

Gemäß §§ 143 und 144 AO müssen der Unternehmer Aufzeichnungen über den Wareneingang bzw. -ausgang (z. B. Lieferschein) anfertigen. Dies gilt auch für die Kunden, die von den Lieferanten mit Waren beliefert werden. Bislang lieferten die Lieferanten dazu papierbasierte Lieferscheine mit, anhand derer die Kunden die Vollständigkeit und Richtigkeit der erhaltenen Ware prüfen können und die als Belege über den Wareneingang dienen.

Da diese papierbasierten Dokumente durch das Inet-Archiv ersetzt werden sollen und den Kunden die Dokumente elektronisch zugänglich gemacht werden, müssen die Daten entsprechend aufbereitet und den Kunden online zugänglich gemacht werden.

Sachverhalt

Die von den Lieferanten übertragenen Daten werden durch die deCODEtron GmbH, indiziert, aufbereitet und online für die Kunden zur Verfügung gestellt. Bei Zugriff auf das Archiv können die entsprechenden Daten eingesehen und auch abgerufen werden. Die Darstellung entspricht im Wesentlichen der Darstellung der papierbasierten Dokumente.

Jedem an diesem Verfahren teilnehmenden Kunden wird ein eigener Zugang zu den Daten eingeräumt, über den nur die diesen Kunden betreffenden Daten abgerufen werden können. Diese Zugänge sind individuell über Name und Kennwort abgesichert.

Ergebnis

Wir haben uns im Rahmen unserer Prüfung davon überzeugt, dass die Daten über den vorgesehenen Zugang einsehbar sind und auch über einen angemessenen Zeitraum abgerufen werden können. Dabei erfolgt die Einrichtung der Benutzerzugänge nur auf Bestätigung des jeweiligen Lieferanten, wodurch sichergestellt ist, dass nur berechtigte Kunden Zugang zu ihren Daten erhalten.

3.2.3 Nutzung des Inet-Archivs und der Jahres-CD

Bei Nutzung des Inet-Archivs und der Jahres-CD (Variante B) werden die Dokumente elektronisch zur Verfügung gestellt (wie bei Variante A), zusätzlich übernimmt die deCODEtron GmbH die folgenden Leistungen:

- Zugriffsmöglichkeit auf das Inet-Archiv

- Lieferung eines Datenträgers mit den Daten eines Kalenderjahrs, jeweils nach Ende des Kalenderjahrs

Die Kunden nutzen somit zur Erfüllung ihrer Aufbewahrungspflichten für die Daten für das laufende Kalenderjahr das Inet-Archiv, anschließend die von der deCODEtron GmbH erstellten Datenträger. Dabei sind die folgenden Anforderungen zu betrachten, die durch die deCODEtron GmbH erfüllt werden müssen:

- Ablage und Speicherung (Vollständigkeit und Zeitnähe der Archivierung, Unveränderlichkeit der Dokumente, notwendige Protokollierungen, Indizierung und Abfrage)
- Langfristige Lesbarkeit und Wiederherstellbarkeit

3.2.3.1 Ablage und Speicherung

Vollständigkeit und Zeitnähe der Archivierung

Anforderung

Zur Vermeidung von Verlusten und Manipulationsmöglichkeiten sind Dokumente zeitnah in das Archivsystem zu überführen. Weiterhin ist technisch sicherzustellen, dass ein zu archivierendes Dokument vollständig an das Archivmedium übergeben wird.

Sachverhalt

Die Lieferanten liefern werktäglich die zu archivierenden Daten. Zu festgelegten Zeiten werden kundenindividuell die entsprechenden Verzeichnisse auf dem FTP-Server automatisch gescannt, in dem die Daten empfangen werden, und die Daten auf einen temporären Datenspeicher verschoben. Bevor am darauffolgenden Werktag die Archivierung dieser Daten erfolgt, werden die Daten in das Inet-Archiv kopiert und aufbereitet. Für den Fall, dass der automatische Durchlauf des Verschiebens der Daten nicht erfolgreich war, können die Administratoren dies im zugehörigen Protokoll ersehen und das entsprechende Skript manuell starten.

Die Zeitspanne ab dem Eingang der Daten bis zu ihrer Archivierung beträgt daher maximal wenige Stunden. Anhand der Prüfung der Signierung unmittelbar vor der Speicherung der Daten auf einem unveränderlichen Datenträger kann eine mögliche Manipulation der Daten zuverlässig erkannt und die Archivierung daraufhin gestoppt werden.

Mittels restriktiver Zugriffsrechte ist der Ablauf der Archivierung einschließlich genutzter Verzeichnisse und Systeme gegen unbefugte Zugriffe geschützt. Nur der technische Benutzer, der softwaregestützt die Archivierung durchführt, hat diesbezügliche Zugriffsberechtigungen.

Ergebnis

In Stichproben haben wir uns von der Wirksamkeit der Signaturprüfung und der zeitnahen Archivierung überzeugt. Die ergriffenen Maßnahmen zum Schutz der temporären Datenhaltung vor und während der Archivierung gegen Manipulation und unbefugte Zugriffe halten wir für angemessen.

Unveränderlichkeit der Dokumente

Anforderung

An die Speicherung und Archivierung aufbewahrungspflichtiger Unterlagen auf anderen Datenträgern i. S. d. § 257 Abs. 3 und §147 Abs. 2 AO stellen Handels- und Steuerrecht grundsätzlich die Anforderung, dass Änderungen an einmal archivierten Dokumenten nicht mehr möglich sind, ohne dass der ursprüngliche Zustand erkennbar ist.

Sachverhalt

Die zu speichernden Daten werden täglich, je Lieferant, direkt nach Prüfung der Signatur im Inet-Archiv und zusätzlich auf optischen, einmal beschreibbaren Medien (CD-R bzw. DVD-R) gesichert. Unmittelbar nach dem Schreibvorgang werden die geschriebenen Daten anhand der Signatur nochmals auf Integrität geprüft. Bei Fehlern wird eine entsprechende Meldung in einer Logdatei generiert. Diese Logdatei wird täglich überwacht und Fehler werden entsprechend behoben.

Zusätzlich wird je Medium eine Prüfsumme errechnet, die in die Prüfsummenberechnung des Folgetags mit einbezogen werden. Durch diese Verkettung der Sicherungsmedien wird verhindert, dass bereits geschriebene optische Medien manipuliert werden können, da sich bei einer inhaltlichen Änderung die Prüfsumme des Mediums ändern würde. Damit wäre die Verkettung der Sicherungsmedien über die Prüfsummen nicht mehr konsistent.

Alle Kunden verfügen mit ihrem Zugang zum Inet-Archiv nur über Leserechte. Schreibrechte sind ausgeschlossen. Lediglich das entsprechende Verzeichnis auf dem FTP-Server der deCODEtron GmbH bietet Schreibzugriff, damit die Lieferanten ihre signierten Daten dort ablegen.

Sofern Verzeichnisse als temporärer Aufbewahrungsort zwischen dem FTP-Server und der endgültigen Archivierung auf CD/DVD verwendet werden, sind diese in der Weise vor Zugriff geschützt, dass nur das jeweils beteiligte Programm Schreibrechte besitzt.

Ergebnis

Wir konnten uns im Rahmen unserer Prüfung von der Wirksamkeit der getroffenen Maßnahmen zur Unveränderlichkeit der Daten überzeugen.

Die Signierung der Daten durch die Lieferanten in Verbindung mit der Verkettung der Sicherungsmedien durch eine Prüfsumme aus den Daten bietet prinzipiell ein Sicherheitsniveau, das die Unveränderlichkeit der Daten in ausreichender Weise gewährleistet und ferner ermöglicht, Manipulationen zu entdecken.

Da aber die Konsistenz der Verkettung der Sicherungsmedien nicht systematisch überprüft wird, besteht daher die Gefahr, dass Manipulationen zwar erkennbar sind, aber mangels Kontrolle nicht aufgedeckt werden. Die deCODEtron GmbH sollte die Konsistenz der Medienverkettung daher regelmäßig prüfen und dokumentieren.

Notwendige Protokollierungen

Anforderung

Um den Prozess der Ablage nachvollziehbar zu gestalten, müssen Bearbeitungsvorgänge an den gespeicherten Dokumenten protokolliert werden. Diese Protokolle unterliegen einer Aufbewahrungsfrist von zehn Jahren. Darüber hinaus müssen bearbeitete Dokumente als Kopie gekennzeichnet werden.

Sachverhalt

Auf Grund der restriktiven Zugriffsberechtigungen gewährt das System während und nach der Archivierung auf CD/DVD keine Bearbeitungsmöglichkeit der Daten. Die Daten des Inet-Archivs hingegen sind änderbar. Insbesondere bei fehlerhaften Datenlieferungen der Lieferanten ist diese Bearbeitungsmöglichkeit erforderlich.

