ADV mitteilungen
DER ARBEITSGEMEINSCHAFT FÜR DATENVERARBEITUNG

2005 – Ausgabe Nr. 4 Auflage: 1600 Exemplare

Aus dem Inhalt

www.softwarequalitaet.at

Hochqualifiziertes IT-Management bleibt unverzichtbar

ADV-Lehrgang bereitet gezielt, umfassend und zukunftsorientiert auf die vielfältigen Aufgaben im IT-Management vor!

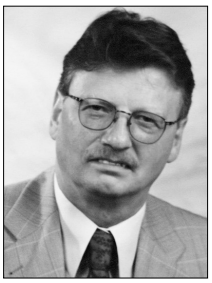
Die IT leistet einen wesentlichen Beitrag zur Wirtschaftlichkeit in Unternehmen und Verwaltung, gleichzeitig trägt sie zunehmend auch zum Unternehmenserfolg und zur unmittelbaren Wertschöpfung von Unternehmen bei, dies ist sicher unbestritten. Um die **IT-Potenziale** aber auch erfolgreich auszuschöpfen, ist jedoch eine leistungsfähige organisatorische Positionierung der IT im Unternehmen sowie **hochqualifiziertes IT-Personal unverzichtbar**.

Die notwendigen Fähigkeiten des IT-Personals lassen sich am besten aus den Aufgaben ableiten. Aktuelle Studien und vielfältige Erfahrungen zeigen, dass die IT-Mitarbeiter vor allem auch für **Management-Aufgaben** befähigt sein müssen. Dazu zählen vor allem

- das Managen von IT-Projekten und das Führen von Projektteams
- das Planen und Bereitstellen von IT-Infrastrukturen
- das Managen hochwertiger IT-Services
- das Entwickeln von IT-Strategien
- das Führen und Coachen von IT-Mitarbeitern und Teams
- die Übernahme von Organisationsaufgaben im IT-Bereich

EDITORIAL

Sehr geehrtes ADV-Mitglied, liebe Leserin, lieber Leser,



der Sommer ist vorbei, der Nachwuchs zurück an die Schulbänke gekehrt – und für alle fortbildungshungrigen Erwachsenen bietet die Arbeitsgemeinschaft für Datenverarbeitung auch diesen Herbst wieder eine Vielzahl von neuen Veranstaltungen, die ein weites Themenspektrum von unserer traditionellen Fachtagung Verwaltungsinformatik über IT-Controlling-Seminare bis hin zu Dokumenten-Management-Veranstaltungen abdeckt.
So ist auch der Schwerpunkt dieser Ausgabe der ADV-Mitteilungen eine Veranstaltung, die im nächsten Jahr stattfinden wird: der ADV-Zertifikats-Lehrgang „Ausbildung zum IT-Manager", der im Jänner 2006 startet und in fünf Modulen abgehalten wird. Informationen zum Lehrgang sowie einführende Erklärungen zur Bedeutung von hochqualifiziertem IT-Management bieten die Veranstaltungsleiter Dipl.-Hdl. Ernst Tiemeyer und Univ.Prof. Dr. Otto Krickl. Von Herrn Tiemayer ist auch das Buch „IT-Servicemanagement kompakt", das in anschaulicher und übersichtlicher Form aufzeigt, wie leistungsfähiges Servicemanagement im IT-Bereich aussehen kann. Der Band kann über die ADV-Buchhandlung bezogen werden. Dipl.-Ing. Helmut Maschek berichtet über die „ADV im Kampf gegen E-Mail-Missbrauch zum Transport von Viren etc." In dieser bereits mehrere Monate laufenden Initiative wurde kürzlich bei österreichischen Providern von externen Mailbox-Diensten eine Erhebung von Kenndaten durchgeführt, deren Ergebnisse hier dargestellt werden.
A-SIT, das Zentrum für sichere Informationstechnologie – Austria informiert über Probleme betrügerischen Missbrauchs von Auktionen im Internet.

Eine traurige Nachricht hat die ADV erreicht: Herr Othmar Markes, Generalsekretär des Verbandes Österreichische Software Industrie (VÖSI), ist im August verstorben. Othmar Markes war Gründungsmitglied der ADV und in den letzten Jahren als Generalsekretär des VÖSI häufig in unserem Büro präsent. Wir werden ihn vermissen.

Einen guten Start in einen vermutlich arbeitsamen, jedoch sicherlich auch erfolgreichen Herbst wünscht Ihnen Ihr

Mag. Johann Kreuzeder
(Generalsekretär)

- das Managen von Software-Entwicklungen und Software-Einführungen sowie
- Planungs-, Entscheidungs- und Kontrollaufgaben unter Berücksichtigung betriebs- und finanzwirtschaftlicher Aspekte bzw. rechtlicher Besonderheiten (etwa bei der Projektplanung und Projektabwicklung, für das Budgeting der IT-Abteilung und der IT-Produkte sowie bei IT-Beschaffungen).

