

COMPUTERWOCHE

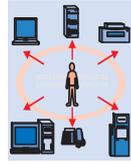
NACHRICHTEN ♦ ANALYSEN ♦ TRENDS



TELEKOM

Obermann, Dobermann?

Der neue Telekom-Chef René Obermann gilt als „harter Hund“. Der anstehende Umbau wird zeigen, ob er auch Diplomat ist. **SEITE 5**



ITK-TRENDS

Gartners Welt

In zehn Thesen beschreiben die Analysten, wohin sich der Markt entwickelt. Alles verändert sich, vor allem der Anwender. **SEITE 14**



KOOPERATION

Windows oder Linux?

Marktbeobachter sind geteilter Meinung darüber, wie glaubwürdig das Linux-Bekenntnis von Microsoft-Chef Steve Ballmer ist. **SEITE 16**

COMPUTERWOCHE TV

FW Für Edmund Küpper, Geschäftsführer von SD&M (links), haben maßgeschneiderte Lösungen Zukunft

- ◆ **Individualsoftware ist nicht tot** SD&M-Chef Küpper erwartet eine Koexistenz von Standardsoftware und maßgeschneiderten Lösungen.
- ◆ **Was Anwender an ERP-Systemen stört** Schlechte Anpassbarkeit und Defizite beim Reporting werden beklagt.

Bearingpoint rutscht erneut in die Krise

Geschäftsführer Peter Schurau muss gehen. Der Ex-Chef Hendrik Ansink gewinnt seinen Arbeitsrechtsprozess.

VON CW-REDAKTEUR JOACHIM HACKMANN

Schurau, seit Januar 2006 stellvertretender Sprecher der Geschäftsführung, ist nach Informationen der COMPUTERWOCHE vom Aufsichtsrat entlassen worden. Das bestätigten mehrere unternehmensnahe Quellen. Über die Gründe der Demission besteht dagegen noch keine Klarheit, die Rede ist von „Unregelmäßigkeiten“ und von „einer Verstrickung in einen Reisekostenskandal“. Der Aufsichtsrat soll Schurau außerdem vorwerfen, Bearingpoint-Mitarbeiter für sein eigenes Unternehmen abgeworben zu haben. Das würde das Unternehmen ins Mark treffen, da es nach wie vor unter einer hohen Fluktuation leiden soll. Ein Bearingpoint-Sprecher bestätigte, dass Schurau freigestellt wurde und eventuelle Verfehlungen untersucht würden. Probleme mit einer Abwanderungswelle unter den Mitarbeitern gebe es indes nicht.

Nebentätigkeiten der Führungsmann-



Geschäftsführer Peter Schurau muss das Unternehmen verlassen.



Ex-Chef Hendrik Ansink muss weiterbeschäftigt werden.

schaft sind bei Bearingpoint nichts Neues: Vor knapp einem Jahr hatte der deutsche Aufsichtsrat das Management zu einem Gutteil entlassen oder ausgetauscht. Mit Steffen Seeger, Geschäftsführer und Europa-Chef, konnte sich das Unternehmen gütlich einigen, er unterschrieb einen Aufhebungsvertrag. Die Trennung von Hendrik Ansink, Sprecher der Geschäftsführung, verlief dagegen weniger reibungslos. **Fortsetzung auf Seite 4**

DIESE WOCHE

SECURITY-EXPERTENRAT
Zur Wissens-Blog der COMPUTERWOCHE

Security-Experten unter sich

Wer sich mit Sicherheitsexperten austauschen will, sollte den neuen Wissens-Blog der COMPUTERWOCHE aufsuchen. **Thema der Woche SEITE 6**

Personalmaßnahmen bei SAS

Der Business-Intelligence-Spezialist SAS Institute baut um und transferiert die Emea-Zentrale von Heidelberg in die USA. **Nachrichten SEITE 10**

Java ist Open Source

Für die Programmierumgebung soll die populäre GPL gelten. Außerdem will Sun Versionen mit kommerziellem Support anbieten. **Nachrichten SEITE 10**

Großbaustelle „Dynamics“

Microsoft will seine ERP-Software-Lösungen zusammenführen und mit der Office-Welt vereinen. **Produkte & Technologien SEITE 24**

Aus dem Leben einer CIO

Jennifer Allerton, CIO von Roche Pharma, ließ sich einen Tag von einem CW-Redakteur über die Schulter schauen. **Job & Karriere SEITE 44**

ZAHL DER WOCHE

549 Euro – das ist voraussichtlich der in Deutschland zu zahlende Betrag für Windows Vista in seiner teuersten Version. Das geht aus Preisen hervor, die der Online-Einzelhändler Amazon.de für Vorbestellungen nennt. Die günstigste Vista-Variante dürfte die „Home-Basic“-Version sein, die als Upgrade 139 Euro kosten soll. Microsoft legt Computern, die derzeit gekauft werden, Coupons für einen günstigeren Übergang auf Vista bei. Damit soll verhindert werden, dass der PC-Absatz im Weihnachtswinter einknickt. Ausgeliefert wird Windows Vista ab 30. Januar 2007.

