ADV mitteilungen
DER ARBEITSGEMEINSCHAFT FÜR DATENVERARBEITUNG

2002 – Ausgabe Nr. 6 Auflage: 2000 Exemplare

Neue Anforderungen an das IT-Management – Lösungen durch Qualifizierung

Der Trend zur Informations- und Wissensgesellschaft ist unaufhaltsam. Dies hat zur Folge, dass die Informations- und Kommunikationstechnologie auch weiterhin eine hohe und steigende Bedeutung für Wirtschaft und Verwaltung haben wird. So werden Produktion, Handel und Dienstleistungen immer mehr von der effizienten Nutzung moderner Informations- und Kommunikationstechnologien abhängig.

Nach wie vor unterliegt auch der Veränderungsbedarf im IT-Bereich einer steigenden Dynamik, die durch die Vielzahl von technischen Möglichkeiten und den steigenden Anforderungen der Anwender noch verschärft wird. All diese Entwicklungen und Rahmenbedingungen machen ein qualifiziertes IT-Management erforderlich, das auf den aktuellen Stand der Informationstechnologie sowie der jeweiligen Organisation in der Lage ist, die erforderlichen Entscheidungen im IT-Bereich effizient und kostenoptimal treffen zu können und daraufhin eine zielgerichtete Umsetzung erfolgreich einzuleiten.

Die Arbeit des Funktionsbereichs IT ist zu einem großen Teil durch das Arbeiten in Projekten gekennzeichnet. Oft müssen eine Vielzahl von Projekten gleichzeitig realisiert werden. IT-Projekte – gleich welcher Art – können aber nur dann erfolgreich abgewickelt werden, wenn ein entsprechendes Projektmanagement und geeignete Rahmenbedingungen vorhanden sind.

Notwendig dazu ist, dass das IT-Management die für ein erfolgreiches Projektmanagement erforderlichen Methoden, Techniken, Vorgehensweisen und Hilfsmittel kennt und beherrscht. Dazu zählen Konzepte und Verfahren für das Erarbeiten von Projektvisionen und Projektanträgen, Projektplanungstechniken sowie die eigentliche Durchführung der Projektarbeit. Aber nicht nur methodisches Know-How ist wichtig; auch soziale Kompetenzen sind für eine erfolgreiche Projektarbeit unverzichtbar (Führungsaufgaben, Teamarbeit etc.). Hinzu kommen neue Herausforderungen im IT-Projektmanagement; beispielhaft seien das Projekt-Risikomanagement, Claim-Management, Change-Management sowie Qualitätsmanagement in IT-Projekten genannt.

Obwohl einzelne technische Komponenten billiger werden, ist aber auch eine steigende Kostentendenz bei IT-Projekten insgesamt zu beobachten. Die Führung von IT-Bereichen ist daher damit konfrontiert, komplexere Aufgaben in kürzerer Zeit unter Beachtung von

Teilnehmer des IT-Manager-Lehrgangs 2002 bei der Zertifizierungsfeier

Aus dem Inhalt

www.softwarequalitaet.at

strengen Wirtschaftlichkeitsvorgaben wahrnehmen zu müssen. Eine effiziente Erfüllung dieser Aufgaben setzt einen aktuellen Stand bei den Kenntnissen in den wichtigsten Themenbereichen des IT-Managements voraus. Dies sind die aktuellen Bedingungen und Möglichkeiten der Informations- und Kommunikationstechnologie, Rahmenbedingungen für die Entwicklung und Auswahl von Software sowie Fragen der Führung und Personalentwicklung von Mitarbeitern im IT-Bereich.

Die zunehmenden Kosten des Einsatzes moderner Informations- und Kommunikationstechnologien in Unternehmungen aber auch die erweiterten strategischen Nutzungsmöglichkeiten der Neuen Technologien werden in der Praxis intensiv diskutiert. Schlagworte wie „Total Cost of Ownership (TCO)“, „Erfolgsfaktor IT“, „Balanced Scorecard in der IT“ sowie der Trend der IT-Abteilung zum Service- und Profitcenter machen die Runde und verlangen nach umsetzbaren Lösungen.

Das steigende Bedürfnis, den Erfolg des Einsatzes moderner Informations- und Kommunikationslösungen zu überwachen, verstärkt außerdem den Wunsch nach einem effizienten Controlling der Informationsverarbeitung im Unternehmen. Deshalb sollte das IT-Management auch die dazu notwendigen Methoden und Instrumente kennen und anwenden. Dazu zählen beispielweise

- Methoden und Vorgehensweisen zur Kostenermittlung in der IT
- Instrumente zur Erstellung von IT-Leistungskatalogen sowie zur Definition von IT-Leistungen (beispielsweise SLAs)
- Möglichkeiten einer internen Verrechnung von IT-Kosten und Leistungen
- Sachgerechte Entscheidung über IT-Outsourcing-Optionen
- Kennzahlen zur Steuerung der Wirtschaftlichkeit und Qualität der IT sowie
- Instrumente für ein umfassendes operatives und strategisches IT-Controlling.