Nach wie vor unterliegt auch **der IT-Bereich einer besonderen Dynamik**, die durch die Vielzahl von technischen Möglichkeiten und den steigenden Anforderungen der Anwender noch verschärft wird. Charakteristisch für die gegenwärtige informationstechnologische Entwicklung sind relativ kurze aufeinanderfolgende Innovationszyklen, die mit großen qualitativen Sprüngen der Informations- und Kommunikationstechnologien (Hardware-, Software- und Netzwerk-Architekturen) und einer enormen Vielfalt an IT-Produkten verbunden sind. 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
- die richtigen Projekte initiiert und diese erfolgreich abwickelt sowie
- permanent gute IT-Services bereitstellt.

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 dem Erwerb eines Zertifikates (Bearbeitung eines Projektes im eigenen Arbeitsumfeld, Präsentation und Abschlussprüfung) abgeschlossen werden. Für das Jahr 2006 wird ein weiterer Lehrgang zum IT-Manager von der ADV angeboten (Starttermin: Jänner 2006).

Welchen Nutzen haben die Teilnehmerinnen und Teilnehmer durch den Besuch des ADV-Lehrgangs zum IT-Manager? 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. Einen Überblick über die Themen der fünf Module, die jeweils 3 Tage Präsenzseminar beinhalten, ist nachfolgend wiedergegeben:
Im Einzelnen bieten die fünf Module des Lehrgangs folgende Qualifizierungsmöglichkeiten:

Module	***Schwerpunkte / Inhalte***
Modul 1:	**IT-Projekte** - Projektplanung, Projektmanagement, Projektteams führen, Projektcontrolling und Qualitätssicherung, Tools im Projektmanagement
Modul 2:	**IT-Architekturen, IT-Netze** (lokale Netze, Internet/Intranet, Web-Technologien), **Informationssicherheit, IT-Mobility**
Modul 3:	**IT-Strategien, IT-Personalführung und IT-Servicemanagement –** Strategieentwicklung, Führung einer IT-Abteilung und IT-Organisation, IT-Architekturmanagement und IT-Serviceprozesse
Modul 4:	**Software** – Software-Entwicklung, Datenbanksysteme, Standard-Anwendungen auswählen und einführen, Prozessmodellierung
Modul 5:	**Betriebswirtschaft und Recht für IT-Verantwortliche** – Geschäftsprozesse und E-Business, Kosten- und Leistungstransparenz in der IT, IT-Beschaffungen und IT-Investitionen, IT-Controlling, IT-Kennzahlen, IT-Recht

- Das **1. Modul** fokussiert auf den Bereich das **IT-Projektmanagement.** Die „richtigen“ Projekte erfolgreich zu realisieren, stellt für das IT-Management nach wie vor eine wichtige Herausforderung dar. Dies wird allein daraus deutlich, dass auch aktuelle Studien aufzeigen, dass der Anteil der gescheiterten IT-Projekte in Österreich immer noch relativ hoch ist. Im Rahmen des Moduls erfahren Sie unter anderem, wie aus Projektvisionen tragfähige Projektaufträge resultieren, lernen Sie bewährte Projektplanungstechniken ebenso wie Methoden zur eigentlichen Durchführung der IT-Projektarbeit. Hinzu kommen neue Herausforderungen im IT-Projektmanagement; beispielhaft seien das Projekt-Risikomanagement, Claim-Management, Change-Management sowie Qualitätsmanagement in IT-Projekten genannt.

- Ein weiterer Kernprozess des IT-Managements ist die **Entwicklung und Umsetzung von IT-Architekturen.** Die Architekturarbeit leistet durch die Definition von Rahmenbedingungen für den IT-Einsatz die Grundlage für eine schnelle DV-technische Bewältigung der immer komplexeren Anforderungen der Betriebe und der dortigen Fachabteilungen und Endbenutzer. Ein zentraler Aspekt ist eine möglichst weitgehende Vereinfachung der integrierten Systemlandschaft, die auf prozess- und produktübergreifende IT-Architekturen zielt. Letztlich geht es dabei darum, Hardware-Systeme (Server, Storage, Netze etc.), Daten (Datenbanken) und Applikationen zu konsolidieren. Um dies zu realisieren, muss das IT-Management die vier Architekturbausteine (Technologiearchi-

tektur, Anwendungsarchitektur, Datenarchitektur und Geschäftsarchitektur) „beherrschen“ und in der Lage sein, die dazu notwendigen Entscheidungen für die eigene Organisation „auf den Weg zu bringen“. Wie dies möglich ist, erfahren Sie unter anderem im **2. Modul** des IT-Manager-Lehrgangs. Weitere Schwerpunkte sind: IT-Netze (lokale Netze, Internet/Intranet, Web-Technologien), Informationssicherheit, IT-Mobility.