IBM will sich in China an Bank beteiligen

Die IBM hat sich nicht bestätigten Presseberichten zufolge einem von der Citigroup angeführten Bieterkonsortium angeschlossen, das die chinesische Guangdong Development Bank übernehmen möchte. Die Unternehmen sind bereit, zusammen drei Milliarden Dollar für einen 85-prozentigen Anteil an dem Institut zu zahlen. Im Erfolgsfall würde Big Blue fünf Prozent an der Bank halten. Offenbar erhofft sich der IT-Hersteller von diesem Deal bessere Geschäfte im chinesischen Bankenmarkt. (tc) ◆



SAP kämpft um den Mittelstand

Mit Hans-Peter Klaey sollen SAPs Geschäfte mit kleinen und mittleren Betrieben endlich ins Rollen kommen.

Zum wiederholten Mal organisiert SAP seine Mittelstandsorganisation neu. Um die ehrgeizigen Wachstumsziele – 100 000 Kunden bis 2010 – zu erreichen, will sich der größte europäische Softwarehersteller nun stärker ins Zeug legen. Darum hat der Konzern die neue Position des President Global Small and Midsize Enterprise (SME) geschaffen, die mit Hans-Peter Klaey besetzt wurde. Donna Troy, die bislang den weltweiten Partnerkanal betreute, bekommt damit einen Vorge-



SAPs neuer Mann für den Mittelstand: Hans-Peter Klaey.

setzen vor die Nase gesetzt. Der Schweizer soll sich vor allem darum kümmern, das „Partner-Edge“-Programm weltweit zu vereinheitlichen und zu synchronisieren. Branchenbeobachtern zufolge bedeutet dies jedoch auch, dass SAP die Zügel anziehen und den Partnern mehr auf die Finger schauen wird. Die zeigen sich jedoch gelassen. Sie verfolgen in erster Linie das Ziel, mit den SAP-Produkten mehr Umsatz zu erwirtschaften. (siehe Seite 12) (ba) ◆



SBS ist noch nicht am Ziel 18
 Siemens-Chef Klaus Kleinfeld präsentierte für den IT-Dienstleister missverständliche Zahlen: Auch im laufenden Quartal fließen Millionenbeträge in die SBS-Sanierung.

Die IP-Revolution schreitet voran 20
 Auf der VoIP-Konferenz VON Europe in Berlin zeigten die Experten, was in Sachen Internet Protocol und Mobiltelefonie künftig möglich ist.



Office als ERP-Frontend 30
 Neben SAP und Microsoft arbeitet eine Reihe anderer Hersteller an der Integration von Büroprogrammen mit betriebswirtschaftlicher Software.



NACHRICHTEN UND ANALYSEN

- Motorola kauft Good Technology 10**
 Mit dem Kauf von Good will Motorola Blackberry-Anbieter Research in Motion angreifen.
- Mäßige Telekom-Zahlen 18**
 Kurz vor dem Machtwechsel gab der Carrier seine Geschäftszahlen bekannt. Besonders bitter ist die Abwanderung der Kunden im Festnetzgeschäft.
- Cisco im Höhenrausch 18**
 Video- und Musik-Downloads strapazieren die Netze. Die Carrier müssen aufrüsten – und Cisco macht Kasse.

PRODUKTE & TECHNOLOGIEN

- Präventiver Malware-Schutz 21**
 Mit dem „Threat Seaker“ von Websense hat die Warterei auf Patches oder Signaturen ein Ende.
- DB2-Warehousing nutzt Viper 22**
 Die neue Datenbank-Engine bringt der „DB2 Data Warehouse Edition“ wichtige Funktionen.
- FSC-Mainframes vor IBM 22**
 Die neuen Großrechner „S165“ und „S200“ von Fujitsu-Siemens sollen die Konkurrenz in Sachen Leistung übertreffen.
- Microsofts neue Großbaustelle 24**
 Die Business-Lösungen von „Dynamics“ haben zwar einen gemeinsamen Namen, die technische Harmonisierung erfolgt jedoch nur schrittweise.

PRODUKTE & TECHNOLOGIEN

PRAXIS

- Test: Midrange-Speicher NSC55 26**
 Hitachis Tagmastore Network Storage Controller bietet Management-Funktionen wie das Highend.
- Gute Erfahrungen mit Nessus 28**
 Der quelloffene Vulnerability-Scanner prüft Systeme in sehr kurzer Zeit auf Schwachstellen.

IT-STRATEGIEN

- Knowledge-Management reloaded 34**
 Bereits totgesagt, erlebt das Thema Wissens-Management derzeit ein Revival. Beispiele von S.Oliver, Metro und Rheinmetall belegen das anschaulich.
- Erfolgsrezept Prozessorientierung 36**
 Weniger Produktionstiefe der IT und dafür mehr Prozessorientierung des CIO – auf diese Formel lässt sich der zu erwartende Wandel der IT-Abteilungen verkürzen.

IT-SERVICES

- Datenflut erfordert neue Konzepte 40**
 Das Wettrennen bei den Speichermedien reicht nicht mehr. Um Aufträge für das intelligente Informations-Management konkurrieren IT-Dienstleister und die Serviceabteilungen der Storage-Hersteller.
- Tausende Jobs wandern ins Ausland ab 42**
 Die großen Service-Provider bauen ihre Präsenz in Indien unaufhaltsam aus. Einige beschäftigen bereits ein Fünftel ihrer Belegschaft in Niedriglohnländern.