Im Falle einer solchen fehlerhaften Datenlieferung wird der Archivierungsvorgang bis zur Produktion einer CD/DVD erneut durchlaufen. Zusätzlich schickt der Lieferant die Daten erneut in korrigierter Form mit einer entsprechenden Anmerkung per eMail. Diesbezüglicher Schriftverkehr (auch eMails) wird zusammen mit den neuen Daten ebenfalls archiviert, so dass der Grund der Änderung sowie der Zustand davor nachvollziehbar bleiben. Für den Lieferanten ist online grundsätzlich die korrigierte Fassung der Daten einsehbar, da der entsprechende Index auf das aktuellste Dokument verweist. Über spezielle Berechtigungen kann jedoch auf die ebenfalls vorhandenen Originaldaten zugegriffen werden. Für das Inet-Archiv verfügen die Lieferanten lediglich über Leseberechtigungen, können also keine Änderungen an den Dokumenten vornehmen. Insofern müssen Änderungen auch nicht protokolliert werden.

Ergebnis

Da die Daten auf CD/DVD archiviert werden und dann unveränderlich sind, ist insofern eine Protokollierung von Änderungen nicht notwendig. Das Vorgehen in Bezug auf die Dokumentation von Korrekturen oder Änderungen am Inet-Archiv halten wir für angemessen.

Indizierung und Abfrage

Anforderung

Um unverzügliche Lesbarmachung zu gewährleisten, muss auf die Dokumente über geeignete Ordnungskriterien gezielt zugegriffen werden können. Der dazu zu führende Index darf nicht veränderbar sein. Der Aufbewahrungspflichtige hat sicherzustellen, dass die eingesetzte Indizierungssystematik einen gezielten Zugriff erlaubt. Die Risiken der Fehlindizierung und dadurch der Unauffindbarkeit sind zu minimieren. Die Anwendung muss geeignete Werkzeuge zur Verfügung stellen, um archivierte Dokumente zeitnah in ausreichender Qualität lesbar zu machen.

Sachverhalt

Im Rahmen der Aufbereitung der Daten für das Inet-Archiv werden die Daten indiziert. Die Indexdaten werden in einer eigenen Datenbank auf dem jeweiligen Inet-Server abgelegt und werktäglich mit den neu hinzukommenden Daten aktualisiert.

Ausgangspunkt der Indizierung ist der von den Lieferanten gelieferte Druckstrom, der anhand von zwei kundenspezifischen Konfigurationsdateien indiziert wird:

- Die ctl-Datei legt fest, an welcher Stelle im Originaldatenstrom welche Daten stehen, welche Felder davon indiziert werden sollen und in welchem Datentyp die Felder jeweils vorliegen (char, number etc.).

- Die conf-Datei steuert die Darstellung im Inet-Archiv. Im Einzelnen werden Kriterien wie Reihenfolge, Bezeichnungen und Sortierung der Daten festgelegt.

Bei den Daten ist die Indizierung von Seiten der Lieferanten grundsätzlich nicht änderbar. In Abstimmung mit der deCODEtron GmbH können jedoch zusätzliche Indexfelder aufgenommen werden. Auf jeden Fall erfolgt die Umsetzung durch die deCODEtron GmbH, da die Lieferanten nur über lesenden Zugriff auf ihre Daten verfügen.

Sollte der Index abhanden kommen, kann er jederzeit mit Hilfe der Konfigurationsdateien aus dem Original-Druckstrom regeneriert werden.

Alle von den Lieferanten gelieferten Daten werden vor Archivierung einer Kontrolle der fortlaufenden Belegnummern unterzogen. Werden doppelte oder fehlende Belegnummern festgestellt, werden die jeweiligen Dokumente bzw. Lücken protokolliert und dem entsprechenden Lieferanten mitgeteilt. Auf diese Weise stellt die deCODEtron GmbH die Eindeutigkeit des Indexes fest. Fehlerprotokolle und Schriftverkehr mit dem Lieferanten werden zur Nachvollziehbarkeit ebenfalls archiviert.

Der Zugriff auf die Daten erfolgt online mittels Webfrontend. Dargestellt werden die Suchmaske, die die Daten der Indexdatenbank anzeigt, sowie das Ergebnis der Suche respektive das gefundene Dokument. Dabei zeigt die Indexdatenbank letztlich selbst auf den Druckstrom. Standardmäßig stehen die Indexfelder Artikelnummer, Belegnummer, Kundennummer, Datum sowie Niederlassungsnummer zur Verfügung, wobei diese Angaben kundenindividuell anpassbar und ausgeprägt sind. Insbesondere ist die Indizierungssystematik von dem gelieferten Druckstrom abhängig, der die indizierbaren Daten vorgibt.

Nach Ablauf eines Jahres werden den Kunden die gesammelten Daten eines Jahres (sofern zusätzlich beauftragt) auf CD (bzw. DVD) zur Verfügung gestellt („Jahres-CD“). Formal ersetzt die Jahres-CD den Zugriff auf die online vorgehaltenen Daten. Faktisch werden die Daten dennoch weiter online zur Verfügung gestellt, da die Onlineabfrage der Daten Vorteile in Bezug auf die Zugriffsgeschwindigkeit bietet.

Für die Anzeige der Daten im Inet-Archiv sind ein Standardbrowser mit aktiviertem JavaScript sowie ein PDF-Viewer nötig. Die Anzeige der Daten auf der Jahres-CD ist mittels der mitgelieferten Software möglich. Als Datenbasis ist auf der CD der Teil des Originaldatenstroms gespeichert, der für den jeweils belieferten Kunden relevant ist respektive ihre Dokumente enthält. Mittels Eingabe von Suchbegriffen in den entsprechenden Feldern filtert die Applikation den Datenbestand und zeigt nur die passenden Dokumente an. Auf Grund der optimierten Indizierung im Vorfeld ist das Auffinden von Dokumenten sehr schnell möglich. Im Anzeigefenster wird das markierte Dokument als PDF angezeigt und kann bei Bedarf auch lokal gespeichert werden.

Ergebnis

Der führende Index wird zusammen mit den Daten abgelegt und ist bei richtiger Definition geeignet, schnell und gezielt auf die Daten zuzugreifen. Bei Verlust des Indexes kann dieser aus dem Datenstrom jederzeit wieder neu aufgebaut werden. Eine Veränderbarkeit des Indexes ist durch die getroffenen Maßnahmen wirksam verhindert. Über gängige Softwarewerkzeuge unter Nutzung verbreiteter Standards (z. B. PDF) kann mit Hilfe der angebotenen Indizierungssystematik schnell auf den Datenbestand zugegriffen werden. Den Anforderungen des Handels- und Steuerrechts ist damit wirksam entsprochen. Wir haben uns in Stichproben von der Wirksamkeit der eingerichteten Maßnahmen überzeugt.

3.2.3.2 Langfristige Lesbarkeit und Wiederherstellbarkeit

Anforderung

Handels- und Steuerrecht erfordern, dass auf Datenträgern geführte aufbewahrungspflichtige Unterlagen während der Dauer der Aufbewahrungsfrist verfügbar sind und innerhalb angemessener Frist lesbar gemacht werden können. Gemäß Steuerrecht sind die Rahmenbedingungen enger definiert: Die Unterlagen müssen jederzeit verfügbar und unverzüglich lesbar gemacht werden können.

Sachverhalt

Sowohl online im Inet-Archiv als auch auf der Jahres-CD werden die Daten im Originalformat der Lieferanten (Druckstrom) gespeichert. Dabei kommen die Zeichenkodierungen ASCII und EBCDIC zum Einsatz. Beide Zeichenkodierungen lassen auf Grund der hohen Marktdurchdringung und der Vielzahl an verfügbaren Tools nach heutigem Kenntnisstand eine dauerhafte und zukunftssichere Verwendung erwarten.

Auf der Jahres-CD sind zusätzlich die Indexdatenbank sowie ergänzende Tools gespeichert. Eine Archiv- bzw. Jahres-CD/DVD ist damit autark und als eigenes Archiv zu betrachten. Die Unverzüglichkeit der Lesbarmachung ist durch die mitgelieferten Tools sowie die Tatsache gewährleistet, dass keine Konvertierungen oder Indizierungen notwendig sind. Die langfristige Lesbarkeit und Auswertbarkeit der archivierten Daten, auch im Sinne der GDPdU, ist damit sichergestellt.