Um den Anforderungen an ein modernes IT-Management gerecht zu werden, bietet die ADV bereits seit mehreren Jahren eine umfassende Ausbildung zum **„Zertifizierten IT-Manager“** an. Dieser Lehrgang kann mit einer Abschlussprüfung/Präsentation abgeschlossen werden. Im Oktober 2002 fand die letzte Zertifizierungsprüfung statt, an der wieder zahlreiche Lehrgangsabsolventen mit gutem bzw. sehr gutem Erfolg teilgenommen haben.
Für das Jahr 2003 wird ein weiterer Lehrgang zum IT-Manager von der ADV angeboten. Das Ziel dieses Lehrganges ist es, den Teilnehmern in kompakter Form den aktuellen Stand des Wissens in den wichtigsten Schwerpunktthemen des IT-Managements zu vermitteln. Insbesonders sollen die Teilnehmer bzw. die Teilnehmerinnen ausgehend von vorhandenem Basiswissen und Erfahrungen im IT-Bereich in die Lage versetzt werden,

- IT-Projekte zu definieren und als Projektleiter erfolgreich zu führen
- IT-Infrastrukturplanungen sowie Software-Einführungsentscheidungen methodengestützt vorzunehmen
- eine leistungsstarke IT-Organisation für eine Unternehmung/Behörde aufzubauen
- Methoden und Techniken für die tägliche Arbeit gezielt einzusetzen (z. B. Führungstechniken, Problemlösungs- und Moderationstechniken)
- IT-Strategiekonzepte zu entwickeln und ein effizientes IT-Controlling zu realisieren.

Ein besonderes Ziel des Lehrganges ist es auch, die Teilnehmer bei der Umsetzung des Erlernten im eigenen Arbeitsfeld gezielt zu unterstützen. Weitere Informationen zum Lehrgang finden Sie im Veranstaltungsprogramm der ADV sowie unter **www.it-manager.at**.

Dipl.-Hdl. Ing. Ernst Tiemeyer
(u. a. Lehrgangsleitung im IT-Manager-Lehrgang) und
Mag. Johann Kreuzeder
(Generalsekretär der ADV)

Gegen Viren, Würmer und Trojanische Pferde – Das Strafrechtsänderungsgesetz 2002

1. Einleitung

Erinnern Sie sich noch an „I Love You“, „Melissa“ und „Kurnikova“? Dabei handelt es sich nicht um innige Liebesworte und deren jeweilige Adressatinnen. Vielmehr sind dies die Namen der schädlichsten Viren der letzten Jahre, die weltweit auf tausenden PCs verbreitet wurden und Schäden in Höhe von mehreren 100 Millionen Euro verursacht haben.

Abgesehen von diesen weithin bekannten Viren finden jährlich zahlreiche Angriffe auf Informationssysteme statt, die von der Öffentlichkeit unbemerkt bleiben, teils weil die Eindringungsversuche von den Systemverwaltern und Nutzern selbst unbemerkt bleiben, teils weil viele Unternehmen Fälle von Computermissbrauch nicht bekannt geben, um einerseits ihr Image zu wahren, andererseits nicht ihre Anfälligkeit für weitere Angriffe preiszugeben. Die EU schätzt die Zahl dieser Angriffe auf 30.000 bis 40.000 pro Jahr in einem Mitgliedstaat. Der Kreis der Betroffenen umfasst dabei neben Betreibern elektronischer Kommunikationsnetze, Anbietern von Diensten oder Unternehmern, die elektronischen Geschäftsverkehr betreiben, auch traditionelle Bereiche wie das verarbeitende Gewerbe, den Dienstleistungssektor, öffentliche Einrichtungen und Regierungsstellen, aber auch Privatpersonen.

2. Angriffsformen

Die Formen, in denen diese Angriffe erfolgen, sind dabei ganz unterschiedlich. Die EU hat sie im wesentlichen in fünf Kategorien zusammengefasst. Danach bestehen Angriffe zunächst vor allem darin, dass sich ein Außenstehender unberechtigt Zugang zu einem Informationssystem verschafft, wie dies z.B. beim „Hacking" der Fall ist.

Angriffe können aber auch in Form einer Störung des Informationssystems erfolgen. So werden etwa beim „Denial of Service"-Angriff Webserver oder Anbieter von Internetdiensten mit automatisch erzeugten Nachrichten überlastet. Beim sogenannten „Spamming" werden massenweise Werbe-Mails versendet und dadurch der Mail-Server der jeweiligen Adressaten blockiert.