- Externe Beratung erfordert Kontrolle 42**
 Viele Anwender kaufen Management-Consulting-Dienste nicht strategisch genug ein. Vor allem bei der Bewertung der Leistungen herrscht Nachholbedarf.

JOB & KARRIERE

- Aus dem Alltag einer CIO 44**
 Das passiert auch nicht oft: Der Schweizer Großkonzern Roche Pharma erlaubte einem CW-Redakteur, seiner IT-Verantwortlichen Jennifer Allerton einen ganzen Tag lang über die Schulter zu schauen. Ein kürzeres Erfolgsrezept im Berufsleben gibt es nicht: „Für einen Vorgesetzten muss man, für einen Leader will man arbeiten.“ Dieser Satz kennzeichnet Allerton mehr als vieles andere.

SCHWERPUNKT: OFFICE MEETS ERP

- Excel ruft R/3 32**
 Wie die Tabellenkalkulation mit SAP-Standardtechnik integriert werden kann.
- Duet-Pilotprojekt 34**
 Die Hochschule Darmstadt will Verwaltungsaufgaben mit der Office-Mysap-Integration erleichtern.

STANDARDS

Impressum	42
Stellenmarkt	46
Zahlen – Prognosen – Trends	50
Im Heft erwähnte Hersteller	50

COMPUTERWOCHE.de

HOTTOPICS

- Auslaufmodell fester Arbeitsplatz
- In Indien ticken die Uhren anders
- CW-TV: Mehr Gehalt für alle

Neuer Karriereratgeber



Tipps zur IT-Karriere gibt Thomas Leibfried unseren Lesern vom 16. bis 29. November 2006. Der Personalexperte ist als Prokurist im Bereich Human Resources bei der Computacenter AG & Co. oHG verantwortlich für die Bereiche Personalentwicklung („Learning & Development“) und Recruiting.

www.computerwoche.de/job_karriere/karriere_ratgeber

COMPUTERWOCHE evaluiert ERP-Software

Unter mehr als 500 Lösungen die richtige ERP-Software zu finden ist nicht leicht. Mit dem Online-Evaluations-Tool IT-Matchmaker Plus helfen COMPUTERWOCHE und Trovarit, die richtige Wahl zu treffen.
www.computerwoche.de/product_guide/it-matchmaker

Bringing it all together.

Es ist ein wunderbares Gefühl: Der Moment, wo endlich alles zusammenpasst. BT macht es möglich. Mit seinem konvergenten Netzwerk und innovativen IP-basierten Infrastrukturlösungen. Für Ihren Erfolg in der digital vernetzten Wirtschaft.

Mehr Informationen finden Sie unter www.bt.com/networked

BT
 Bringing it all together

Networks • IT • Services

MENSCHEN

Wachablösung bei Toshiba Europe



Dirk Thomaere (Foto) wird ab Dezember die Position des General Managers der Toshiba Europe GmbH Computersysteme Deutschland/Österreich bekleiden. Der 45-jährige Belgier folgt auf den langjährigen Vice President und General Manager Michael Fassbender, der in den Ruhestand geht. Thomaere ist seit 2000 für Toshiba tätig. Zuletzt zeichnete er als General Manager für die Geschäfte in der Beneluxregion verantwortlich.

Neuer Verantwortlicher für die RAG-IT

Dieter Pfaff legt Ende des Jahres seinen Posten als CIO des Essener Energie- und Bergbaukonzerns RAG AG nieder. Wie das CW-Schwester-Magazin „CIO“ berichtet, übernimmt seine Aufgaben Jochen Gintzel. Der 48-Jährige ist seit September 2005 IT-Chef beim Chemiekonzern Degussa, den die RAG AG übernommen hat. Pfaff, der aus gesundheitlichen Gründen in den Vorruhestand geht, stand von 1998 bis 2005 an der Spitze der IT-Tochter RAG Informatik. Zugleich leitete er den Zentralbereich Informationsverarbeitung des Essener Konzerns. Nachdem die RAG Informatik an SBS verkauft wurde (heute SBI-Ruhr), wurde Pfaff schließlich CIO des RAG Aktiengesellschaft.

Kurth zieht den Kürzeren

Der Leiter der Bundesnetzagentur, Matthias Kurth, musste bei der Wahl des neuen Generalsekretärs der Internationalen Fernmeldeunion (ITU) eine Niederlage einstecken. Obwohl im Vorfeld als Favorit gehandelt, unterlag der 54-jährige Jurist im dritten Wahlgang seinem Gegenkandidaten aus Mali, Hamadou Touré. Noch ist offen, ob die Bundesregierung nun den Vertrag des SPD-Mitglieds als Leiter der Bundesnetzagentur verlängert oder ob sie für die kommende Amtsperiode einen Unionskandidaten bevorzugt. Möglicherweise könnte Kurth auch die Fronten wechseln und einen – vermutlich besser bezahlten – Posten in der Industrie annehmen.



Sun Deutschland ernennt Storage-Chef

Rainer Thieme übernimmt ab sofort die Verantwortung für das gesamte Speichergeschäft bei Sun Microsystems in Deutschland. In seiner neuen Position soll Thieme die Integration des übernommenen Anbieters von Bandspeicher-Systemen StorageTek vorantreiben. Sun setzt dabei auf Thiemes Erfahrungen in der Speicherbranche. Zu den Karrierestationen des 50-Jährigen zählen Unternehmen wie Control Data, NEC sowie Quantum. Seit seinem Eintritt bei Sun im Januar 2001 leitete Thieme strategische und produktorientierte Vertriebsgruppen.