Zur Sicherung der Daten im Inet-Archiv hat die deCODEtron GmbH die folgenden Maßnahmen ergriffen:

- Für die unveränderliche Archivierung der Daten werden spezielle CDs/DVDs, die sich durch eine --im Verhältnis zu handelsüblichen CDs/DVDs-- verhältnismäßig hohe Lebensdauer von 30-50 Jahren (Herstellerangabe) auszeichnen, verwendet. Um die Lebensdauer zu erhöhen, werden die CDs/DVDs in schwarzer Folie vakuumverschweißt. Auf Grund der Herstellerangaben zur Lebensdauer der Datenträger sind Tests der Lesbarkeit auskunftsgemäß nicht vorgesehen.

- Die Datensicherung des Inet-Archivs erfolgt sowohl auf Festplatten als auch auf Bändern. Die Datensicherungen dienen der Absicherung der Installationen der einzelnen Lieferanten, um diese im Bedarfsfall kurzfristig wiederherstellen zu können. Der Fokus liegt hierbei auf der Sicherung der Programmstände, die täglich inkrementell und wöchentlich voll gesichert werden. Um Lebensdauer verkürzende Einflüsse auf die Festplatten und Bänder auf ein Mindestmaß zu verringern, werden die Datenträger vor der Aufbewahrung ebenfalls in schwarzer Folie luftdicht verschweißt. Da Festplatten über eine kürzere Lebensdauer als Bänder und CDs/DVDs verfügen, sind alle zwei bis drei Jahre Lesbarkeitstests vorgesehen.

Die Lesbarkeitstests für die Festplatten umfassen eine Defragmentierung, das stichprobenartige Öffnen der darauf gespeicherten Dateien sowie Größenvergleiche mit den Originalen auf dem entsprechenden Inet-Server. Um Vorsorge für die langfristige Lesbarkeit zu unterstützen, ist das Umspulen der Bänder in einem Intervall von drei bis fünf Jahren vorgesehen. Neben dem Datenträger wird dem Folienbeutel eine Karteikarte beigelegt, auf der wichtige Daten zu Inhalt und Lebenszyklus des Datenträgers vermerkt werden (z. B. Inhalt, Überprüfungsintervall, Handzeichen des Testers, Ergebnisse der Lesbarkeitstests). Auf einer zusätzlich geführten Excelliste sind diese Daten ebenfalls dokumentiert, um die Wartungszyklen steuern zu können und jederzeit eine Übersicht der gespeicherten Daten und ihres Aufbewahrungsorts zu haben.

- Neben der Datensicherung auf Festplatten und Bändern verfügt jeder Inet-Server über weitere Sicherungsmaßnahmen, um eine dauerhafte Lesbarkeit der Daten gewährleisten zu können. Dazu gehört im Wesentlichen die Konfiguration der Daten- und Programmspeicher als RAID-System, wobei die Systeme so genanntes HotSpare unterstützen. Fällt eine Festplatte aus, kann sie im laufenden Betrieb ersetzt werden, ohne dass das entsprechende Inet-Archiv eine eingeschränkte Verfügbarkeit oder sogar einen Ausfall hinnehmen müsste.

Die Übernahme der Aufbewahrungspflichten von der deCODEtron GmbH endet mit der Bereitstellung der Jahres-CD. Für die anschließende ordnungsgemäße Aufbewahrung der Jahres-CD sind die Kunden verantwortlich.

Trotz offenbar auf Langfristigkeit ausgerichteter Bauweise der Archiv-CDs/DVDs sind auch diese gegen den schleichenden Zerfall nicht resistent. Um die behauptete lange Lebensdauer der CDs/DVDs zu überprüfen, sollten daher stichprobenartige Lesbarkeits- und Wiederherstellungstests durchgeführt werden, um mögliche Schwachstellen frühzeitig zu erkennen.

Die deCODEtron GmbH führt regelmäßig Lesbarkeitstests durch und dokumentiert diese auf den den Datenträgern beigelegten Karten.

Ergebnis

In Stichproben haben wir uns von der Wirksamkeit der ergriffenen Maßnahmen überzeugt. Wir sind davon überzeugt, dass die getroffenen Maßnahmen angemessen und geeignet sind, um die archivierten Daten für die Dauer der Aufbewahrungsfrist verfügbar zu halten und im Bedarfsfall unverzüglich lesbar zu machen.

3.3 Softwaresicherheit und Systemadministration

3.3.1 Zugriffs- und Zutrittsschutz

3.3.1.1 Logische Sicherheit

Anforderung

Die GoBS verlangen zum Schutz von rechnungslegungsrelevanten Daten wirksame Zugriffsberechtigungskontrollen, die so zu gestalten sind, dass nur berechtigte Personen in dem ihrem Aufgabengebiet entsprechenden Umfang auf Programme und Daten zugreifen können.

Um die Wirksamkeit der eingerichteten Zugriffsschutzverfahren zu gewährleisten, ist das System nach anerkannten Sicherheitsrichtlinien zu konfigurieren. Die angebotenen Kommunikationsdienste sollten Passworte nur verschlüsselt übertragen.

Sachverhalt

Betriebssystem

Als Betriebssystem auf einem so genannten Inet-Server --ein für den Lieferanten individuell konfiguriertes Archivsystem-- fungiert Windows XP. Auf die für den Archivierungsprozess verwendeten Verzeichnisse hat lediglich ein Systembenutzer Zugriff, der von den einzelnen Archivierungskomponenten verwendet wird.

Auf allen Servern wird TrendMicro als Virenschutz eingesetzt. Automatisch lädt das Programm täglich neue Virendefinitionen aus dem Internet herunter und bietet so angemessenen Schutz vor aktuellen Bedrohungen wie Viren, Würmern und Trojanern.

Netzwerk

In der Kommunikation mit den Benutzern --Abfrage der Kunden im Inet-Archiv, administrative Zugriffe der Lieferanten auf ihr Inet-Archiv-- wird https eingesetzt. Das dafür notwendige Zertifikat ist als Wildcard-Zertifikat ausgestaltet und war zum Zeitpunkt der Prüfung gültig. Ein Wildcard-Zertifikat bietet den Vorteil, dass die entsprechende Domain als vertrauenswürdig eingestuft wird, wobei unterschiedliche Subdomains (*.inetarchiv.de) verwendet werden können.

Der Zugriff auf die Systeme der deCODEtron GmbH bzw. der Inet-Server per Fernzugriff ist mittels einer VPN-Software gegen unautorisierte Zugriffe geschützt. Als Protokolle werden dabei je nach Lieferant entweder IPSec oder Point2Point verwendet.

In der Firewallkonfiguration sind nur die für die Kommunikation nach außen notwendigen Ports freigegeben. Nicht benötigte sowie für Angriffe häufig genutzte Ports sind dagegen gesperrt, d. h. nur benötigte Dienste sind aktiviert (Secure FTP, http etc.). Als zusätzlicher Serverschutz werden alle aktiven Serverdienste durch den externen Überwachungsdienst Watchdog permanent einem Monitoring unterzogen. Täglich schickt der Dienst automatisch eine Auswertung der Überwachungsergebnisse mit Kennzeichnung von sicherheitskritischen Vorfällen. Dadurch können entsprechende Vorfälle genau dem entsprechenden Dienst zugeordnet werden, was die Fehleranalyse im Bedarfsfall erheblich erleichtert.

FTP

Alle Lieferanten, die ihre Datenströme der deCODEtron GmbH zur Archivierung bereitstellen, übertragen ihre Daten über das Secure-FTP-Protokoll an den FTP-Server bei der deCODEtron GmbH. Das Protokoll wird im „Passive Mode“ verwendet. Dadurch werden sowohl die Authentifizierung des Clients mit Namen und Kennwort als auch der Datenstrom verschlüsselt übertragen. Die Authentifizierung und Datenübertragung respektive die gesamte Sitzung wird mit einer Schlüssellänge von 256 Bit nach dem AES-Verfahren verschlüsselt. Das Verschlüsselungsverfahren verwendet für die Erzeugung eines Hash-Werts den SHA-Algorithmus.

Als weiteres Sicherheitsmerkmal ist für die Kommunikation ein Timeout von zwei Minuten konfiguriert, d. h. nach zwei Minuten ohne Aktivität in der laufenden Kommunikationsverbindung wird die entsprechende Sitzung geschlossen. Dabei kann der eingestellte Timeout-Wert je nach Anforderung kundenindividuell konfiguriert werden.

Der Archivierungsstrang bzw. die daran beteiligten Systeme sind im Hinblick auf Berechtigungen dadurch geschützt, dass Zugriffe nur für Systembenutzer im Verlauf der Archivierung möglich sind.