Weiters finden Angriffe auf Informationssysteme durch bösartige Software statt, die Daten verändern oder zerstören. Dies kann nicht nur durch Viren, wie die eingangs genannten, geschehen, sondern auch durch „Trojanischen Pferde" – auf den ersten Blick gutartige Programme, die aber per Aufruf bösartige Angriffe auslösen – sowie durch „Würmer" – Programme, die sich selbst kopieren und durch das häufige Kopieren letztendlich das gesamte System überschwemmen.

Schließlich stellen auch die Überwachung des Fernmeldeverkehrs sowie die Täuschung bzw. Irreführung des Benutzers durch Annahme der Identität einer anderen Person im Internet Attacken gegen Informationssysteme dar.

3. Maßnahmen auf internationaler Ebene

Auf internationaler Ebene wird nun versucht, derartigen Angriffen wirksam entgegenzutreten. Dabei wird auf der einen Seite versucht, die Entwicklung, die Verfügbarkeit und die tatsächliche Nutzung präventiver Technologien zu fördern. Zu denken ist dabei an Verschlüsselungstechniken und digitale Signaturen, neue Verfahren der Zugangskontrolle und Authentifizierung sowie verschiedene Softwarefilter, die den Informationsfluss auf sämtlichen Ebenen filtern und steuern, wie z.B. die Firewall, die Datenpakete prüft, Filter für bösartige Software, E-Mail-Filter, die unerwünschte Werbung herausfiltern, und der Browser, der den Zugang zu schädlichen Inhalten blockiert.

Auf der anderen Seite wird versucht, Angriffe auf Informationssysteme vermehrt auch rechtlich, insbesondere strafrechtlich zu erfassen. Jüngstes Ergebnis dieser Bemühungen ist die vom Europarat verabschiedete Cybercrime-Konvention (CC-K), die bisher von 26 Europaratsländern, darunter auch Österreich, sowie den USA, Kanada, Japan und Südafrika am 23.11.2001 in Budapest unterzeichnet wurde. Die CC-K umfasst vier Kategorien von materiellen Straftatbeständen, nämlich unerlaubte Angriffe auf Computersysteme, strafbare Handlungen mit Hilfe von Computersystemen, Verbreitung strafbarer Inhalte über Computersysteme und schließlich Urheberrechtsverletzungen. Daneben enthält sie Regelungen im Strafprozess- und Rechtshilfebereich.

4. Umsetzung in Österreich

In Österreich wurde die CC-K nun durch das Strafrechtsänderungsgesetz 2002 teilweise umgesetzt. Dabei beschränkte man sich zunächst auf die Regelung der computerspezifischen Straftaten, also die unerlaubten Angriffe auf Computersysteme und die strafbaren Handlungen mit Hilfe von Computersystemen. Hiefür wurden im Rahmen des Strafgesetzbuches (StGB) zum Teil neue Delikte geschaffen, zum Teil bestehende Strafbestimmungen angepasst.

Bisher bestanden nur zwei Computerdelikte im StGB, die durch das Strafrechtsänderungsgesetz 1987 eingefügt worden waren, nämlich die „Datenbeschädigung" gemäß § 126a StGB und der „Betrügerische Datenverarbeitungsmissbrauch" gemäß § 148a StGB. Durch die erstgenannte Bestimmung werden automationsunterstützt verarbeitete, übermittelte oder überlassene Daten vor einer Beschädigung durch Verändern, Löschen, Unbrauchbarmachen und Unterdrückung geschützt. In der letztgenannten Bestimmung wird bestraft, wer mit Bereicherungsabsicht das Ergebnis einer automationsunterstützten Datenverarbeitung beeinflusst und dadurch einen anderen am Vermögen schädigt.

Zu diesen beiden Bestimmungen sind nun insgesamt 5 neue Tatbestände hinzugetreten. Sie sind einheitlich mit Freiheitsstrafe bis zu 6 Monaten bzw. mit Geldstrafe bis zu 360 Tagessätzen bedroht.

4.1. Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)

§ 118a StGB, der sogenannte „Hackerparagraph", stellt die Verschaffung des Zugangs zu einem Computersystem (oder zu einem Teil eines solchen), über das der Täter nicht oder nicht allein verfügen darf, unter Strafe. Dies allerdings nur dann, wenn der widerrechtliche Zugriff unter Verletzung spezifischer Sicherheitsvorrichtungen stattfindet, die im Computersystem angebracht worden sind, um sicherzustellen, dass nur berechtigte Personen auf das System zugreifen, wie z.B. Computerpasswörter oder Zugangscodes. Werden nur „herkömmliche" Sicherungsmaßnahmen, wie eine versperrte Türe oder eine Alarmanlage, umgangen, so unterliegt dieser Zugriff nicht dem § 118a StGB. Weiters kommt es auf die Verletzung, nicht auf die bloße Überwindung der genannten Sicherheitsvorrichtungen an. Die unbefugte Verwendung eines fremden Passwortes, die ohne Eingriff in die Daten- und Sachsubstanz erfolgt, ist daher nicht von § 118a StGB erfasst.