Achim Berg wird Microsoft-Chef

Zuletzt als Bereichsvorstand der T-Com aktiv, wird Achim Berg ab Februar 2007 General Manager von Microsoft Deutschland. Der 42-jährige Diplom-

Informatiker beerbt Interims-Manager Klaus Holse Andersen, der für den im Streit ausgeschiedenen Jürgen Gallmann in die Bresche gesprungen war. Berg gehörte in den letzten fünf Jahren als Verantwortlicher für Vertrieb und Kundenservice dem T-Com-Vorstand an. Davor war er Vorsitzender der Geschäftsführung der Fujitsu Siemens Computers GmbH und Vertriebsdirektor bei Dell Computer in Deutschland.



Personalmittelungen bitte an Menschen@Computerwoche.de

Kolumne

Nicht einmal Klinsmann könnte es richten



Christoph Witte
Chefredakteur CW

Ob die Telekom ihre Probleme allein mit einem Personalwechsel an der Spitze in den Griff bekommen wird, ist fraglich. Europas größter Carrier kämpft gegen Marktanteilsverluste im Fest- und im Mobilfunksegment, er hat zu viele (unmotivierte) Leute an Bord und mit dem Bund einen Großaktionär, dessen Interessen nicht immer deckungsgleich sind mit denen des Unternehmens. Hinzu kommt die Notwendigkeit, die Netzinfrastruktur zu modernisieren (Next Generation Network) und Unternehmens- wie Privatkunden ordentliche und preiswerte Services anzubieten.

Dass René Obermann als Nachfolger von Kai-Uwe Ricke diese Herausforderungen meistern wird, ist keineswegs sicher. Was qualifiziert ihn dazu? Er ist nicht einmal ein neuer Besen. Und im Mobilfunkbereich, der zumindest im heimischen Markt Anteile verliert, ist Obermann eher Teil des Problems als Teil der Lösung.

Obermann wird weiter mit der Last der zu vielen falsch qualifizierten und daher oft unmotivierten Mitarbeiter leben müssen, ein Gutteil davon immer noch Beamte. Es wäre Wunschdenken zu glauben, all diese Leute weiterbilden zu können. Ebenfalls naiv wäre es anzunehmen, der Bund würde ihm in dieser (oder anderen wichtigen Ent-

scheidungen) mehr Freiraum geben als seinem Vorgänger. Das Gezerre um den Börsengang der Deutschen Bahn hat einmal mehr gezeigt, wie der Bund mit seinen Beteiligungen und deren Chefs umgeht.

Aus den beschriebenen Defiziten resultiert der niedrige Aktienkurs. Dem hilft es auch nicht auf die Beine, wenn die Telekom in VDSL investiert und dafür seitens der Politik ein Monopol auf Zeit eingeräumt bekommt. Zum einen wird sich die Europäische Union dagegen stemmen, zum anderen halten Ex-telecomer die Anbindung der Haushalte per Glasfaser (fibre to home) für die zukunftssichere Variante.

Das Bündel an Herausforderungen, denen die Telekom gegenübersteht, lässt sich nur bewältigen, wenn dem Vorstandsvorsitzenden generell mehr Bewegungsraum zugestanden wird. Bleiben die Machtverhältnisse so wie sie sind, hätte nicht mal Ex-Bundestrainer Jürgen Klinsmann eine Chance gehabt. Aber der hätte den Job unter diesen Bedingungen gar nicht erst angetreten.

Diese Kolumne finden Sie auch im Blog der COMPUTERWOCHE unter blog.computerwoche.de. Dort können Sie Ihre Meinung abgeben und sofort veröffentlicht. Wir freuen uns auf Ihren Kommentar.

Bearingpoint rutscht erneut in die Krise

Fortsetzung von Seite 1

Was zum Ausschluss der Manager geführt hat, ist bislang nicht an die Öffentlichkeit gedrungen. Ansink und Seeger waren zumindest Anfang 2006 noch – wie auch andere Bearingpoint-Manager – an der Firma Prodim beteiligt, die oft als Subunternehmen verpflichtet wurde.

Ansink klagte gegen seine fristlose Kündigung und bekam Recht. Seit Ende Oktober ist er wieder – zumindest formell – als Managing Director bei Bearingpoint beschäftigt. „Ob er je wirklich für Bearingpoint arbeiten wird, bezweifle ich“, sagte ein dem Unternehmen nahe stehender IT-Berater. Der Bearingpoint-Sprecher erklärte dazu: „Zu laufenden Verfahren geben wir keine Stellungnahme ab.“

Einen zweiten Rechtsstreit konnte das Unternehmen dagegen zunächst gewinnen. Ein Aufsichtsratsmitglied aus der Arbeitnehmerschaft, das als Con-

sultant am Standort Leipzig arbeitet, hielt die Aufsichtsratsitzung vom Dezember 2005, in der die fristlose Kündigung von Ansink und Seeger beschlossen worden war, für nicht rechtmäßig und erhob Anklage.