Applikation

Um die Wartbarkeit des Inet-Archivs zu erleichtern, hat die deCODEtron GmbH eine Trennung von Applikationslogik und Daten etabliert. Die Applikationslogik einschließlich aller Systemprogramme in der notwendigen Konfiguration ist sowohl logisch als auch physisch getrennt durch unterschiedliche logische Laufwerke und Festplatten. Dadurch wird auch die Datensicherung und Wiederherstellbarkeit der Applikation erheblich erleichtert bzw. verbessert.

Für den Zugang zu den Daten im Inet-Archiv muss der Lieferant seine Mitarbeiter sowie die angeschlossenen Kunden entsprechend autorisieren. Das geschieht in Abstimmung mit der deCODEtron GmbH, die entsprechend dem dafür vorgesehenen Berechtigungskonzept die

einzelnen Berechtigungen im System einrichtet. Jedem Benutzer wird ein Benutzerzugang mit Passwort zugeteilt, mit dem er sich im Inet-Archiv authentifiziert. Für die Ausgestaltung der Passwörter hat die deCODEtron GmbH für den Lieferanten eine Passwortrichtlinie erarbeitet, die aktuelle Empfehlungen des BSI zum Thema Passwortschutz umsetzt. Die Passwortgestaltung umfasst eine vorgeschriebene Mindestlänge von sechs Zeichen, eine maximale Lebensdauer von sechs Monaten sowie Restriktionen der Passwortkomplexität (Verwendung von Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen) in Verbindung mit einer Anleitung zum Anlegen sicherer Passwörter. Die Clientauthentifizierung erfolgt mittels Benutzername und Passwort direkt auf der Website.

Die Differenzierung der Zugriffsberechtigungen der Lieferanten und Kunden wird mit Hilfe eines Berechtigungskonzepts, das in einer Konfigurationsdatei aufseiten der deCODEtron GmbH gespeichert und verwaltet wird, durchgesetzt. Das Berechtigungskonzept bietet die Möglichkeit, Benutzerprofile für verschiedene Benutzergruppen (z. B. Pharmagroßhändler, Apotheke, deCODEtron, Finanzverwaltung) sowie beliebige Kombinationen einzelner Berechtigungen abzubilden.

Protokollierung

Sämtliche Zugriffe auf das Inet-Archiv vonseiten der Nutzer über das Internet werden mit Benutzerkennung, Zugriffszeit und Zugriffsdauer protokolliert. Das hat in der Vergangenheit schon zur Aufklärung von Missbrauchsfällen beigetragen.

Daneben wird der gesamte FTP-Verkehr protokolliert. So ist nachvollziehbar, wer sich mit welcher IP-Adresse wann eingeloggt und welche Daten übertragen hat.

Intern werden sowohl die Übertragung des Datenstroms vom FTP- auf den Inet-Server, die Erzeugung der Indexdatenbank für den wahlfreien Zugriff auf die Daten im Inet-Archiv sowie die unveränderliche Archivierung auf CD/DVD protokolliert. Bei Fehlern oder Sicherheitsvorfällen können die Protokolle die Analyse unterstützen.

Sämtliche Protokolle werden zusammen mit den ZIP-Archiven im jeweiligen Jahresordner der Lieferanten gespeichert und zehn Jahre aufbewahrt. Mit Hilfe einer Excelliste werden die einzelnen Archivierungsdaten, Aufbewahrungsfristen und entsprechenden Restlaufzeiten verwaltet und sind so jederzeit abrufbar.

Ergebnis

Die Verwendung von erprobten Verschlüsselungsverfahren mit angemessenen Schlüsselstärken gewährleistet eine sichere Kommunikation über das Internet, ohne den dabei vollzogenen Datenaustausch unnötig erhöhter Angreifbarkeit preiszugeben.

In Stichproben haben wir uns von der ordnungsmäßigen Systemkonfiguration überzeugt. Die ergriffenen Maßnahmen im Sinne der Gewährleistung der Wirksamkeit der Zugriffsschutzverfahren halten wir für angemessen.

3.3.1.2 Physische Sicherheit

Anforderung

Die physischen Sicherungsmaßnahmen dienen dem Schutz der Hardware sowie der Programme und Daten vor Verlust, Zerstörung und unberechtigter Veränderung.

Sachverhalt

Die deCODEtron GmbH verfügt über zwei Serverräume, wobei der zweite Raum zur Erhöhung der Ausfallsicherheit dient und alle notwendigen Funktionen des ersten übernehmen kann. Die Komponenten für den Betrieb sowohl der eigenen Infrastruktur als auch der Anwendung sind redundant ausgelegt.

Beide Serverräume sind in das Schließkonzept eingebunden. Danach verfügen nur Mitarbeiter der deCODEtron GmbH über einen Schlüssel. Der zweite Serverraum befindet sich im Keller des Gebäudes und ist zusätzlich zur feuerfesten Stahltür mit doppelt vergitterten Kellerfenstern und einem Sichtschutz darin versehen. Serverraum 1 befindet sich in einem abgetrennten Bereich in den Geschäftsräumen der deCODEtron GmbH. Sowohl Keller als auch Geschäftsräume sind alarmgesichert, so dass nach Scharfschaltung die Alarmanlage mit akustischem Warnsignal und Aufschaltung zur Polizei aktiviert wird. Zusätzliche Sicherheit geben die installierten Bewegungsmelder, die ebenfalls nach Scharfschaltung der Alarmanlage aktiviert sind.

Die gesamte Infrastruktur verfügt über mehrere USVs, die regelmäßig im Rahmen von Notfalltests überprüft werden. Um längere Stromausfälle zu überbrücken, steht zudem ein Dieselaggregat zur Verfügung, das ebenfalls regelmäßiger Wartung und Tests unterliegt.

Beide Serverräume sind voneinander durch mehrere Etagen und Brandabschnitte getrennt. In Reichweite befinden sich jeweils Feuerlöscher.

In Serverraum 1 ist eine Klimatisierung installiert. Die Temperatur wird in beiden Räumen überwacht. Bei Überschreitung bestimmter Schwellenwerte werden die Administratoren automatisch benachrichtigt.

Die Rauchmelder in beiden Serverräumen sind direkt zur örtlichen Feuerwehr aufgeschaltet.

Ergebnis

Die physischen Sicherheitsmaßnahmen bieten einen angemessenen Schutz der Hard- und Software vor Verlust, Zerstörung und unberechtigter Veränderung. Insofern sind die handels- und steuerrechtlichen Anforderungen erfüllt.

3.3.2 Datensicherungs- und Wiederanlaufverfahren

Anforderung

Gemäß Handels- und Steuerrecht hat der Aufbewahrungspflichtige Maßnahmen zur Sicherung der Informationen vor Verlust und schädlichen Einwirkungen zu treffen. Dazu ist die Durchführung von Datensicherungsprozeduren erforderlich, die alle wesentlichen Datenbestände berücksichtigen. Implementierte Wiederanlaufverfahren sollen sicherstellen, dass das Datenarchiv im Katastrophenfall zeitnah wiederhergestellt werden kann.

Sachverhalt

Die Datensicherung erfolgt sowohl auf Bändern als auch auf Festplatten. Dabei werden Daten, Programme und konfigurierte Systeme separat gesichert. Lieferantendaten werden täglich unveränderlich archiviert. Insoweit verweisen wir auf Abschnitt „3.2.3.1 Ablage und Speicherung“. Daneben werden die aktuellen Archive täglich inkrementell auf wechselnden Fileservern sowie wöchentlich als Vollbackup auf einem dritten Fileserver gesichert.

Jährlich wird der gesamte Datenbestand des vergangenen Geschäftsjahres des kompletten Programmbestands einschließlich Konfigurations- und Logdateien auf zwei separaten Festplatten, wovon eine extern aufbewahrt wird, und zusätzlich auf Band gesichert. Dadurch wird eine zeitnahe Arbeitsaufnahme nach Ausfall der Infrastruktur unterstützt.

Daneben wird eine Reihe von zusätzlichen initialen, monatlichen und jährlichen Sicherungen der komprimierten und dekomprimierten Datenbestände, der betriebsnotwendigen Anwendungsentwicklungs- und Administrationstools sowie sonstiger Dienstprogramme durchgeführt – jeweils darauf ausgerichtet, im Notfall eine schnelle Wiederaufnahme des Betriebs zu erreichen. Die Sicherung des Inet-Servers umfasst dabei die kundenindividuelle Zusammenstellung aller Bestandteile der Anwendung in der notwendigen Konfiguration. Fällt ein solches System aus, kann durch Austausch der entsprechenden Festplatte das System binnen weniger Minuten wieder zur Verfügung gestellt werden.

Um den Langzeitschutz der verwendeten Sicherungsdatenträger (Bänder und Festplatten) zu erhöhen, werden diese in schwarzer Folie lichtgeschützt vakuumverschweißt. Dadurch wird der materialbedingten Anfälligkeit gegen Sonnenlicht entgegengewirkt.