Der widerrechtliche Zugriff ist zudem nur dann strafbar, wenn er mit besonderem Vorsatz begangen wird. Gefordert ist dabei sowohl die Absicht, sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen, als auch die Absicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, uzw. dadurch, dass der Täter die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht.

Mit dieser „doppelten" Absicht wollte der Gesetzgeber dem Umstand Rechnung tragen, dass § 118a nicht nur

Nachrichten oder (sonst) besonders schutzwürdige (etwa personenbezogene) Daten, sondern sämtliche Daten (vgl § 74 Abs 2 StGB) umfasst. Der Zugriff auf diese Daten sollte daher nur unter besonderen Umständen strafbar sein. Sichergestellt ist damit jedenfalls, dass Jugendliche, die allein aus dem Grund im Computersystem eindringen, um ihre Fähigkeiten und ihr Geschick zu erproben, ohne aber an den geschützten Daten selbst interessiert zu sein, straffrei bleiben.

4.2. Missbräuchliches Abfangen von Daten (§ 119a StGB)

Der nun angepasste § 119 und der neu eingefügte § 119a regeln allgemein formuliert das Abfangen von Informationen durch Benützung spezieller Vorrichtungen. Dabei geht es in § 119 um das Benützen einer Vorrichtung, die an einer Telekommunikationsanlage oder an einem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, zwecks Kenntnisnahme von auf diesem Weg übermittelten Nachrichten. In § 119a wird dagegen das Benützen einer Vorrichtung, die an einem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, sowie das Auffangen elektromagnetischer Abstrahlung eines Computersystems zwecks Kenntnisnahme von auf diesem Weg übermittelten Daten unter Strafe gestellt.

§ 119a unterscheidet sich von § 119 in zweifacher Hinsicht: Zum einen sind von dieser Bestimmung sämtliche Daten (außer Nachrichten, die § 119 vorbehalten bleiben) umfasst, weshalb die Strafbarkeit – wie in § 118a – an eine besondere Absicht geknüpft ist. Während in § 119 bereits die Absicht, sich oder einem anderen Unbefugten von der Nachricht Kenntnis zu verschaffen, für die Strafbarkeit der Handlung ausreicht, verlangt § 119a zusätzlich die Absicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, uzw. dadurch, dass der Täter die Daten selbst benützt, einem anderen für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht. Zum anderen enthält § 119a über § 119 hinausgehend einen weiteren Tatbestand, nämlich neben dem Benützen einer oben näher bezeichneten Vorrichtung auch das Auffangen der elektromagnetischen Abstrahlung eines Computers.

4.3. Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB)

Durch § 126b sollen vor allem jene Phänomene erfasst werden, die in den letzten Jahren immer häufiger komplette Computernetzwerke ausgeschaltet haben, wie Computerviren, Spamming und Trojaner. Im Gegensatz zu dem bereits durch das Strafrechtsänderungsgesetz 1987 eingefügten § 126a, der alle Formen von Datenbeschädigungen umfasst, kommt es für die Strafbarkeit nach § 126b allein auf eine schwere Störung der Funktionsfähigkeit des Computers an. Das bedeutet, dass nicht etwa jedes Spamming strafbar ist, sondern der Angriff einen entsprechenden Schweregrad erreichen muss. Ein schlichter Verstoß gegen das Spamming-Verbot ist weiterhin nur als Verwaltungsübertretung zu ahnden (§ 104 Abs. Z 24 TKG).

4.4. Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB)

Nach § 126c sind Handlungen strafbar, die der Vorbereitung der in den §§ 118a, 119, 119a, 126a oder 126b bezeichneten Delikte dienen. Zu bestrafen ist danach, wer 1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung der zuvor genannten Delikte geschaffen oder adaptiert worden ist; oder 2. ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen; herstellt, einführt, vertreibt, veräußert oder sonst zugänglich macht mit dem Vorsatz, dass diese Computerprogramme und Zugangsdaten zur Begehung einer der genannten strafbaren Handlungen gebraucht werden. Der bloße Besitz solcher Computerprogramme und Zugangsdaten wurde dagegen nicht unter Strafe gestellt.