Schließungspläne aufgegeben

Warum und mit welcher Begründung der Einspruch eingereicht wurde, ist unklar, die Klage wurde jedoch abgewiesen. Ansink galt als Förderer des Bearingpoint-Standorts Leipzig. Mit rund 40 Mitarbeitern handelt es sich um die kleinste Niederlassung des IT-Beratungshauses. Sie stand unabhängig von ihrer wirtschaftlichen Leistung immer zur Diskussion.

Die Geschäftsführung präsentierte den Mitarbeitern im vergangenen Sommer den Plan, den ostdeutschen Standort abzuwickeln. Laut einer anonymen Quelle verfolgte das Manage-

ment damit das Ziel, im Zuge der Schließung das dort beschäftigte Aufsichtsratsmitglied zu entlassen, weil die Unternehmensführung trotz einer Abwehr der ersten Klage eine Fortsetzung des Rechtsstreits befürchtete. „Die Schlussfolgerung ist denkbar, aber sehr gewagt“, urteilte ein IT-Berater aus dem Umfeld des Unternehmens. Er bestätigte jedoch Mobbing-Vorwürfe gegen das Aufsichtsratsmitglied.

Die Schließungspläne gab Bearingpoint nach Verhandlungen mit der Arbeitnehmervertretung auf. Der Betriebsrat konnte der Geschäftsführung einige Zugeständnisse abringen, was die Kosten der Stilllegung in die Höhe getrieben hätte. „Es gibt keine Pläne zur Schließung des Standortes Leipzig“, sagte der Bearingpoint-Sprecher. Auf die Frage, ob es in der Vergangenheit entsprechende Vorhaben gab, hieß es: „Kein Kommentar.“ (jha) ♦

FRAGE DER WOCHE
Werden Server auf Basis von x64 und Linux die herkömmlichen RISC/Unix-Systeme ablösen?



Telekom in der Krise

*Auf Ricke-Nachfolger René Obermann wartet eine Herkules-Aufgabe:
Das einstige Vorzeigunternehmen gilt als wenig kundenorientiert und technisch rückständig.*



Kann der neue Telekom-Chef René Obermann den Konzern wieder auf Kurs bringen?



Kai-Uwe Ricke hat den Schuldenabbau vorangetrieben. Doch die Telekom hat an Konkurrenzfähigkeit verloren.

VON CW-REDAKTEUR JÜRGEN HILL

Die Börsenzahlen spiegeln die Lage der Telekom nur bedingt wider. So wie der Carrier jetzt unter Kai-Uwe Ricke ein verkorkstes drittes Quartal mit einem Gewinnrückgang um 34 Prozent hinlegte, so schrieb der Konzern unter seiner Führung im Jahr 2005 noch einen Nettoprofit von rund 4,6 Milliarden Euro. Doch auch diese Zahl kann nicht darüber hinwegtäuschen, dass es im Telekom-Gebälk mächtig knirscht.

»Die Telekom hat bei vielen Kunden ein schlechtes Image.«

Das Unternehmen, das sich einst mit der schnellen Einführung von ISDN oder den TV-Kabelverteilernetzen sowie dem Glasfaserausbau in den neuen Bundesländern einen Ruf als technischer Vorreiter erarbeitete, gilt heute in Europa als Sanierungsfall. Während sich andere europäische Carrier der Herausforderung des liberalisierten TK-Marktes mit neuen Technologien gestellt haben, konzentrierte sich der deutsche Ex-Monopolist auf die Defensive. Machterhalt war das Thema, es galt lästige Konkurrenten abzuwehren – zur Not auch mit juristischen Winkelzügen, etwa der Lex Telekom in Sachen VDSL.

Auf den neuen Telekom-Chef René Obermann kommt nun viel

Arbeit zu. 1,5 Millionen Kunden liefen dem Konzern im Festnetzgeschäft seit Jahresbeginn weg, nicht nur weil die Konkurrenz mit günstigeren Angeboten lockt und die Telekom trotz Rickes „Bierdeckel“-Offensive im Frühjahr noch immer keine transparente Preispolitik vorweisen kann. Vielmehr haben die Bonner bei vielen Kunden ein schlechtes Image.

Unzufriedene Kunden

So kritisieren Benutzer den Support der Telekom-Hotlines häufig als mangelhaft, weil sie den Eindruck haben, dass dort die linke Hand nicht weiß, was die rechte tut. Zu dem negativen Bild der Telekom trugen auch die Heidelberger Rechtsanwälte Seiler und Kollegen bei, die im Auftrag des Konzerns offene Rechnungen eintreiben sollen. In zahlreichen Internet-Foren beklagen sich die Kunden darüber, dass sie selbst dann Mahnschreiben erhalten hätten, wenn sie vorher gegen die Rechnung Einspruch einlegten. Verärgerte Nutzer setzen dieses Geschäftsgebahren auch mal mit dem berühmtesten „Moskau-Inkasso“ gleich. Andere berichten, dass sie nach einem Anruf bei der Telekom-Hotline plötzlich eine der zahlreichen kostenpflichtigen Tarifoptionen auf ihrer Rechnung fanden, obwohl sie diese nie geordert hatten.

