

Neben Empfehlungen, wie die Drucker, Druckserver, Dokumentenscanner, Kopierer und Multifunktionsgeräte geschützt werden können, werden auch Vorgehensweisen zum Umgang mit diesen Geräten und damit verarbeiteten schützenswerten Dokumenten vorgestellt.

Wie wichtig Sicherheitsmaßnahmen beim Austausch von Datenträgern sind, haben die Meldungen aus Großbritannien gezeigt, wo mehrfach Datenträger mit Millionen sensibler Daten von Bürgern beim Versand verschwunden sind. Im Baustein B 5.2 Datenträgeraustausch werden die Schutzvorkehrungen beschrieben, die beim Austausch von Datenträgern umzusetzen sind. Dazu gehört nicht nur die Auswahl verlässlicher Transportwege und einer geeigneten Versandart, sondern auch der Schutz durch Verschlüsselung und Digitale Signaturen.

Beim Datenträgeraustausch werden häufig CD-ROMs, DVDs oder Magnetbänder benutzt. Die Bandbreite mobiler Datenträger ist aber mittlerweile riesig geworden, hierzu gehören beispielsweise neben USB-Sticks auch Handys, MP3-Player und Digitalkameras. Es gibt aber auch Armbanduhr, Kugelschreiber und Spielzeug mit integriertem Speicher. Jeder mobile Datenträger ist aber potentiell dafür geeignet, Informationen von IT-Systemen einer Institution unbemerkt aufzunehmen. Genauso könnten über diese aber auch Computer-Viren und andere Schadsoftware weitergegeben werden. Es zeigt sich immer wieder, dass durch diese Vielzahl an Formen und Einsatzgebieten nicht immer alle Arten von mobilen Datenträgern als solche wahrgenommen und somit auch nicht alle erforderlichen Sicherheitsbetrachtungen vorgenommen werden.

Darüber hinaus wurden zahlreiche Gefährdungen und Maßnahmen an neue technische Entwicklungen, neue Bedrohungsszenarien und neue Entwicklungen in der IT-Sicherheit angepasst. Neu aufgenommen wurden beispielsweise Sicherheitsempfehlungen zu den Themen Speicherbeschränkungen (Quotas), Man-in-the-Middle-Angriffen, Zurücksetzen von Passwörtern sowie Auswahl und Nutzung von Passwort-Speicher-Tools.

Workshops

Papierlose Beweismittel in Streitfällen vor Gericht, Teil II

Rechtssichere Erfassung elektronischer Daten wird immer wichtiger

Judith Balfanz, AuthentiDate International AG, Frank Zscheile, SAPERION AG

Durch den Einsatz elektronischer Workflow- und Dokumenten Management Systeme (DMS) lassen sich bisher papiergestützte Vorgänge wesentlich schneller, sicherer und effektiver abwickeln. Im Zuge des globalen Austausches digitaler Informationen spielt aber auch die Rechtssicherheit solcher Vorgänge eine immer wichtigere Rolle. Im zweiten Teil der Workshop-Reihe geht es um den Einsatz von qualifizierten Zeitstempeln und personenbezogenen Signaturen.

Greift man das Beispiel der Reklamationsbearbeitung aus dem ersten Teil auf, so lässt sich hier gut verdeutlichen, dass für bestimmte betriebswirtschaftliche Prozesse der kombinierte Einsatz von personenbezogenen Signaturen und Zeitstem-

IT-Grundschutz-Kataloge

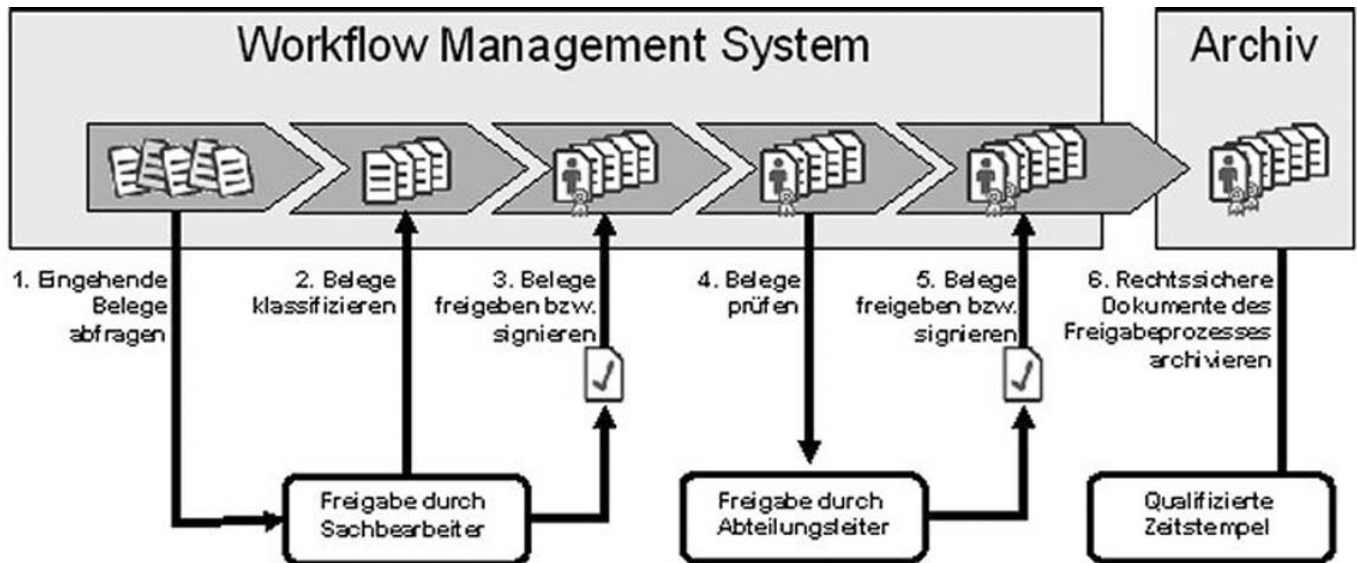
Das Grundwerk (Loseblattsammlung) umfasst rund 3800 Seiten in 4 Ordnern, mit CD-ROM.