Wie in den meisten Vorbereitungsdelikten ist auch in § 126c eine Regelung der „tätigen Reue“ enthalten. Demnach bleibt straffrei, wer freiwillig verhindert, dass die genannten Computerprogramme oder Zugangsdaten zu den an sich beabsichtigten kriminellen Zwecken benützt werden. Der Täter bleibt auch dann straffrei, wenn die Gefahr eines Gebrauchs gar nicht besteht oder sie ohne Zutun des Täters beseitigt worden ist, er sich aber in Unkenntnis dessen freiwillig und ernstlich bemüht hat, die Gefahr zu beseitigen.

4.5. Datenfälschung (§ 225a StGB)

Parallel zum Tatbestand der Urkundenfälschung des § 223 StGB wurde im neu geschaffenen § 225a der Tatbestand der „Datenfälschung“ eingefügt. Strafbar ist danach die Herstellung von falschen Daten – das sind Daten, die nicht von der Person stammen, die als Hersteller bzw. Aussteller angegeben ist – und die Verfälschung echter Daten – das sind bestehende Daten, die nachträglich durch Austausch der Angabe des Ausstellers oder durch einen anderen gedanklichen Inhalt geändert werden – durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten. Die Strafbarkeit ist an den Vorsatz geknüpft, dass diese manipulierten Daten im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden. § 225a StGB wird vor allem im Bereich der elektronischen Signatur und der elektronischen Urkunden Bedeutung erlangen.

Dem österreichischen Gesetzgeber bleibt nun noch, in einem weiteren Schritt die restlichen materiellen Bestimmungen der Cybercrime-Konvention umzusetzen. Mittlerweile ist der Europarat allerdings schon wieder tätig geworden: Das Zusatzprotokoll zur Bekämpfung des Rassenhasses im Internet wurde bereits in seiner dritten Version auf der Website des Europarates veröffentlicht. Ein weiteres Zusatzprotokoll, das den Kampf gegen den Terrorismus im Internet erleichtern soll, ist derzeit in Vorbereitung. Ob und inwieweit diese Maßnahmen tatsächlich geeignet sind, der Computerkriminalität wirksam zu begegnen, werden erst künftige Untersuchungen zeigen. In jedem Fall haben sie aber Signalwirkung: Computerstraftätern ist nunmehr der Kampf angesagt.

Kanzlei andréewitch & simon, wien
– office@andsim.at –

Österreich setzt Maßstäbe: Elektronische Rechnung, bitte warten!

An Rechnungen, auf der die Umsatzsteuer ausgewiesen ist und die daher Grundlage für Rückvergütung von Umsatzsteuer sein können, werden besondere Anforderungen gestellt.
Abgesehen von inhaltlichen Erfordernissen hat eine solche Rechnung bisher eine „Urkunde“ sein müssen. Da unser Urkundenbegriff an der Papierform festgemacht ist, konnte eine elektronisch übermittelte Rechnung daher nicht gegenüber dem Finanzamt geltend gemacht werden.

Die Anerkennung hätte schon ab Anfang 2000 mit dem Inkrafttreten des Signaturgesetzes und der damit bestehenden Möglichkeit der Verwendung einer sicheren elektronischen Signatur geschehen können – Möglicherweise hätte man damit die Durchsetzung der digitalen Signatur gefördert!
Tatsächlich kann man die Praxis der Finanzverwaltung, auch mit sicherer elektronischer Signatur versehene Rechnungen nicht papierschriftlichen Rechnungen gleichzustellen, als gesetzeswidrig qualifizieren. Denn der § 4 Signaturgesetz bestimmt:
„(1) Eine sichere elektronische Signatur erfüllt das rechtliche Erfordernis einer eigenhändigen Unterschrift, insbesondere der Schriftlichkeit im Sinne des § 886 ABGB, sofern durch Gesetz oder Parteienvereinbarung nicht anderes bestimmt ist.
(2) (…)
(3) Die Bestimmung des § 284 ZPO über die Vermutung der Echtheit des Inhalts einer unterschriebenen Privaturkunde ist auf elektronische Dokumente, die mit einer sicheren elektronischen Signatur versehen sind, anzuwenden.
(4) (…)“
Das Gesetz hat nichts anderes bestimmt, das Finanzministerium sagte aber trotzdem nein.

Die Verpflichtung der Anerkennung trifft Österreich auch vom Gemeinschaftsrecht. Artikel 5 Abs 1 der Richtlinie 1999/93/EG (Signaturrichtlinie) schreibt vor:
„Die Mitgliedstaaten tragen dafür Sorge, daß fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und die von einer sicheren Signaturerstellungseinheit erstellt werden,
a) die rechtlichen Anforderungen an eine Unterschrift in bezug auf in elektronischer Form vorliegende Daten in gleicher Weise erfüllen wie handschriftliche Unterschriften in bezug auf Daten, die auf Papier vorliegen, und
b) in Gerichtsverfahren als Beweismittel zugelassen sind.“