Sämtliche Sicherungsdatenträger stehen mindestens als Duplikat zur Verfügung und werden als Sicherungsmaßnahme monatlich ausgelagert. Sowohl intern als auch extern stehen entsprechend physisch gesicherte Lagereinrichtungen zur Verfügung, die Rauchmelder, feuerfeste Aufbewahrung und Zugangsschutzmaßnahmen gewährleisten.

Wiederherstellungstests der Bänder und Festplatten werden in unregelmäßigen Abständen durchgeführt. Dazu werden stichprobenartig Datenträger aus der Schutzfolie entnommen und Lesbarkeitstests durchgeführt. Auf einer beiliegenden Karte werden die Ergebnisse der Tests sowie Datum und Name des Testers vermerkt.

Der Notfallplan der deCODEtron GmbH berücksichtigt mehrere Szenarien (Hardwaredefekte, Softwarefehler, unvollständige Daten, Zerstörung einzelner Komponenten oder des gesamten Standorts) und listet entsprechend konkrete Checklisten, Ablaufpläne und Handlungsanweisungen sowie Kontaktdaten auf. In unregelmäßigen Abständen werden Notfalltests einzelner Komponenten (z. B. Test des Dieselgenerators, vollständige Neueinrichtung eines Inet-Servers) durchgeführt, jedoch nicht oder nur unvollständig und über mehrere Dokumente verstreut dokumentiert. Das erschwert eine Gesamtbetrachtung und Analyse möglicher Schwachstellen.

In Bezug auf Ausfallsicherheit und Redundanz der Systeme steht für jeden Lieferanten ein entsprechendes System als kostenpflichtige Ergänzung zur Verfügung. Dadurch kann im Bedarf Hochverfügbarkeit erreicht werden. Auskunftsgemäß setzen bereits zwei Drittel der Lieferanten diese Option ein.

Ergebnis

Im Sinne einer besseren Gesamtschau und Analysemöglichkeit der Notfallmaßnahmen und ihrer Wirksamkeit, insbesondere als Erfahrungswerte aus den Notfalltests, sollten die Tests einheitlicher konzipiert und dokumentiert werden.

In Stichproben haben wir uns von der Wirksamkeit der Datensicherung und der Verfahren zur Rücksicherung überzeugt. Die eingesetzten Verfahren zur Datensicherung und zur Datenwiederherstellung halten wir für angemessen.

3.3.3 Programmentwicklung, -wartung und -freigabe

Anforderung

Die bei der Programmentwicklung verwendeten Methoden sollten schriftlich dokumentiert sein. Um die erstellten Programme und Programmbestandteile dauerhaft warten und wieder verwenden zu können, sollten Regelungen für den Programmaufbau, Namenskonventionen und Dokumentationsanforderungen in einer Programmierrichtlinie zusammengefasst sein.

Um durch Fehlerkorrekturen und Funktionserweiterungen die Qualität des existierenden Programmcodes nicht zu gefährden, sollte zur Umsetzung ein schriftlich fixiertes Verfahren existieren. Dessen Umsetzung muss durch eine geeignete Protokollierung nachvollziehbar sein. Ein derartiges Verfahren sollte mindestens folgende Schritte beinhalten:

- Schriftliche Anforderung für Fehlerbeseitigung bzw. Funktionserweiterung mit Stellungnahme der Projektleitung
- Test der fehlerkorrigierten Programmfunktion bzw. der Funktionserweiterung --dieser Test darf nicht von den Entwicklern durchgeführt werden-- und Freigabe
- Integrationstests und Freigabe
- Gesamtfreigabe der fehlerkorrigierten bzw. neuen Version durch die Projektleitung

Sachverhalt

Bestandteil der Verfahrensdokumentation sind verschiedene Richtlinien in Bezug auf verschiedene Aspekte der Softwareentwicklung wie Dokumentation und Änderungsmanagement. Eine separate Entwicklungsrichtlinie ist auf Grund der überschaubaren Zahl der Entwickler auskunftsgemäß nicht nötig.

Die Softwareentwicklung bei der deCODEtron GmbH ist derzeit stark durch die Anforderungen der Lieferanten getrieben. Insoweit werden Entwicklungsprojekte in enger Abstimmung mit den Lieferanten konzipiert und durchgeführt. Dabei ist das Mittel der Kommunikation und Abstimmung hauptsächlich das Pflichtenheft, das von der deCODEtron GmbH anhand der Anforderungen der Lieferanten verfasst und in einem Abstimmungsprozess mit dem Lieferanten umgesetzt wird. Der nachfolgende Vertrag mit dem Lieferanten umfasst eine Projektplanung sowie das Pflichtenheft als integrale Bestandteile. Funktions- und Leistungsumfang sind damit dokumentiert, abgestimmt und genehmigt.

Implementierte Komponenten werden von den Entwicklern sofort getestet und später Integrationstests unterzogen. Nach erfolgreichen Tests der Entwickler wird die Software von den Administratoren ins Testsystem eingespielt und dort Tests in produktivnahen Umgebungsbedingungen unterzogen. Anschließend werden fachliche Tests durchgeführt. Entscheidend ist dabei der im Pflichtenheft festgeschriebene Funktions- und Leistungsumfang.

In einer abschließenden Phase wird die Anwendung für den Lieferanten freigeschaltet, der dann seinerseits fachliche Tests nach Maßgabe des Pflichtenhefts durchführt.

Auftretende Fehler in allen Phasen der Entwicklung werden zeitnah behoben und entsprechend dokumentiert. Programmänderungen können so mit Datum, Bearbeiter und Grund sowie Umfang der Änderung nachvollzogen werden. Nachträgliche Fehler und Änderungen, die der

Lieferant feststellt, werden per eMail mitgeteilt. Diesbezüglicher Schriftverkehr wird den Projekt- bzw. Lieferantenunterlagen hinzugefügt.

Eine Änderungshistorie der einzelnen Programmstände steht den Lieferanten online auf einer Unterseite ihres Inet-Archivs zur Verfügung. Geänderte Module, Versionen, Datum, Bearbeiter sowie angepasste Funktionalitäten sind dort beschrieben. Ebenfalls online stehen die Änderungsprotokolle der einzelnen Programmmodule sowie Handbücher bzw. Bedienungsanleitungen zur Verfügung. Der Lieferant kann also jederzeit online nachvollziehen, welcher Programmstand seinem Inet-Archiv aktuell zu Grunde liegt.

Vor Produktivschaltung der Anwendung erteilt der Lieferant eine letzte Freigabe, die dokumentiert wird. An die Freischaltung schließt sich die Produktiv- und Supportphase an, die durch Betrieb der Lösung gemäß Vertrag und laufende Anpassung der Anwendung an die Anforderungen des Lieferanten gekennzeichnet ist.

Ergebnis

Durch Einsichtnahme in die Programmentwicklung, -wartung und -freigabe anhand von aktuellen Projekten haben wir uns von der Ordnungsmäßigkeit des Verfahrens überzeugt und halten dies für angemessen. Den Anforderungen an eine ordnungsmäßige Programmentwicklung, -wartung und -freigabe ist damit wirksam entsprochen.

3.4 Dokumentation

Anforderung

Nach den GoBS müssen aus der Verfahrensdokumentation Inhalt, Aufbau und Ablauf des Verfahrens vollständig ersichtlich sein. Die Verfahrensdokumentation umfasst daher die Systemdokumentation, die Betriebsdokumentation und die Anwenderdokumentation.

Die Verfahrensdokumentation hat insbesondere folgende Teile zu beinhalten:

- Die Beschreibung der sachlogischen Lösung
- Die Beschreibung der programmtechnischen Lösung
- Eine Beschreibung, wie die Programmidentität gewahrt wird
- Eine Beschreibung, wie die Integrität von Daten gewahrt wird
- Arbeitsanweisungen für den Anwender

Sie hat das eingesetzte Verfahren richtig zu beschreiben und muss für einen sachverständigen Dritten verständlich sein.

Sachverhalt

Die sachlogische Lösung ist in Kapitel 1 „Unternehmen deCODEtron“ sowie 3 „Berechtigungskonzepte für Hard- und Software“ und 11 „Qualitätsmanagement“ anforderungsgemäß beschrieben.

Die programmtechnische Lösung wird maßgeblich in den Kapiteln 2 „Technische Organisation“ und 5 „Software“ beschrieben. Zusätzlich enthält der Quelltext der selbsterstellten Software entsprechende Kommentare zur Beschreibung der Programmfunktionalität im Detail. Regelmäßig ist diese Dokumentation jedoch nicht Bestandteil der frei verfügbaren Dokumentation.