- **Im 3. Modul des Lehrgangs** erwerben die Teilnehmerinnen und Teilnehmer das fachliche Know-how und die grundlegende Kompetenz,
  - IT-Strategien „aufzusetzen“,
  - IT-Personal erfolgreich zu führen sowie
  - IT-Serviceprozesse effizient und effektiv zu gestalten.

  In der Praxis des IT-Management ist es besonders wichtig, an der Entwicklung und Umsetzung von IT-Strategien und IT-Architekturen erfolgreich mitzuwirken. Geschäfts- und IT-Strategie müssen so in Übereinstimmung gebracht werden, dass die Gesamtstrategie der Organisation die Ausgestaltung der IT-Strategie ganzheitlich – und wechselseitig – bedingen kann („Strategic Alignment“). Aber auch personelle Fragen sind nicht zu unterschätzen und werden deshalb in diesem Modul vor allem aus Führungssicht behandelt.

- Das **4. Modul** stellt Themen rund um die „Softwareentwickung“ und „Softwareimplementation“ in den Mittelpunkt. Dabei wird neben der Individualentwicklung anhand zukunftsfähiger Vorgehensmodelle auch dem Aspekt der Auswahl und Einführung von Standardsoftware (insbesondere anhand von Case-Studies zu ERP-Lösungen) besonderes Augenmerk geschenkt.

- Das **5. Modul des Lehrgangs** nimmt ganz bewusst die neue Herausforderung für das IT-Management auf, zur optimalen Wahrnehmung von Planungs-, Steuerungs- und Kontrollaufgaben immer mehr auch betriebswirtschaftliche und rechtliche Kenntnisse besitzen zu müssen. Auf Grund der verschärften Wettbewerbssituation vieler Unternehmen und dem damit verbundenen Kostendruck treten betriebswirtschaftliche Betrachtungen (ROI, TCO) auch für IT-Spezialisten immer mehr in den Vordergrund. Ziel muss es vor allem sein, Kosten- und Leistungstransparenz im IT-Bereich herstellen zu können.

Was sind damit die **Kernziele und Kernkompetenzen**, die mit der Absolvierung des IT-Manager-Lehrgangs angestrebt werden können? Insbesonders sollen die Teilnehmer bzw. die Teilnehmerinnen ausgehend von vorhandenem Basiswissen und Erfahrungen im IT-Bereich in die Lage versetzt werden,

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

Ein besonderes **Anliegen des ADV-Lehrganges** ist es, die Teilnehmerinnen und Teilnehmer bei der Umsetzung des Erlernten im eigenen Arbeitsfeld gezielt zu unterstützen. Deshalb findet sich auch im Nachgang ein webgestützter Informationsaustausch sowie das Angebot von spezifischen Follow-up-Veranstaltungen für das IT-Management. Weitere Informationen zum Lehrgang finden Sie im Veranstaltungsprogramm der ADV (www.adv.at) sowie auf der gesonderten Informationsplattform für IT-Manager (www.it-manager.at).

Dipl.-Hdl. Ing. Ernst Tiemeyer *(u. a. Lehrgangsleitung im IT-Manager-Lehrgang)*

Univ.Prof. Dr. Otto Krickl *(wissenschaftlicher Leiter des IT-Manager-Lehrgangs)*

ADV im Kampf gegen E-Mail-Missbrauch zum Transport von Viren etc.

In den ADV-Mitteilungen 4/2004 und 5/2004 sowie 3/2005 haben wir über die Fragestellungen und die Aktivitäten der Arbeitsgruppe zu diesem Projekt berichtet.

Im Mai 2005 hat sich die Arbeitsgruppe zu einer **„ADV-Erhebung von Kenndaten für Mail-Dienste“** entschlossen. Dazu wurde eine Gruppe von Providern ausgewählt, die insgesamt einen großen Teil der österreichischen Nutzer externer Mailbox-Dienste als Kunden hat. Darin befinden sich auch jene **Provider**, mit denen die Mitglieder der Arbeitsgruppe eigene Erfahrungen haben, z.B. weil sie dort Kunde sind.

Die Auswahl stellt keine Wertung dar, sie dient nur der Arbeitseinteilung und der Begrenzung des Aufwandes.

Provider, die sich nachträglich beteiligen wollen, sind willkommen.

Eine Besonderheit ist darin zu sehen, dass die Wiener Firma Ikarus Software GmbH einerseits die Viren- und Spam-Filter-Technologie für die Telekom Austria bereitstellt, aber andererseits auch selbst Kunden mit beliebigem Internetzugang einen direkten Filtering-Service anbietet.

Zum Thema „Firmennetze und Sicherheitslösungen“, auch betreffend Mail, bis hin zu Outsourcing war die **Telekom Austria** zu ausführlichen Gesprächen bereit, wofür wir hier danken.