Die EU-Kommission wollte es anders: Sie veröffentlichte am 17. November 2000 einen Vorschlag zur Änderung der Richtlinie 77/388/EWG (6. Mehrwertsteuer-Richtlinie) mit dem Ziel der Vereinfachung, Modernisierung und Harmonisierung der mehrwertsteuerlichen Anforderungen an die Rechnungslegung[1]. Dieser Vorschlag sah vor, dass Rechnungen auf Papier **oder** auf elektronischem Wege übermittelt werden können. Die Echtheit der Herkunft und die Unversehrtheit des Inhalts ist durch eine „fortgeschrittene elektronische Signatur“ zu gewährleisten. Die Mitgliedsstaaten sollten den Steuerpflichtigen keine darüber hinausgehenden weiteren Pflichten oder Formalitäten in Bezug auf elektronisch übermittelte Rechnungen auferlegen.

Die Finanzverwaltung reagierte und veröffentlichte eine modernisierte Regelung für den elektronischen Rechnungsaustausch, die jedoch nicht von der Forderung des Vorliegens schriftlicher Abrechnungen in Papierform abgeht; es müssen zumindest schriftliche Sammelrechnungen vorliegen.[2]

Es ist aber beim Kommissionsvorschlag geblieben; die 6. Mehrwertssteuer-Richtlinie wurde bis dato nicht in diesem Sinne geändert.

Aber jetzt läßt frohe Kunde aufhorchen: Der Bundesgesetzgeber hat diesen Vorschlag dennoch umgesetzt! Bundesgesetzblatt I 132/2002 vom 13.8.2002 fügt unter anderem folgenden Passus in den Absatz 2 des § 11 UstG ein:

„Als Rechnung gilt auch eine auf elektronischem Weg übermittelte Rechnung, sofern der Empfänger zustimmt. Sie gilt nur unter der Voraussetzung als Rechnung, dass die Echtheit der Herkunft und die Unversehrtheit des Inhalts gewährleistet sind. Der Bundesminister für Finanzen bestimmt mit Verordnung die Anforderungen, bei deren Vorliegen diese Voraussetzungen erfüllt sind.“

Nicht so schnell, lieber noch Zeit gewinnen! Anstatt gleich die Verwendung der sicheren elektronischen Signatur vorzuschreiben, lassen wir über die Verordnungsermächtigung vorher noch den Finanzminister ran!

Natürlich wurde die dazu gehörige Verordnung des Finanzministers noch nicht erlassen und sie wird angesichts der politischen Situation auch noch länger auf sich warten lassen.

Wie es anders geht, zeigt die Bundesrepublik Deutschland, die mit Wirkung 1.1.2002 ihr Umsatzsteuergesetz um folgende Bestimmung ergänzt hat:
„Als Rechnung gilt auch eine mit einer qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung nach § 15 Abs. 1 des Signaturgesetzes versehene elektronische Abrechnung.“

Innovatives Österreich – Wir verhindern, so lange es geht!

Dipl.Ing DDr Walter J. Jaburek
Mag Ralf Blaha MAS
Beide EDV Concept Technisches Büro für Informatik GmbH

1 KOM (2000) 650 v. 17.11.2000.
2 Amtsblatt der Finanzverwaltung, Stück 128 vom 22. Dezember 2000, Nr. 233.

Hans-Jürgen Pollirer Obmann der neuen Sparte „Information und Consulting“

Der Wiener Unternehmensberater Hans-Jürgen Pollirer, 60, wurde am 21. Oktober einstimmig von allen politischen Fraktionen zum Obmann der neuen Sparte „Information und Consulting“ in der Wirtschaftskammer Österreich gewählt. „Dieses klare Vertrauensvotum sehe ich als eindeutigen Auftrag, für 87.000 Unternehmungen in der Informations-, Kommunikations- und Consultingwirtschaft eine neue professionelle interessenspolitische Plattform zu schaffen“, betont Pollirer in einer ersten Stellungnahme.
Ebenfalls einstimmig wurden die Wiener Kabel-TV-Betreiberin Alfreda Bergmann-Fiala und der oberösterreichische Immobilientreuhänder Gerhard Dietmar Steller als Obmann-Stellvertreter gewählt. Weiters umfasst das Spartenpräsidium die einstimmig kooptierten Helmut Ogulin (Abfall- und Abwasserwirtschaft) und Maximilian Hofmann (Technische Büros).
Für Pollirer verkörpern die Unternehmen in der neuen Sparte „Information und Consulting“ das Bild der modernen Dienstleister. „Eine innovative und sich schnell verändernde Wirtschaft braucht