ISBN 978-3-88784-915-3

Preis: 152,00 EUR

Der Preis der 9. Ergänzungslieferung liegt bei 93,80 EUR.

peln im Workflow sinnvoll oder sogar erforderlich ist. Ist ein externes Unternehmen beispielsweise mit der Bearbeitung der Reklamation beauftragt, so wird dies verlangen, dass im Prozess nachgewiesen wird, wer die Bearbeitung der Reklamation beauf-



Prozessablauf rechtssicheres Dokumentenmanagement

trägt hat. Insbesondere in IT-Projekten, in denen häufig eine Vielzahl von Projektbeteiligten involviert ist, tritt dieses Problem auf. Exakt auf diese Anforderung sollte ein Workflow System bei der Bereitstellung von Signaturfunktionalitäten eingehen. Zusätzlich zu qualifizierten Zeitstempeln müssen hier qualifizierte personenbezogene Signaturen zum Einsatz kommen, die nachweisen, wer den Vorgang bearbeitet hat. Je nach Anforderung genügt es dabei, teils personenbezogene Signaturen derart zentral innerhalb des Workflow-Systems zu integrieren, dass die Signatur eine gesamte Abteilung repräsentiert. Grundsätzlich können Signaturen nur von natürlichen Personen erstellt werden, d.h. es können keine „Abteilungssignaturkarten oder Firmensignaturkarten“ eingesetzt werden. Das Signaturgesetz sieht jedoch Pseudonyme, bzw. Attribute vor, welche die Nutzung der Signaturkarte einer natürlichen Person für den zentralen Einsatz für zum Beispiel eine gesamte Abteilung ermöglichen. Aufgrund dieser Erweiterung kann im Beispiel der Reklamation jede Dokumenten-Änderung mit

einem qualifizierten Zeitstempel und einer qualifizierten personenbezogenen Signatur zentral und automatisch versehen werden. Somit ist rechtssicher belegt, welche Abteilung, Projektgruppe oder Firma die Bearbeitung zu welchem Zeitpunkt und in welcher Form vorgenommen hat.

■ Einsatz von qualifizierten Zeitstempeln und personenbezogenen Signaturen für klar definierte natürliche Personen zur rechtssicheren Freigabe von Dokumenten

Schließlich müssen bei den Überlegungen zur Signaturintegration auch derartige Workflow-Prozesse einbezogen werden, bei denen bislang eine Abwicklung in Papierform erforderlich war, um die rechtssichere Freigabe (Genehmigung), einer einzelnen explizit benennbaren natürlichen Person zu dokumentieren. An dieser Stelle ist der Einsatz einer weiteren kombinierten Signaturlösung anzuraten – der zentrale Einsatz von qualifizierten Zeitstempeln zur Dokumentation, wann bestimmte Daten

genehmigt wurden und der additive Einsatz von Client-Komponenten.

Diese sollten derart eingebunden werden, dass die Mitarbeiter, die die Genehmigungen erteilen sollen, automatisch über die Konfiguration im Regelwerk die relevanten elektronischen Dokumente auf ihrem Arbeitsplatzrechner angezeigt bekommen. Dort werden die Dokumente mittels qualifizierter personenbezogener Signatur freigegeben und ebenfalls automatisch dem nächsten Workflow-Bearbeitungsschritt zugeführt. Parallel kann dabei auch die automatische Archivierung des signierten Dokumentes sinnvoll sein.

Zur automatischen Bearbeitung typischer Geschäftsvorgänge wie etwa Reisekostenabrechnungen sind im Dokumenten Management System Komponenten für dokumentenbasierten Workflow standardmäßig integriert. Dokumentensignierung und -weiterleitung, Remindingfunktionen etc. laufen damit auf Basis vorgenerierter Prozesse.