Weitere Kunden vergrault der Carrier mit seiner konservativen DSL-Politik, wie Beschwerden in zahlreichen Internet-Foren zeigen. Während die Telekom den künftigen Nutzern des schnellen

Internet-Zugangs aufgrund einer zu langen Telefonleitung häufig mit „DSL light“ nur eine gebremste Variante schalten will, lockt die Konkurrenz mit Transferraten von 2 bis 6 Mbit/s.

In Sachen DSL blamierte sich der Carrier im Sommer gründlich, als der Startschuss für das neue VDSL-Netz praktisch unter Ausschluss der Öffentlichkeit fiel. Zudem zweifeln viele Experten am Sinn der unter Ricke beschlossenen Milliardeninvestitionen in VDSL. In ihren Augen handelt es sich schon jetzt um eine veraltete Technik, die Zukunft gehöre den Glasfasernetzen bis zum Endkunden (fibre to the home). Auch bei einer anderen potenziellen Zukunftstechnologie ist der Bonner Konzern nicht mit von der Partie: An der für Dezember angesetzten Versteigerung von Funkfrequenzen für den breitbandigen Internet-Zugang beteiligt sich der Kon-

»Experten zweifeln am Sinn der Milliardeninvestitionen in VDSL.«

zern nicht. Die dabei verwendete Wimax-Technologie wird in Branchenkreisen als eine günstige DSL-Alternative gesehen, um die letzte Meile zum Kunden drahtlos zu überbrücken.

Technische und strategische Fehlentscheidungen sind jedoch nicht die einzigen Probleme, mit denen der neue Telekom-Chef Obermann fertig werden muss.

Schwer wiegt auch die Erblast, die noch immer auf dem einstigen Staatskonzern liegt. Verärgerte Mitarbeiter berichten beispielsweise immer wieder, dass es noch eine Zweiklassengesellschaft mit Beamten aus den früheren Postmonopol-Zeiten und den normalen Angestellten auf der anderen Seite gebe.

Demotivierte Mitarbeiter

Deshalb sei es kein Wunder, dass viele Angestellte – bedingt durch die Dauerangst um ihren Arbeitsplatz – wenig motiviert seien. Als weitere Spaßbremse gelten die internen Entscheidungsstrukturen des Konzerns. So hätten die Service- und Außendienstmitarbeiter, die alltäglich mit den Problemen der Kunden konfrontiert sind, meist keine Entscheidungsbefugnis und müssten bei jeder Kleinigkeit im Backoffice nachfragen. Erschwerend komme hinzu, dass der Konzern im Vergleich zur Konkurrenz seine Dienstleistungen zu teuer produziere, da er den Beschäftigten in den Call-Centern und an den Hotlines den kostspieligen Telekom-Tarif bezahle.

Selbst der Mobilfunkbereich, unter der Führung des neuen Telekom-Chefs Obermann zur Vorzeigesparte des Konzerns avanciert, glänzt lediglich auf dem Papier. Wirklich erfolgreich sind die Mobilfunke nur in den USA. In heimischen Gefilden sind sie dagegen eher Getriebene. Beim innovativen Datenfunk mit UMTS und HSDPA stahl Vodafone den Bonnern die Show. Und bei der Jagd nach

dem jungen Publikum, das als vielversprechende Zielgruppe gilt, überflügelte O₂ mit seinem frischeren Auftritt den ehemaligen Monopolisten. Geht es dagegen um die Preisführerschaft, so kann E-Plus mit seinen pauschalen Base-Angeboten bei den Kunden punkten. Kritik erfahren die T-Mobilfunke auch von der lukrativen Business-Klientel. Sie fühlt sich von T-Mobile – allerdings auch von den anderen Mobilfunkern – mit ihren Problemen alleine gelassen, und dies obwohl T-Mobile im Unter-

»T-Systems hat Trends wie VoIP oder Offshoring verschlafen.«

nehmensgeschäft auf die Unterstützung des hauseigenen IT-Dienstleisters T-Systems zurückgreifen kann.

Allerdings hat T-Systems selbst mit genügend Problemen zu kämpfen. So verschief das Unternehmen wichtige Trends wie etwa das Offshoring. Zudem sprang der Anbieter, der stark von Einnahmen aus TK-Services abhängig ist, aus nachvollziehbaren Gründen erst spät auf den VoIP-Zug auf. Des Weiteren belasten margenschwache Services wie etwa PC-Support oder das Hosting die Bilanz.

Selbst für Obermann, der intern den Spitznamen „Bulldozer“ trägt, dürfte es schwer werden, den Konzern in kurzer Zeit wieder auf Kurs zu bringen. ♦

SECURITY-EXPERTENRAT

Ein Wissens-Blog der COMPUTERWOCHE

Mit dem Security-Expertenrat startet die COMPUTERWOCHE einen Wissens-Blog rund um das Thema IT-Sicherheit. Zum Auftakt geht das Gremium auf die aktuell größten Bedrohungen für die IT und die damit verbundenen Herausforderungen ein.



Klaus-Peter Kossakowski, Geschäftsführer DFN-Cert Services GmbH.



Sachar Paulus, CSO, SAP AG.



Claudia Eckert, Leiterin des Fraunhofer Instituts für Sichere Informationstechnologie (SIT), TU Darmstadt.



Alexander Tsolkas, CSO, Schenker AG.