unbedingt flexible, moderne und wettbewerbsfähige Rahmenbedingungen“, so Pollirer.
In einem ersten Schritt fordert der neue Spartenobmann die Stärkung des e-business-Standorts Österreich und die Reform der Besteuerung von Kommunikationsdienstleistungen. Dazu zählen für Pollirer in erster Linie die Entwicklung einer Digitalisierungsstrategie, die Förderung von e-government und e-business, ein neues Unternehmerrecht und die Stärkung der Berufsrechte sowie die Abschaffung der Werbesteuern und die aufwandsadäquate Finanzierung der Regulierungsbehörden.
Pollirer weiß um den hohen Erwartungsdruck der Informations-, Kommunikations- und Consultingwirtschaft an die neue Sparte in ihrer Rolle als Interessenvertreterin und EU-Lobbyistin. „Daher habe ich heute meine Funktionärskollegen in den Fachorganisationen und den Landeskammern eingeladen, mit mir gemeinsam ein Stück des interessenspolitischen Weges zu gehen“, legt Pollirer ein Bekenntnis zur „Teamarbeit“ ab. Mit diesem Team will Pollirer ein Programm erarbeiten, das die politischen Schwerpunkte der Informations-, Kommunikations- und Consultingwirtschaft umfassen wird: „Auf dieser Basis werden wir dann unser Polit- und Strategiekonzept aufbauen, das selbstverständlich auch einen professionellen Marketingplan und einen ambitionierten Zeitplan enthalten wird“, schließt Pollirer.

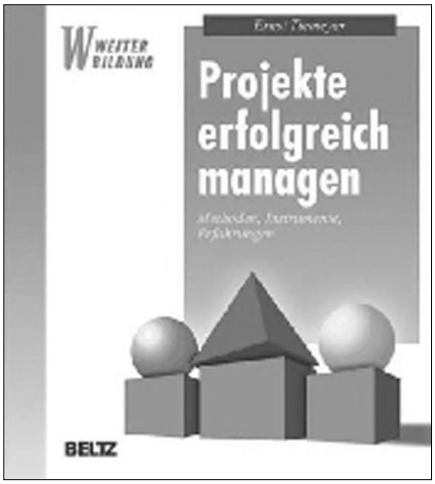
Aktuelle Literatur

MACHT in der WISSENS- und KOMPETENZ-GESELLSCHAFT

Wissen ist Macht
Unwissen ist Ohnmacht
Ist geteiltes Wissen geteilte Macht?

Autor: F. Barachini, SHAKER Verlag GmbH, ISBN: 3-8322-0656-6

Macht spielt seit Menschengedenken in jeder Gesellschaftsform eine wichtige Rolle. Vor dem Hintergrund gesellschaftspolitischer und technischer Entwicklungen werden die Instrumente der Macht als Basis für eine neue Führungsdisziplin im Management erläutert. Wir können mit Macht wesentlich besser umgehen, wenn wir verstehen, wie Macht entsteht und welche Instrumente zur Machtausübung eingesetzt werden können. Obwohl sich die Rahmenbedingungen zur Machtausübung durch gesellschaftspolitische Entwicklungen deutlich verändert haben, kommen aufgrund der Entwicklungsgeschichte des Menschen immer wieder dieselben Mechanismen zur Anwendung. Aufgrund von persönlichen Erfahrungen, aber auch mit Hilfe von Allegorien schildert der Autor, welche Mächte unser tägliches Leben maßgeblich beeinflussen und wie wir damit umgehen. Es wird gezeigt, wie die neuen Wertvorstellungen der Wissensgesellschaft Veränderungen im Unternehmensmanagement erzwingen. Neben einer Erweiterung der Achsenzeittheorie von Karl Jaspers stellt der Autor selbst zwei neue Theorien vor. Zum einen bildet er den zwischenmenschlichen Informationsaustausch auf ein Modell der Finanzwirtschaft ab, zum anderen entwickelt er die Pyramide der Macht, ein Pendant zur Maslow Pyramide.



Projekte erfolgreich managen

Methoden, Instrumente, Erfahrungen

Autor: Ernst Tiemeyer, Beltz-Verlag, Weinheim 2002, 180 Seiten, Pappband,
Preis: 24,90 Euro, ISBN 3-407-36390-7

Projektarbeit ist aus vielen Arbeits- und Berufsfeldern heute nicht mehr wegzudenken, so insbesondere auch im IT-Management. Erfolgreiche IT-Projekte sind ohne ein effizientes Projektmanagement undenkbar. Nur so sind die für die Projektabwicklung anfallenden Teilaufgaben überschaubar und lassen sich Problemsituationen rechtzeitig erkennen. Außerdem wird es den Mitarbeitern im Projekt dann weniger schwer fallen, zielorientiert zu handeln. Wirkungsvolles IT-Projektmanagement wird daher zu einem zentralen Erfolgsfaktor, der Bedarf an qualifizierten IT-Projektleitern und Mitarbeitern steigt.