Wegen der beachtlichen Anzahl von Mailboxen und der – wenn auch nun mehr im Hintergrund – hohen Bedeutung des Zentralen Informatikdienstes der **Universität Wien** für das Internet in Österreich wurde auch dieses Rechenzentrum um Stellungnahme zu unseren Fragen ersucht. Herrn **Dir. Dr. Peter Rastl** gilt unser besonderer Dank für seine Unterstützung. Als namhaften Repräsentanten kostenloser bzw. sehr moderat bepreister Maildienste haben wir GMX einbezogen.

Die **Kriterien** für die Erhebung wurden in der Arbeitsgruppe und teils mit Providern diskutiert. Es ist nicht möglich, das Thema in kompakter Form vollständig abzubilden. Auch die Interpretation der Kriterien kann zu Missverständnissen führen, weshalb sich Rücksprachen immer wieder als nötig erwiesen. Dies, obwohl bei Übermittlung der Tabelle neben der Spalte der Kriterien eine Spalte mit Hinweisen auf die gewünschten Aussagen geliefert wurde (Beilage).

Wir hoffen trotz dieser Problematik, dass unser Zielpublikum in den Antworten nützliche Informationen und Anregung für gezielte eigene Fragen bei Beurteilung der Maildienste findet.

Unter der „Service-Zeit“ wurde zumeist die Verfügbarkeit der Hilfe (Call-Center) beim Provider angegeben. Die Mailserver selbst laufen permanent – zumindest ist das so geplant.

Erfahrungen bei den Kontakten mit den **Providern**:
Es war bei einigen Providern langwierig, eine kompetente Auskunftsperson zu finden. Anfragemails mit unserem Anliegen wurden zum Teil lange ignoriert. In diesen Fällen kam der Kontakt erst nach Urgenzen per Mails, Telefon oder in einem Fall per eingeschriebenem Brief an die Geschäftsleitung zustande. Tele2UTA und hotmail haben trotz mehrerer Kontaktversuche auf verschiedenen Wegen nicht geantwortet.

Das Verhalten der Provider bei Mails an die offizielle Adresse, auch im Fall von Problemen mit der eigenen Mailbox in dieser Zeit, war generell unbefriedigend und keine Werbung für die Branche. Die Mindestforderung ist eine Reaktion in 1 bis 2 Tagen. Eine prompte automatisierte Bestätigung mit Geschäftsfall-Identnummer, nach der dann nichts geschieht, zählt nicht.

Wenn dann auch noch die Hotline kostenpflichtig gemacht wird, wird die Geduldgrenze des Kunden langsam überschritten.

Die Hotline war aber bei manchen Providern wirklich hilfreich.

Einige Provider verstanden zunächst nicht, warum unsere Arbeitsgruppe die angefragten Informationen nicht dem Internetauftritt des Providers entnimmt. Die von den Ansprechpersonen dann doch vorgenommenen Eintragungen in die Tabelle zeigten aber, dass es diesbezüglich durchaus Diskussionsbedarf gab und längst nicht alle Angaben einfach den Produktdarstellungen der Provider-Homepage entnommen werden können. Die zumeist erforderliche Abklärung wurde teils telefonisch, per E-Mail und teils in Besprechungen beim Provider durchgeführt.

Bei den Kontakten mit den Providern ergaben sich zusätzliche Erkenntnisse, die wir vielleicht in gesonderten Berichten verarbeiten werden.

Zusammenfassung der Ergebnisse (die Tabellen werden in dieser und in den nächsten Nummern der ADV-Mitteilungen veröffentlicht, können aber ab sofort im Mitgliederbereich der ADV-Website abgeholt werden; Details lesen Sie bitte dort nach):

Wir haben Antworten von folgenden Providern (alphabetisch):
Eunet, GMX, Ikarus, Inode, Telekom Austria aon, Telekom Austria Firmenkunden, Universität Wien, UPC Telekabel erhalten.

Den Provider-Angaben zufolge wird der **Viren-Schutz** mit folgenden Software-Produkten bzw. mit Produkten folgender Hersteller bewerkstelligt: ClamAV (open source), Full Body Scan, Ikarus, Kaspersky, McAffee, Network Associates, Symantec Antivirus.

Die Aktualisierung der Signaturdatenbank für den Virenschutz erfolgt zumindest täglich (im Einzelfall alle 10 Minuten!),

manche Provider signalisierten einen rascheren Zyklus mit „laufend“ oder „jede halbe Stunde“.

Mails mit Viren werden:
- automatisch gelöscht (mit oder ohne Verständigung von Absender und Empfänger),
- nach Kundenwunsch in einen speziellen Ordner verschoben bzw. als Attachment mit der Warnmitteilung zugestellt,
- vom Virus gereinigt und mit entsprechendem Vermerk zugestellt.

Eine **Steuerung** des Virenschutzes durch den Anwender ist teils durch Ein-Ausschalten und teils durch „Finetuning“ mittels Webinterface oder durch Rücksprache mit der Hotline möglich.