Zur Wahrung der Datenintegrität hat die deCODEtron GmbH verschiedene Maßnahmen getroffen, die detailliert in den Kapiteln 2.7 „vorbeugende Maßnahmen“, 7 „Kontrollmaßnahme“ sowie 8 „Un-veränderliche Datensicherung“ und 10 „Backup und Datensicherung“ beschrieben werden. Darüber hinaus enthalten die Arbeitsanweisungen in den entsprechenden Kapiteln zusätzlich Anweisungen, die zur Wahrung der Datenintegrität zu befolgen sind.

Zur Gewährleistung der Programmidentität ist der Entwicklungsprozess in den Kapiteln 5.3 „Individuale Eigenentwicklung“ sowie 5.4 „Protokollierung zu Softwareveränderungen“ dokumentiert und erfordert an wesentlichen Schritten Freigaben durch die beteiligten Prozessverantwortlichen. Systemseitig erfolgt die Ablage der Funktionalitäten in Form von eigenständigen Dienstprogrammen, welche einer Versionskontrolle unterliegen. Eine Installation ist daher anhand der verwendeten und einsehbaren Programmversionen eindeutig identifizierbar. Die Versionskontrolle ist in einem geschützten Bereich online abrufbar und umfasst neben der Änderungsprotokollierung auch die Administrationsdokumentation.

Die zum ordnungsgemäßen Einsatz des Archivsystems notwendigen Arbeitsanweisungen sind ebenfalls integraler Bestandteil der Dokumentation. In den Kapiteln 2.5 „Notfallszenarien“ und 2.6 „Notfallplan“ sowie in Kapitel 4 „Überwachungs- und Kontrollmechanismen“, 12 „Dokumentation allgemein“ und 13 „Backup“ sind die zum Betrieb des Archivsystems notwendigen Anweisungen und Verfahrensweisen dokumentiert.

Ähnlich der Software unterliegt auch die Dokumentation dem Change Management und wird bei Änderungen entsprechend angepasst. Einige Teile der Dokumentation waren zum Prüfungszeitpunkt jedoch unvollständig.

Ergebnis

Die vorgelegte oder abrufbare Verfahrensdokumentation ist größtenteils vollständig, bildet die eingesetzten Verfahren und Systeme richtig ab und ist für einen sachverständigen Dritten in

angemessener Zeit nachvollziehbar. Sie ist in den von uns geprüften Teilen richtig, aktuell und umfasst in ihrer Gesamtheit die geforderte Betriebs- und Anwenderdokumentation.

Empfehlung

Die Dokumentation sollte an den entsprechenden Stellen vervollständigt werden. Wir empfehlen weiterhin, das vorgesehene Change Management diesbezüglich auch konsequent auf die Dokumentation anzuwenden.

Anlagen

Konfiguration der Hard- und Software

Server-Hardware

- Intel Celeron 775 mit 3 GHz
- 2048 MByte RAM
- SATA-Raid1 für Bootplatten mit Samsung HD160HJ
- SATA-Raid5 für Datenplatten mit Samsung HD500LJ 1,5TB
- Grafik Intel 945G Express
- Netzwerk Intel Pro 1000 und D-Link Gigabit
- Standard-Diskettenlaufwerk
- Standard-DVD-Laufwerk
- Anschlüsse ECP-Druckeranschluss, Serial COM, Firewire 400 und USB 2.0

Server-Software – Standardkomponenten der Archivlösung

- akascan in der Version 2.02 vom 4. Februar 2008
- azimprgt in der Version 1.02 vom 25. Februar 2008
- azup in der Version 1.00 vom 2. Februar 2008
- nstore in der Version 2.02 vom 28. November 2007
- udeltemp in der Version 2.01 vom 28. November 2007
- udsp in der Version 2.02 vom 30. November 2007
- uedit in der Version 2.02 vom 27. November 2007
- uestore in der Version 2.02 vom 27. November 2007
- ufile in der Version 2.02 vom 27. November 2007
- ugaps in der Version 2.02 vom 14. Januar 2008
- ugetdata in der Version 2.02 vom 27. November 2007
- ugetdoc in der Version 2.02 vom 2. Februar 2008
- ugetpool in der Version 2.02 vom 27. November 2007
- uhelp in der Version 1.00 vom 15. Februar 2008
- uicmd in der Version 2.02 vom 15. April 2008

- uimpci in der Version 2.02 vom 27. November 2007
- uimpnci in der Version 2.01 vom 27. November 2007
- uinfo in der Version 2.02 vom 15. April 2008
- ulogin in der Version 2.02 vom 7. April 2008
- ulstpool in der Version 2.02 vom 27. November 2007
- umore in der Version 2.02 vom 11. April 2008
- undx in der Version 2.02 vom 16. April 2008
- upass in der Version 2.02 vom 27. November 2007
- upz in der Version 0.01 vom 28. April 2008
- uquery in der Version 2.02 vom 29. Januar 2008
- usrlst in der Version 2.02 vom 27. November 2007
- uucmd in der Version 2.02 vom 27. November 2007
- uuser in der Version 2.02 vom 28. November 2007

Server-Software – Betriebssystem-, Hilfs- und Administrationssoftware

- Microsoft Windows XP, Service Pack 3 mit Internet Explorer 7.0
- Microsoft .NET Framework 2 und 3
- Microsoft Resource Kit Tools
- Microsoft Excel und Word Viewer
- Apache HTTP Server v2.0.63
- Apache Webserver v2.0.59 für Win32 mit OpenSSL v0.9.7m
- Areca RAID Manager v1.20
- Intel Matrix Storage Manager v5.1
- Mozilla Firefox v2.0.0.14
- Mozilla Thunderbird v2.0.0.14
- Trend Micro OfficeScan Client v8.7
- 7-Zip v4.42
- Adobe Reader v8.1
- GnuPG 1.41

- PSPad Editor 4.5.2
- VNC 4.1.2

Client-Hardware

- Intel Dual Core mit 3 GHz
- 2048 MByte RAM
- HDD Samsung SP1654N mit 160 GB
- Grafik Nvidia FX 5500
- Netzwerk SIS 900 OnBoard Gigabit
- Anschlüsse: ECP-Druckeranschluss, Serial COM, Firewire 400 und USB 2.0
- Standard-Diskettenlaufwerk
- Standard-DVD-Laufwerk

Client-Software

- Microsoft Windows XP Professional, Service Pack 2 mit Internet Explorer 7.0
- Microsoft .NET-Framework 2 und 3
- Microsoft Resource Kit Tools
- Microsoft Office 2003 SP3
- Adobe Reader 8.1
- Mozilla Firefox 2.0.0.14
- 7-Zip 4.42
- GnuPG 1.41
- PSPad Editor 4.5.2
- VNC 4.1.2
- Trend Micro OfficeScan Client 8.7

Anlage 2

Allgemeine Auftragsbedingungen

Allgemeine Auftragsbedingungen

für

Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften

vom 1. Januar 2002

1. Geltungsbereich

(1) Die Auftragsbedingungen gelten für die Verträge zwischen Wirtschaftsprüfern oder Wirtschaftsprüfungsgesellschaften (im nachstehenden zusammenfassend „Wirtschaftsprüfer" genannt) und ihren Auftraggebern über Prüfungen, Beratungen und sonstige Aufträge, soweit nicht etwas anderes ausdrücklich schriftlich vereinbart oder gesetzlich zwingend vorgeschrieben ist.

(2) Werden im Einzelfall ausnahmsweise vertragliche Beziehungen auch zwischen dem Wirtschaftsprüfer und anderen Personen als dem Auftraggeber begründet, so gelten auch gegenüber solchen Dritten die Bestimmungen der nachstehenden Nr. 9.

2. Umfang und Ausführung des Auftrages

(1) Gegenstand des Auftrages ist die vereinbarte Leistung, nicht ein bestimmter wirtschaftlicher Erfolg. Der Auftrag wird nach den Grundsätzen ordnungsmäßiger Berufsausübung ausgeführt. Der Wirtschaftsprüfer ist berechtigt, sich zur Durchführung des Auftrages sachverständiger Personen zu bedienen.

(2) Die Berücksichtigung ausländischen Rechts bedarf – außer bei betriebswirtschaftlichen Prüfungen – der ausdrücklichen schriftlichen Vereinbarung.