Wolfram Funk, Senior Advisor ICT-Service, Experton Group.

Wo die IT-Gefahren lauern

Angesichts der zunehmenden Komplexität der IT und dem anhaltenden Kostendruck ist es für Unternehmen alles andere als einfach, ihre technische Infrastruktur sowie sensible Firmeninformationen angemessen vor Angriffen zu schützen. Es gilt, die sich ständig wandelnden Bedrohungsszenarien im Auge zu behalten und abzuwägen, inwieweit sie für die eigene Organisation ein Risiko darstellen. Die Mitglieder des Security-Expertenrats antworten zum Auftakt auf die Frage: „Was sind aktuell die größten IT-Bedrohungen für Unternehmen?“

„Angst ist das falsche Gefühl“

Klaus-Peter Kossakowski, Geschäftsführer DFN-Cert Services

Zwei große Probleme, die sich nicht an der Technik festmachen lassen, sind Angst und Geld. Zunächst zur Angst: Da sie mitunter Menschen antreibt, sind Berater allzu leicht versucht, mit einem Schreckgespenst hausieren zu gehen, um „ihr“ Produkt schnell an den Menschen zu bringen. Angst ist aber genau das falsche Gefühl und hilft niemandem weiter. Vielmehr ist Respekt angesagt, denn niemand sollte sagen: „Das passiert uns doch nicht!“ Angesichts immer neuer Bedrohungen – und damit neuen Sicherheitsprodukten – gilt es für den Entscheider, einen kühlen Kopf zu behalten und sauber abzuwägen, wie ein ganzheitliches und ausgewogenes Risiko-Management aussehen muss, das nachhaltige Lösungen bevorzugt.

Natürlich lässt sich dies nur mit Hilfe von Ressourcen (also Geld) erreichen. Während Entscheider aber immer wieder über zu geringe Mittel klagen, wird auch viel Geld verschwendet – indem kurzfristige Teillösungen unter Missachtung anderer Aspekte und nicht gelöster Integrationsprobleme priorisiert, oder Projekte angefangen und einfach nicht zu Ende geführt werden. IT-Sicherheit ist kein kurzlebiger Zeitvertreib, der sich immer mit den neuesten Dingen beschäftigen darf, sondern eine langfristige Tätigkeit mit vielen Routineaufgaben und einer ganzen Reihe schlicht langweiliger Hausaufgaben.

Und weil wir in Deutschland sind, ist noch ein anderer Aspekt wichtig: Es geht nicht um die perfekte Sicherheit. Selbst Security darf nur „gut genug“, sprich: der Situation angemessen sein. Stattdessen liegt der Fokus häufig zu sehr auf einzelnen Problemen – etwa nach dem Motto: „Wenn wir hierfür noch etwas mehr aufwenden, dann sind wir sicher.“ Anderes, manchmal sogar noch Wichtigeres, fällt dabei unter den Tisch.

„Verteidigungsmaßnahmen anpassen“

Sachar Paulus, CSO, SAP

Galten bisher Virus- und Wurmmattacken als Hauptbedrohung, stellt der Einsatz „zielgerichteter Malware“ mittlerweile eine weitaus größere Gefahr dar. Statt IT-Systeme lahm zu legen, zielt diese Malware darauf ab, Passwörter auszuspähen oder Web-Server mit illegalen Inhalten zu betreiben. Würden Würmer oder Viren noch von „Script Kids“ verbreitet, ist nun das organisierte Verbrechen auf dem Vormarsch, das Schwachstellen in IT-Systemen ausnutzt, um schnell an Geld zu kommen. Besonders bedrohlich sind dabei die „Phishing-Attacken“. Heutige Sicherheitslösungen spüren die hierzu eingesetzte Software oft nicht auf – die Erkennungsrate liegt gerade einmal zwischen 30 und 40 Prozent.

Parallel zu dem sich wandelnden Bedrohungspotenzial muss sich auch die Verteidigung ändern. Als größtmögliche Schäden stehen nicht mehr Ausfallzeiten im Fokus. Was heute und künftig ganz oben auf der Sicherheitsagenda der Unternehmen stehen sollte, ist der Schutz von geistigem Eigentum – und Wettbewerbsvorteilen. Das bedeutet zweierlei: 1. Das Thema Sicherheit treibt ist nicht mehr ausschließlich die IT voran (schließlich ist diese vor allem daran interessiert, Service-Levels sicherzustellen), sondern eher eine Corporate Security, ein Risiko-Management oder auch eine Rechtsabteilung. 2. Die Angriffsmethoden ändern sich, folglich ist dem Problem mit einem rein technischen Ansatz nicht beizukommen.

„Mit der Mobilität steigt die Anzahl der Angriffsziele“

Claudia Eckert, Fraunhofer-Institut für Sichere Informationstechnologie (SIT), TU Darmstadt

Die größten Sicherheitsbedrohungen ergeben sich durch die zunehmende Mobilität und Vernetzung der IT-Systeme. Die dadurch stetig wachsende Komplexität der IT-Landschaften stellt hohe Anforderungen an das Management und die zuständigen Fachabteilungen.