Kommentar zum Virenschutz:
Die in ersten Gesprächen von Provider-Seite geäußerte Meinung, dass Mails jedenfalls zugestellt werden müssten und sogar ein Schutz wegen der nötigen Einsichtnahme und der damit verbundenen Verletzung des „Briefgeheimnisses“ nicht zulässig wäre, dürfte inzwischen aufgegeben worden sein. Eine derartige Argumentation wurde nunmehr von keiner einzigen der Ansprechpersonen vorgebracht.

Allerdings verlangen einige Provider eine prinzipielle Zustimmung durch den Kunden vor Aktivierung der Mailprüfung auf Viren (bzw. Spam). Teils erfolgt diese implizit durch die vom Kunden zu betätigende Ein-/Ausschaltmöglichkeit.

Der **Spamschutz** ist bei allen erhobenen Maildiensten kostenlos im Virenschutz includiert und stützt sich auf folgende Produkte bzw. Verfahren (im Einzelfall eine Teilmenge daraus):
Briefkopf-Analyzer, Brightmail (Symantec), Eigenentwicklungen zur Erkennung, lernfähige Textmuster-Profiler, Multilayered spam protection (filter, heuristics, language identification etc.), Spam Assassin, Spamserver-Blocker, Spamtraps, White- Grey- und Black-Lists, Zentrale Klassifikationslogik, Bayes’sche Textanalyse, Lexikalische Analyse, Spamdatenbank, Subject Analyse, Schutz vor Directory Harvesting-Attacken, Mailbombing Protection, Relay Spoofing Protection.
Mails unter Spamverdacht werden:
- im Betreff mit einem Hinweis versehen oder
- in speziellen Ordnern bereitgestellt, wo sie teils nach einer einstellbaren Frist gelöscht werden.

An der Universität Wien gibt es einen zentralen Spamschutz, der bei eindeutiger Klassifikation die betroffene Mail blockiert, also nicht weiterleitet, was aber vom Anwender abschaltbar ist. Die nächste Ebene des Schutzes ist dann auf dem Arbeitsplatzrechner durch entsprechende Funktionen im Mailprogramm gegeben.

Eine **Steuerung** des Spamschutzes ist teils durch Ein-Ausschalten und teils durch Bedienoberflächen zur Pflege der Black- and Whitelists sowie zur Einstellung von Parametern der Schutzmechanismen möglich.

Die Service-Zeiten der **Hotlines** sind ebenso deutlich verschieden wie deren Kosten und Effektivität. Der **Support über Mail** dürfte häufig unbefriedigend sein, wie sich aus Erfahrungen mit den eigenen Mail-Providern und dem Verhalten bei unserer Anfrage schließen lässt. Hier besteht massiver **Verbesserungsbedarf**.

Insgesamt sehen wir ein **hohes Niveau der Schutzangebote** gegen Viren, sodass man bestimmt einen Provider finden kann, der im Umgang mit der Mail bis hin zum Support den individuellen Erwartungen und Anforderungen entspricht.

Uns ist bewusst, dass die **Anwender** dadurch **nicht vom Schutz** der am Internet angeschlossenen Maschinen **entbunden werden**. Es gibt genügend Gefahren unabhängig vom Mailverkehr.

Aber wenigstens bei den Mails ist ein gut gepflegter Schutz möglich, der die zum jeweiligen Zeitpunkt erkennbaren Schadprogramme von der Maschine des Anwenders fernhält.

Dipl.-Ing. Helmut Maschek
maschek@a1.net

Fragenkatalog an die Provider

Provider	Name
Bezeichnung des Dienstes	Text
Preis pro Mailbox	EUR
Virenschutz möglich	J/N
Preis Virenschutz	EUR
Virenschutztechnologie (Technik, Hardware/Software, Hersteller)	Text
Aktualisierungszyklus der Signaturdatenbank	Text
Behandlung der Mails mit Schadprogrammen	z.B. Bereitstellung in gesondertem Ordner und Löschen nach x Tagen
Einstellmöglichkeiten für den Anwender beim Virenschutz	Wenn JA: Mechanismus der Einstellung: Bedienoberfläche in Webmail oder Anruf bei Hotline etc.
Spamschutz möglich	J/N
Preis Spamschutz	EUR
Spamschutztechnologie (Technik, Software, Trefferwahrscheinlichkeit)	Text
Behandlung der Spammails	z.B. Bereitstellung in gesondertem Ordner und Löschen nach x Tagen
Einstellmöglichkeiten für den Anwender beim Spamschutz	Wenn JA: Mechanismus der Einstellung: Bedienoberfläche in Webmail oder Anruf bei Hotline etc.
Service-Zeit	Zeiten
Besondere Hinweise (z.B. womit heben Sie sich von der Konkurrenz ab)	Text

Problematik betrügerischen Missbrauchs von Auktionen im Internet (jüngstes Beispiel: eBay)

In den Medien wurde berichtet, dass unbekannte Betrüger die Mitgliedskonten von Kunden des virtuellen Auktionshauses eBay geknackt und auf Kosten ihrer Besitzer Luxusautos sowie Waren – in einem Fall um 350.000,– Euro – ersteigert haben. Die Geschädigten könnten nun mit Schadenersatzforderungen der Verkäufer konfrontiert werden.