(3) Der Auftrag erstreckt sich, soweit er nicht darauf gerichtet ist, nicht auf die Prüfung der Frage, ob die Vorschriften des Steuerrechts oder Sondervorschriften, wie z. B. die Vorschriften des Preis-, Wettbewerbsbeschränkungs- und Bewirtschaftungsrechts beachtet sind; das gleiche gilt für die Feststellung, ob Subventionen, Zulagen oder sonstige Vergünstigungen in Anspruch genommen werden können. Die Ausführung eines Auftrages umfaßt nur dann Prüfungshandlungen, die gezielt auf die Aufdeckung von Buchfälschungen und sonstigen Unregelmäßigkeiten gerichtet sind, wenn sich bei der Durchführung von Prüfungen dazu ein Anlaß ergibt oder dies ausdrücklich schriftlich vereinbart ist.

(4) Ändert sich die Rechtslage nach Abgabe der abschließenden beruflichen Äußerung, so ist der Wirtschaftsprüfer nicht verpflichtet, den Auftraggeber auf Änderungen oder sich daraus ergebende Folgerungen hinzuweisen.

3. Aufklärungspflicht des Auftraggebers

(1) Der Auftraggeber hat dafür zu sorgen, daß dem Wirtschaftsprüfer auch ohne dessen besondere Aufforderung alle für die Ausführung des Auftrages notwendigen Unterlagen rechtzeitig vorgelegt werden und ihm von allen Vorgängen und Umständen Kenntnis gegeben wird, die für die Ausführung des Auftrages von Bedeutung sein können. Dies gilt auch für die Unterlagen, Vorgänge und Umstände, die erst während der Tätigkeit des Wirtschaftsprüfers bekannt werden.

(2) Auf Verlangen des Wirtschaftsprüfers hat der Auftraggeber die Vollständigkeit der vorgelegten Unterlagen und der gegebenen Auskünfte und Erklärungen in einer vom Wirtschaftsprüfer formulierten schriftlichen Erklärung zu bestätigen.

4. Sicherung der Unabhängigkeit

Der Auftraggeber steht dafür ein, daß alles unterlassen wird, was die Unabhängigkeit der Mitarbeiter des Wirtschaftsprüfers gefährden könnte. Dies gilt insbesondere für Angebote auf Anstellung und für Angebote, Aufträge auf eigene Rechnung zu übernehmen.

5. Berichterstattung und mündliche Auskünfte

Hat der Wirtschaftsprüfer die Ergebnisse seiner Tätigkeit schriftlich darzustellen, so ist nur die schriftliche Darstellung maßgebend. Bei Prüfungsaufträgen wird der Bericht, soweit nichts anderes vereinbart ist, schriftlich erstattet. Mündliche Erklärungen und Auskünfte von Mitarbeitern des Wirtschaftsprüfers außerhalb des erteilten Auftrages sind stets unverbindlich.

6. Schutz des geistigen Eigentums des Wirtschaftsprüfers

Der Auftraggeber steht dafür ein, daß die im Rahmen des Auftrages vom Wirtschaftsprüfer gefertigten Gutachten, Organisationspläne, Entwürfe, Zeichnungen, Aufstellungen und Berechnungen, insbesondere Massen- und Kostenberechnungen, nur für seine eigenen Zwecke verwendet werden.

7. Weitergabe einer beruflichen Äußerung des Wirtschaftsprüfers

(1) Die Weitergabe beruflicher Äußerungen des Wirtschaftsprüfers (Berichte, Gutachten und dgl.) an einen Dritten bedarf der schriftlichen Zustimmung des Wirtschaftsprüfers, soweit sich nicht bereits aus dem Auftragsinhalt die Einwilligung zur Weitergabe an einen bestimmten Dritten ergibt.

Gegenüber einem Dritten haftet der Wirtschaftsprüfer (im Rahmen von Nr. 9) nur, wenn die Voraussetzungen des Satzes 1 gegeben sind.

(2) Die Verwendung beruflicher Äußerungen des Wirtschaftsprüfers zu Werbezwecken ist unzulässig; ein Verstoß berechtigt den Wirtschaftsprüfer zur fristlosen Kündigung aller noch nicht durchgeführten Aufträge des Auftraggebers.

8. Mängelbeseitigung

(1) Bei etwaigen Mängeln hat der Auftraggeber Anspruch auf Nacherfüllung durch den Wirtschaftsprüfer. Nur bei Fehlschlagen der Nacherfüllung kann er auch Herabsetzung der Vergütung oder Rückgängigmachung des Vertrages verlangen; ist der Auftrag von einem Kaufmann im Rahmen seines Handelsgewerbes, einer juristischen Person des öffentlichen Rechts oder von einem öffentlich-rechtlichen Sondervermögen erteilt worden, so kann der Auftraggeber die Rückgängigmachung des Vertrages nur verlangen, wenn die erbrachte Leistung wegen Fehlschlagens der Nacherfüllung für ihn ohne Interesse ist. Soweit darüber hinaus Schadensersatzansprüche bestehen, gilt Nr. 9.

(2) Der Anspruch auf Beseitigung von Mängeln muß vom Auftraggeber unverzüglich schriftlich geltend gemacht werden. Ansprüche nach Abs. 1, die nicht auf einer vorsätzlichen Handlung beruhen, verjähren nach Ablauf eines Jahres ab dem gesetzlichen Verjährungsbeginn.

(3) Offenbare Unrichtigkeiten, wie z. B. Schreibfehler, Rechenfehler und formelle Mängel, die in einer beruflichen Äußerung (Bericht, Gutachten und dgl.) des Wirtschaftsprüfers enthalten sind, können jederzeit vom Wirtschaftsprüfer auch Dritten gegenüber berichtigt werden. Unrichtigkeiten, die geeignet sind, in der beruflichen Äußerung des Wirtschaftsprüfers enthaltene Ergebnisse in Frage zu stellen, berechtigen diesen, die Äußerung auch Dritten gegenüber zurückzunehmen. In den vorgenannten Fällen ist der Auftraggeber vom Wirtschaftsprüfer tunlichst vorher zu hören.

9. Haftung

(1) Für gesetzlich vorgeschriebene Prüfungen gilt die Haftungsbeschränkung des § 323 Abs. 2 HGB.

(2) Haftung bei Fahrlässigkeit, Einzelner Schadensfall

Falls weder Abs. 1 eingreift noch eine Regelung im Einzelfall besteht, ist die Haftung des Wirtschaftsprüfers für Schadensersatzansprüche jeder Art, mit Ausnahme von Schäden aus der Verletzung von Leben, Körper und Gesundheit, bei einem fahrlässig verursachten einzelnen Schadensfall gem. § 54 a Abs. 1 Nr. 2 WPO auf 4 Mio. € beschränkt; dies gilt auch dann, wenn eine Haftung gegenüber einer anderen Person als dem Auftraggeber begründet sein sollte. Ein einzelner Schadensfall ist auch bezüglich eines aus mehreren Pflichtverletzungen stammenden einheitlichen Schadens gegeben. Der einzelne Schadensfall umfaßt sämtliche Folgen einer Pflichtverletzung ohne Rücksicht darauf, ob Schäden in einem oder in mehreren aufeinanderfolgenden Jahren entstanden sind. Dabei gilt mehrfaches auf gleicher oder gleichartiger Fehlerquelle beruhendes Tun oder Unterlassen als einheitliche Pflichtverletzung, wenn die betreffenden Angelegenheiten miteinander in rechtlichem oder wirtschaftlichem Zusammenhang stehen. In diesem Fall kann der Wirtschaftsprüfer nur bis zur Höhe von 5 Mio. € in Anspruch genommen werden. Die Begrenzung auf das Fünffache der Mindestversicherungssumme gilt nicht bei gesetzlich vorgeschriebenen Pflichtprüfungen.

(3) Ausschlußfristen

Ein Schadensersatzanspruch kann nur innerhalb einer Ausschlußfrist von einem Jahr geltend gemacht werden, nachdem der Anspruchsberechtigte von dem Schaden und von dem anspruchsbegründenden Ereignis Kenntnis erlangt hat, spätestens aber innerhalb von 5 Jahren nach dem anspruchsbegründenden Ereignis. Der Anspruch erlischt, wenn nicht innerhalb einer Frist von sechs Monaten seit der schriftlichen Ablehnung der Ersatzleistung Klage erhoben wird und der Auftraggeber auf diese Folge hingewiesen wurde.

Das Recht, die Einrede der Verjährung geltend zu machen, bleibt unberührt. Die Sätze 1 bis 3 gelten auch bei gesetzlich vorgeschriebenen Prüfungen mit gesetzlicher Haftungsbeschränkung.