Von Ernst Tiemeyer, seit vielen Jahren Referent und Tagungsleiter auf zahlreichen ADV-Veranstaltungen (Seminaren, Lehrgängen, Tagungen), ist aktuell im Beltz-Verlag ein interessantes neues Buch erschienen, das in anschaulicher und praxisnaher Form allen Beteiligten die für die Projektarbeit notwendigen Methoden und Techniken vermittelt.

Dieses Buch enthält zahlreiche Hinweise, Tipps und Orientierungshilfen für ein erfolgreiches Projektmanagement. Es ist in 9 Kapitel gegliedert:

- In den ersten 3 Kapiteln erhalten Sie Informationen zu den wesentlichen Rahmenbedingungen, die Sie kennen sollten, bevor ein Projekt gestartet wird. Dabei erfahren Sie, wie ein Projekt initiiert wird, wie sich aus einem Projektantrag ein Projektauftrag ergibt und welche Erfolgsfaktoren ein modernes Projektmanagement ausmachen.
- Eine gelungene Startphase beeinflusst entscheidend den Projekterfolg. Im 4. Kapitel wird Ihnen deshalb gezeigt, wie optimale Startbedingungen geschaffen werden können. Diese reichen von der Bildung des Projektteams, der Organisation eines Start-up-Meetings über den Zielbildungsprozess bis hin zur Festlegung der gesamten Projektorganisation.
- Die verschiedenen Projektplanungsaufgaben können Sie im 5. Kapitel kennen lernen. Dazu rechnen das Erstellen eines Projektstrukturplan, die Nutzung von Balkendiagrammen und Netzplänen, die Ressourcenbedarfsplanung, die Kostenplanung,

Redaktionschluss für die „ADV-Mitteilungen 1/2003“:

15. Februar 2003

Helfen Sie bitte mit, auch mit den „ADV-Mitteilungen“ einen Informationsaustausch unter den Mitgliedern zu ermöglichen. In diesem Sinn sind Ihre Beiträge sehr willkommen!

IMPRESSUM:
Medieninhaber: ADV Handelsges.m.b.H.
Herausgeber: Arbeitsgemeinschaft für Datenverarbeitung (ADV)
Redaktion: Mag. Johann Kreuzeder, Generalsekretär der ADV
Alle: A-1010 Wien, Trattnerhof 2
DVR: 0119911

Vervielfältigung: Wiener Zeitung, Digitale Publikationen, Wiedner Gürtel 10, 1040 Wien

ADV-Bürostunden:
Montag bis Donnerstag 8.30-17 Uhr, Freitag von 8.30-14 Uhr
Telefon: (01) (int. ++43-1) 5330913, Fax: DW 77, e-mail: office@adv.at,
URL: http://www.adv.at

die Qualitätsplanung und die Risikoplanung.

- Da Projektarbeit im Team realisiert wird, ist eine erfolgreiche Kooperation aller Beteiligten von enormer Bedeutung für den Projekterfolg. Wie Sie diese sichern können, erfahren Sie im 6. Kapitel des Buches. Themen sind dabei unter anderem Fragen der Teamentwicklung, die Organisation und Abwicklung von Teamsitzungen, die Kooperation mit Beratern, Führungsfragen sowie Konfliktmanagement.
- Um das Projekt während der Durchführung auf Erfolgskurs zu halten, ist eine laufende Projektsteuerung und Projektkontrolle notwendig. Welche Maßnahmen dabei bewährt sind sowie Fragen des Claim-Management, des Projekt-Marketing sowie des Change Management in Projekten werden im 7. Kapitel ausführlich erörtert.
- Die Kenntnis von Methoden und Techniken der Problemlösung und ihre Anwendung in Projekten ist ebenfalls bedeutsam für erfolgreiche Projektarbeit. Gleiches gilt für die Nutzung von Software sowie für die Organisation von Projektabstimmungs- und -kooperationsprozessen im Web. All diese Themen finden sich im 8. Kapitel.
- Das letzte Kapitel des Buches zeigt Ihnen, wie ein erfolgreicher Projektabschluss gestaltet werden kann. Dazu gehört nicht nur die Projektabnahme durch Auftraggeber, sondern auch die Bewertung der Projektarbeit durch die Projektbeteiligten, die Projekt-Abschlusspräsentation und die Auflösung des Projektteams.

Fazit: Nach Durcharbeiten des Buches besitzen Sie das fachliche Wissen und die administrative Kompetenz, IT-Projekte erfolgreich zu starten, zu leiten und zu steuern. Durch eine Orientierung der Hauptkapitel des Buches am gesamten Prozess des Projektmanagement (beginnend bei der Projektinitiative bis hin zu einem erfolgreichen Projektabschluss) wird eine leichte Umsetzung auf typische Projektsituationen aus der Praxis möglich.