Da die Passwörter der Mitgliedskonten nicht durch Eindringen in eBay-Systeme kompromittiert wurden, lehnt eBay – so die Berichte – jede Haftung ab, da die zur Verfügung gestellten Sicherheitsmechanismen korrekt zu nutzen seien. Allerdings soll ein Verzicht auf die erhebliche Provision in Aussicht gestellt worden sein.

Nach Meinung einiger Juristen hätte eBay eine Fürsorge- und Schutzpflicht für seine Kunden, hätte also selbst sicherere Verfahren als Passwörter – wie z.B. elektronische Signaturen – zur Verfügung zu stellen.

Im Fall von eBay kann jedermann ein Mitgliedskonto anlegen und an Auktionen teilnehmen. Wie bei konventionellen Auktionen ist das Bieten dann rechtsverbindlich. Das eigentliche Problem ist damit der Vertragsabschluss durch Mausklick im Internet.

Zur Authentizität und Sicherheit einer „eBay-Identität“

Zum Anlegen eines Mitgliedskontos sind Adressdaten (kein Postfach) und eine gültige E-Mail Adresse notwendig. Ebenfalls muss ein Geburtsdatum und eine Telefonnummer angegeben werden. Zur Aktivierung des Mitgliedskontos erhält der Kunde eine E-Mail mit einem Bestätigungscode, die vom Anmeldesystem an die angegebene E-Mail Adresse gesendet wird. Wird bei der Anmeldung eine E-Mail Adresse angegeben, bei der eBay keine Informationen hat, ob der E-Mail-

Anbieter die Anmeldedaten des Besitzers der E-Mail Adresse überprüft hat, wird entweder ein Bestätigungscode an die angegebene Postadresse verschickt, oder der Kunde muss zur Überprüfung seiner Identität eine gültige Kreditkarte angeben, deren Daten verifiziert werden. Bei eBay-Deutschland erfolgt bei derartigen E-Mail Adressen eine SCHUFA-Abfrage zur Verifikation der Adresse (eBay nutzt die SCHUFA-Abfrage[1]) nicht zur Überprüfung der Kreditwürdigkeit des Kunden, es werden Name, Adresse und Geburtdatum an die SCHUFA übermittelt und bei Übereinstimmung bestätigt). Nach der Eingabe des Bestätigungscodes kann der Kunde an Auktionen teilnehmen.

eBay nimmt zur Identifizierung von Kunden in seinen AGB (§ 6, Punkt 24) wie folgt Stellung: *„Der Handel über das Internet birgt Risiken, die in der Natur des Mediums liegen. Da die Identifizierung von Mitgliedern im Internet schwierig ist, kann eBay nicht zusichern, dass jedes Mitglied die natürliche oder juristische Person ist, für die es sich ausgibt. Trotz unterschiedlicher Sicherheitsmaßnahmen ist es möglich, dass ein Mitglied falsche Adressdaten gegenüber eBay angegeben hat. Das Mitglied hat sich deshalb selbst von der Identität seines Vertragspartners zu überzeugen.“*

Der Zugang zu einem eBay-Mitgliedskonto ist lediglich durch Eingabe von Benutzername und Passwort abgesichert und kann von jedem beliebigen Ort mit Internetzugang erfolgen. Das Passwort selbst muss mindestens 6 Zeichen lang sein, eBay gibt Hinweise zur Wahl eines sicheren Passworts (Verwendung von Buchstaben, Zahlen und Sonderzeichen; Vermeidung von in Wörterbüchern aufgeführten Wörtern; Vermeidung von persönlichen Informationen wie Name, Geburtsdatum, Telefonnummer, E-Mail Adresse). Technisch wird von eBay lediglich die Wahl des eBay-Benutzernamens als Passwort verhindert und die Mindestlänge von 6 Zeichen überprüft. Es gibt auch keinen Sperrmechanismus, der das Ausprobieren verschiedener Passwörter verhindert. Die Absicherung der Übertragung des Passwortes bei der Anmeldung an ein eBay-Mitgliedskonto mittels SSL entspricht dem Stand der Sicherheitstechnik.