52001 KND
1/2002

10. Ergänzende Bestimmungen für Prüfungsaufträge

(1) Eine nachträgliche Änderung oder Kürzung des durch den Wirtschaftsprüfer geprüften und mit einem Bestätigungsvermerk versehenen Abschlusses oder Lageberichts bedarf, auch wenn eine Veröffentlichung nicht stattfindet, der schriftlichen Einwilligung des Wirtschaftsprüfers. Hat der Wirtschaftsprüfer einen Bestätigungsvermerk nicht erteilt, so ist ein Hinweis auf die durch den Wirtschaftsprüfer durchgeführte Prüfung im Lagebericht oder an anderer für die Öffentlichkeit bestimmter Stelle nur mit schriftlicher Einwilligung des Wirtschaftsprüfers und mit dem von ihm genehmigten Wortlaut zulässig.

(2) Widerruft der Wirtschaftsprüfer den Bestätigungsvermerk, so darf der Bestätigungsvermerk nicht weiterverwendet werden. Hat der Auftraggeber den Bestätigungsvermerk bereits verwendet, so hat er auf Verlangen des Wirtschaftsprüfers den Widerruf bekanntzugeben.

(3) Der Auftraggeber hat Anspruch auf fünf Berichtsausfertigungen. Weitere Ausfertigungen werden besonders in Rechnung gestellt.

11. Ergänzende Bestimmungen für Hilfeleistung in Steuersachen

(1) Der Wirtschaftsprüfer ist berechtigt, sowohl bei der Beratung in steuerlichen Einzelfragen als auch im Falle der Dauerberatung die vom Auftraggeber genannten Tatsachen, insbesondere Zahlenangaben, als richtig und vollständig zugrunde zu legen; dies gilt auch für Buchführungsaufträge. Er hat jedoch den Auftraggeber auf von ihm festgestellte Unrichtigkeiten hinzuweisen.

(2) Der Steuerberatungsauftrag umfaßt nicht die zur Wahrung von Fristen erforderlichen Handlungen, es sei denn, daß der Wirtschaftsprüfer hierzu ausdrücklich den Auftrag übernommen hat. In diesem Falle hat der Auftraggeber dem Wirtschaftsprüfer alle für die Wahrung von Fristen wesentlichen Unterlagen, insbesondere Steuerbescheide, so rechtzeitig vorzulegen, daß dem Wirtschaftsprüfer eine angemessene Bearbeitungszeit zur Verfügung steht.

(3) Mangels einer anderweitigen schriftlichen Vereinbarung umfaßt die laufende Steuerberatung folgende, in die Vertragsdauer fallenden Tätigkeiten:

a) Ausarbeitung der Jahressteuererklärungen für die Einkommensteuer, Körperschaftsteuer und Gewerbesteuer sowie der Vermögensteuererklärungen, und zwar auf Grund der vom Auftraggeber vorzulegenden Jahresabschlüsse und sonstiger, für die Besteuerung erforderlicher Aufstellungen und Nachweise

b) Nachprüfung von Steuerbescheiden zu den unter a) genannten Steuern

c) Verhandlungen mit den Finanzbehörden im Zusammenhang mit den unter a) und b) genannten Erklärungen und Bescheiden

d) Mitwirkung bei Betriebsprüfungen und Auswertung der Ergebnisse von Betriebsprüfungen hinsichtlich der unter a) genannten Steuern

e) Mitwirkung in Einspruchs- und Beschwerdeverfahren hinsichtlich der unter a) genannten Steuern.

Der Wirtschaftsprüfer berücksichtigt bei den vorgenannten Aufgaben die wesentliche veröffentlichte Rechtsprechung und Verwaltungsauffassung.

(4) Erhält der Wirtschaftsprüfer für die laufende Steuerberatung ein Pauschalhonorar, so sind mangels anderweitiger schriftlicher Vereinbarungen die unter Abs. 3 d) und e) genannten Tätigkeiten gesondert zu honorieren.

(5) Die Bearbeitung besonderer Einzelfragen der Einkommensteuer, Körperschaftsteuer, Gewerbesteuer, Einheitsbewertung und Vermögensteuer sowie aller Fragen der Umsatzsteuer, Lohnsteuer, sonstigen Steuern und Abgaben erfolgt auf Grund eines besonderen Auftrages. Dies gilt auch für

a) die Bearbeitung einmalig anfallender Steuerangelegenheiten, z. B. auf dem Gebiet der Erbschaftsteuer, Kapitalverkehrsteuer, Grunderwerbsteuer,

b) die Mitwirkung und Vertretung in Verfahren vor den Gerichten der Finanz- und der Verwaltungsgerichtsbarkeit sowie in Steuerstrafsachen und

c) die beratende und gutachtliche Tätigkeit im Zusammenhang mit Umwandlung, Verschmelzung, Kapitalerhöhung und -herabsetzung, Sanierung, Eintritt und Ausscheiden eines Gesellschafters, Betriebsveräußerung, Liquidation und dergleichen.

(6) Soweit auch die Ausarbeitung der Umsatzsteuerjahreserklärung als zusätzliche Tätigkeit übernommen wird, gehört dazu nicht die Überprüfung etwaiger besonderer buchmäßiger Voraussetzungen sowie die Frage, ob alle in Betracht kommenden umsatzsteuerrechtlichen Vergünstigungen wahrgenommen worden sind. Eine Gewähr für die vollständige Erfassung der Unterlagen zur Geltendmachung des Vorsteuerabzuges wird nicht übernommen.

12. Schweigepflicht gegenüber Dritten, Datenschutz

(1) Der Wirtschaftsprüfer ist nach Maßgabe der Gesetze verpflichtet, über alle Tatsachen, die ihm im Zusammenhang mit seiner Tätigkeit für den Auftraggeber bekannt werden, Stillschweigen zu bewahren, gleichviel, ob es sich dabei um den Auftraggeber selbst oder dessen Geschäftsverbindungen handelt, es sei denn, daß der Auftraggeber ihn von dieser Schweigepflicht entbindet.

(2) Der Wirtschaftsprüfer darf Berichte, Gutachten und sonstige schriftliche Äußerungen über die Ergebnisse seiner Tätigkeit Dritten nur mit Einwilligung des Auftraggebers aushändigen.

(3) Der Wirtschaftsprüfer ist befugt, ihm anvertraute personenbezogene Daten im Rahmen der Zweckbestimmung des Auftraggebers zu verarbeiten oder durch Dritte verarbeiten zu lassen.

13. Annahmeverzug und unterlassene Mitwirkung des Auftraggebers

Kommt der Auftraggeber mit der Annahme der vom Wirtschaftsprüfer angebotenen Leistung in Verzug oder unterläßt der Auftraggeber eine ihm nach Nr. 3 oder sonstwie obliegende Mitwirkung, so ist der Wirtschaftsprüfer zur fristlosen Kündigung des Vertrages berechtigt. Unberührt bleibt der Anspruch des Wirtschaftsprüfers auf Ersatz der ihm durch den Verzug oder die unterlassene Mitwirkung des Auftraggebers entstandenen Mehraufwendungen sowie des verursachten Schadens, und zwar auch dann, wenn der Wirtschaftsprüfer von dem Kündigungsrecht keinen Gebrauch macht.

14. Vergütung

(1) Der Wirtschaftsprüfer hat neben seiner Gebühren- oder Honorarforderung Anspruch auf Erstattung seiner Auslagen; die Umsatzsteuer wird zusätzlich berechnet. Er kann angemessene Vorschüsse auf Vergütung und Auslagenersatz verlangen und die Auslieferung seiner Leistung von der vollen Befriedigung seiner Ansprüche abhängig machen. Mehrere Auftraggeber haften als Gesamtschuldner.

(2) Eine Aufrechnung gegen Forderungen des Wirtschaftsprüfers auf Vergütung und Auslagenersatz ist nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen zulässig.

15. Aufbewahrung und Herausgabe von Unterlagen

(1) Der Wirtschaftsprüfer bewahrt die im Zusammenhang mit der Erledigung eines Auftrages ihm übergebenen und von ihm selbst angefertigten Unterlagen sowie den über den Auftrag geführten Schriftwechsel zehn Jahre auf.

(2) Nach Befriedigung seiner Ansprüche aus dem Auftrag hat der Wirtschaftsprüfer auf Verlangen des Auftraggebers alle Unterlagen herauszugeben, die er aus Anlaß seiner Tätigkeit für den Auftrag von diesem oder für diesen erhalten hat. Dies gilt jedoch nicht für den Schriftwechsel zwischen dem Wirtschaftsprüfer und seinem Auftraggeber und für die Schriftstücke, die dieser bereits in Urschrift oder Abschrift besitzt. Der Wirtschaftsprüfer kann von Unterlagen, die er an den Auftraggeber zurückgibt, Abschriften oder Fotokopien anfertigen und zurückbehalten.

16. Anzuwendendes Recht

Für den Auftrag, seine Durchführung und die sich hieraus ergebenden Ansprüche gilt nur deutsches Recht.