Es hat in der Vergangenheit immer wieder Fälle gegeben, in denen es Hackern gelungen ist, fremde Mitgliedskonten zu knacken (z.B. durch Phishing-Attacken, Schadsoftware wie trojanische Pferde, oder durch simples Ausprobieren von „schwachen“ Passwörtern). Der Benutzer ist selbst für die Wahl und sichere Verwahrung des Passworts zuständig, und muss auch selbst feststellen, ob die Internetseite auf der er zur Eingabe seines Passwortes aufgefordert wird, tatsächlich von eBay stammt. An diesem Punkt setzen Hacker an, von der Nutzung groben Leichtsinns über Programme, die „schwache“ Passwörter ausprobieren, gefälschte Webseiten die zur Passworteingabe auffordern bis zu Schadprogrammen, die Tastatureingaben abfangen und die so ermittelten Passworte an den Angreifer übermitteln.
Das beschriebene Verfahren mit den dargestellten Risken ist keine Besonderheit von eBay bzw. Online-Auktionshäusern, denn es wird auch bei den meisten Online-Shops bzw. Versandhäusern und auch bei Online-Bezahlsystemen wie z.B. PayPal oder bezahlen.at so oder ähnlich angewendet.

1) SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden, www.schufa.de

Allerdings gibt es bei „normalen“ Webgeschäften (Warenausgabe durch Zustellung) ein Rücktrittsrecht laut Fernabsatzgesetz (Rücktrittsrecht innerhalb einer gewissen Frist) oder zumindest die Zahlungskopplung (z.B. Kreditkarte) als Identitätsanhaltspunkt.

e-Bay unterscheidet sich weiters von Online-Shops bzw. Versandhäusern durch den hohen Anteil von Privatverkäufen, bei denen der rechtliche Schutz nicht wirkt (bei Privatauktionen wird das Rücktrittsrecht oft ausgeschlossen). Das macht die Problematik in diesem Fall größer als im kommerziellen Fernabsatz.

Schlussfolgerungen:

1. Obwohl die von eBay vorgesehenen Sicherheitsmaßnahmen korrekt funktioniert haben, konnte Betrug und Schädigung erfolgen, da sich die Angreifer gültige Passworte erschlichen und diese dann verwendet haben. Die Schwäche liegt im Passwort selbst, das vom Benutzer sicher verwahrt und verwendet werden muss. Damit sind Benutzer angesichts der vielfältigen Bedrohungen jedoch zunehmend überfordert.
2. Die Übertragung des Passworts zu eBay (SSL) kann als sicherheitstechnisch einwandfrei betrachtet werden. Problematisch (bei so gut wie allen Online-Shops) ist, dass die Absicherung der elektronischen Identität lediglich auf einer wissensbasierten Komponente (Passwort) beruht. Ein Diebstahl des Passwortes kann vom Benutzer i.A. erst entdeckt werden, wenn dieses bereits missbräuchlich verwendet wurde. Eine stärkere Absicherung bieten hier Authentifizierungsverfahren, die neben der Wissenskomponente eine Besitzkomponente verwenden (2-Faktor-Authentifizierung). In Österreich sieht das Konzept der Bürgerkarte, beispielsweise zur Absicherung der elektronischen Identität, eine derartige starke Authentifizierung zwingend vor. Als Besitzkomponente kommen hier derzeit entweder eine Signaturkarte oder ein Mobiltelefon zum Einsatz. Die Verbindung zwischen elektronischer und tatsächlicher Identität wird in diesem Konzept durch die so genannte Personenbindung erreicht, die auf der Bürgerkarte (bzw. beim Mobiltelefonnetzbetreiber) gespeichert ist. Die Methode des wirtschaftsbereichsspezifischen Personenkennzeichens (wbPK) zur Identifikation von Personen ermöglicht den Einsatz dieses Konzepts auch durch die Wirtschaft für den elektronischen Geschäftsverkehr.
3. Ein weiteres grundsätzliches Problem ist der Abschluss von Verträgen (bzw. die Abgabe von verbindlichen Geboten) durch einen einfachen Mausklick. Elektronische Signaturen können hier wesentlich mehr Sicherheit bieten, müssten dann aber verbindlich eingesetzt werden (zumindest müsste erkennbar sein, dass ein bestimmter Käufer nur signierte Gebote schickt). Ihnen mangelt es jedoch nach wie vor an der Akzeptanz und Verbreitung, selbst angesichts der geschilderten Gefahren.
4. Somit bleibt dem Benutzer derzeit nur die Möglichkeit, mit seinem Passwort äußerst sorgfältig umzugehen, und u.a. auch die Sicherheitsrichtlinien von eBay zu beachten.
5. Allerdings geht oft – durch die geschilderte Auktionsproblematik – das Rücktrittsrecht verloren. Daher gibt es die oben geschilderten Rechtsmeinungen, dass der Betreiber von elektronischen Auktionen dann eine verstärkte Fürsorge- und Schutzpflicht für seine Kunden hätte, die jedenfalls über das Angebot von Passworten und Tipps für den sicheren Umgang damit hinausgehen müsste.
6. Die in Deutschland verwendete SCHUFA-Abfrage schützt den Verkäufer vor unaufrichtigen Bietern. Die kolportierten Missbräuche hätte sie wohl nicht verhindert, da die Angreifer offenbar existierende Daten verwendet haben und die Betroffenen nichts von solchen Abfragen erfahren, d.h. ihnen nicht bewusst sein kann, dass sie womöglich Ziele von derartigen Angriffen sind, erst recht nicht dagegen vorgehen können.
7. Es muss immer bewusst sein, dass man es im Internet mit virtuellen Partnern zu tun hat. So schön und professionell eine Seite auch aussieht, so verlockend das Angebot sich liest: Ohne die Nutzung sicherer Verfahren zur Authentifizierung des Kommunikationspartners weiß man letztlich nicht, mit wem man es tatsächlich zu tun hat.

Autoren, A-SIT:
Manfred Holzbach
Daniel Konrad
Dipl.-Ing. Thomas Aichinger
Helga Spacek-Stangl

IT-Servicemanagement kompakt

IT-Servicemanagement kompakt zeigt Ihnen in anschaulicher und übersichtlicher Form, wie ein leistungsfähiges Servicemanagement im IT-Bereich hergestellt werden kann. Dieses Buch gibt Ihnen einen Überblick über Prozesse, Methoden und Best-Practice-Lösungen, die Sie bei der Realisierung von IT-Servicemanagement unterstützen können. Sie lernen kennen

- welche Methodik sich für ein zeitgemäßes IT-Servicemanagement bewährt hat,
- welche organisatorischen Vorarbeiten für die Anwendung moderner IT-Servicemanagement-Lösungen erforderlich sind;
- wie Sie IT-Servicemanagement zur professionellen Steuerung Ihrer IT-Abteilung nutzen, IT-Ressourcen planen, überwachen und optimal einsetzen sowie Ihre IT-Prozesse auf der Basis von ITIL zu unterstützen und zu professionalisieren.

Jedem Kapitel des Buches **IT-Servicemanagement kompakt** sind verschiedene Leitfragen vorangestellt, die sofort eine Orientierung geben, was Sie erwartet. Nach Durcharbeiten des Buches besitzen Sie das fachliche Know-how und die grundlegende Kompetenz,

- die Rolle eines modernen IT-Servicemanagement für die IT-Praxis zu etablieren,
- verschiedene IT-Serviceprozesse zu beschreiben und zu beurteilen sowie
- Verfahren und Instrumente des IT-Servicemanagement in der Praxis erfolgreich einzusetzen.

Dipl.-Hdl. Ing. **Ernst Tiemeyer** hat nach seinem Studium der Betriebswirtschaft, Wirtschaftsinformatik und Wirtschaftspädagogik zahlreiche Projekterfahrungen im IT- und Bildungsbereich gesammelt. Seine aktuellen Tätigkeitsschwerpunkte (Beratung, Forschung, Lehre) sind: Projektmanagement, IT-Controlling, IT-Servicemanagement, Geschäftsprozessorganisation und Geschäftprozessmanagement sowie E-Human Resource Management (Bildungsmanagement, E-Learning, E-Knowledge-Management).

Tiemeyer, Ernst
IT-Servicemanagement kompakt
2005, 159 S., 35 s/w Abb., 26 s/w Tab.
Kartoniert
ISBN 3-8274-1619-1, Preis: **15,50 Euro**
Erhältlich unter **www.adv.at** – Buchhandlung

In memoriam Othmar Markes

Othmar Markes ist im August dieses Jahres verstorben. Die ADV hat mit ihm ein Gründungsmitglied und ein über viele Jahre im Vorstand engagiertes Mitglied verloren.

Othmar Markes ist am 21. Mai 1959 Mitglied der ADV mit der Mitgliedsnummer 1 geworden. Beruflich war er damals Lochkartenabteilungsleiter der Gloriette Wäschefabrik. Im Gründungsvorstand der ADV, damals noch Arbeitsgemeinschaft Österreichischer Lochkartenfachleute (AOL), war Othmar Markes Schriftführer. Später als Vizepräsident und Finanzreferent des inzwischen in ADV umbenannten Vereins war er bis 1991 als Mitglied des ADV-Vorstands stets wichtiger Motor der ADV-Entwicklung. Als Praktiker hat er viel dazu beigetragen, dass die ADV ihrem Veranstaltungsmotto „Aus der Praxis für die Praxis" gerecht werden konnte.

Othmar Markes hat in seinen Funktionen als ADV-Vorstandsmitglied und als langjähriger Generalsekretär des Verbandes der Österreichischen Software Industrie (VÖSI) einen wichtigen Beitrag zur Förderung des rationellen und sinnvollen Einsatzes der Informations- und Kommunikationstechnik geleistet.

Othmar Markes wird uns sehr fehlen! Wir werden ihm stets ein ehrendes Andenken bewahren.

SC Dr. Arthur Winter, ADV-Präsident

Redaktionschluss für die „ADV-Mitteilungen 5/2005":

31. Oktober 2005

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: 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