Mobile Endgeräte wie Handys, PDAs oder Laptops mit ihren mangelhaften Sicherheitsdiensten stellen nach wie vor eine Bedrohung für die Unternehmenssicherheit dar, da klare Nutzungsvorgaben meist fehlen oder aufgrund dezentraler Administration nicht konsequent eingehalten

werden. Die Grenze zwischen innen (geschütztes Unternehmensnetz) und außen (Internet) verschwimmt, wodurch sich die Zahl der Angriffsziele erhöht und die Gefahr eines Informationsdiebstahls etwa über Phishing-Angriffe steigt.

Der Übergang zu einer Prozess- oder Service-orientierten Informationsverarbeitung in dezentralen Service-orientierten Architekturen (SOA) konfrontiert Firmen zudem mit immer mehr Abhängigkeiten. Diesen werden von unterschiedlichen, zum Teil wechselnden Partnern angeboten. Dabei ist offen, welches Sicherheitsniveau die Serviceanbieter garantieren können, was aufgrund der steigenden Compliance-Anforderungen zu neuen Unwägbarkeiten führt.

Zu den entscheidenden Herausforderungen für Industrie und Forschung zählt die

Security-Expertenrat – ein Wissens-Blog

Welchen Stellenwert hat das Thema IT-Security in der deutschen Firmenschaft? Wo liegen die größten Risiken und Bedrohungen, welche technischen Trends sind relevant, und wie können sich Anwender angemessen schützen?

Mit Fragen wie diesen beschäftigt sich der Security-Expertenrat der COMPUTERWOCHE. Mitglieder des Gremiums sind hochkarätige Spezialisten aus Anwenderunternehmen, Forschungseinrichtungen, Beratungshäusern sowie der IT-Industrie.



Katharina F. Moderatorin Expertenrat

Entwicklung von Lösungen für die nahtlose Zusammenarbeit unterschiedlicher IT-Systeme und Netze. Hinzu kommen Sicherheitstechniken, die mit der Dynamik der Ad-Hoc-Vernetzung und der zunehmenden Dezentralität der Dokumenten- und Informationsverarbeitung Schritt halten.

„Mangel an Security-Awareness“

Alexander Tsolkas, CSO, Schenker AG

Fehlendes IT-Sicherheitsbewusstsein stellt die größte Bedrohung für den Erfolg einer IT-Security-Strategie dar. Die nötige Aufgeschlossenheit ist bei Mitarbeitern und Dritten nicht durchgängig vorhanden. So erfolgt der Umgang mit Informationen und Sicherheitstechnik häufig nicht nach vorgegebenen Richtlinien, sondern willkürlich.

Was noch schlimmer ist: Nicht selten werden Prozesse und IT-Sicherheitstechnik dabei kreativ umgangen.

An zweiter Stelle stehen potenzielle Bedrohungen bei IT-gestützten Geschäftsprozessen. Ein Beispiel hierfür sind definierte Business- beziehungsweise Security-Abläufe, die umgangen werden. Sehr oft wirkt die IT-Sicherheit bei Geschäftsprozessen störend und verlangsamt und wird deshalb ausgehebelt. Technische Schnittstellen zwischen Geschäftsabläufen, die insbesondere bei abteilungsorientierten Unternehmen Medienbrüche hervorrufen, können das IT-Sicherheitsniveau nicht durchgängig abbilden und bieten somit Angriffsflächen.

Eine weitere ernst zu nehmende Gefahr geht von der zunehmenden IT-Komplexität aus. So entstehen Bedrohungen, die zuvor in reinen IP-Netzen nicht vorhanden waren. Beispiele hierfür sind „Spam over Internet Telephony“ (SPIT) in Voice over IP bei Multi-Service-Netzen, aber auch der gesamte Bereich Web-Services mit seinen Bedrohungen etwa durch die fehlende Perimetersicherheit. Daher heißt es: Aufgepasst auf die Kronjuwelen!

„Malware sucht sich neue Zielplattformen“

Wolfram Funk, Senior Advisor ICT-Service, Experton Group

Die größte externe Bedrohung für Unternehmen besteht aktuell in der zunehmenden Ausgefeiltheit der immer häufiger wirtschaftlich motivierten „Malware“-Angriffen, die künftig auch vor neuen Zielplattformen wie Linux oder mobilen Lösungen nicht Halt machen werden. Eine große Herausforderung für Anwenderunternehmen ist dabei die plattformübergreifende Automatisierung und Verwaltung von Security-Patch-Prozessen.

Wissens-Blog der COMPUTERWOCHE

Ihre Vorteile:

Hochwertiges Expertenwissen, die besten Fachartikel aus der COMPUTERWOCHE und andere Informationsquellen rund um das Thema IT-Sicherheit – auf einen Blick. Als Wissens-Blog bietet der Expertenrat (www.computerwoche.de/security-expertenrat) sowohl eine Knowledge-Basis als auch eine interaktive Plattform für die Security-Community. Diskutieren Sie mit, veröffentlichen Sie eigene Beiträge und stellen Sie Fragen an die Mitglieder des Expertenrats. Auf Seite 8 erfahren Sie, wie der Blog funktioniert.

Christina Friedmann, Vorsitzende des Expertenrats.

Nachdem sich die IT-Sicherheit lange Zeit primär auf Netze konzentriert hat, rückt nun auch die Anwendungssicherheit in den Vordergrund. Hier geht es insbesondere um Security für ERP, Datenbanken, Portale und Service-orientierte Architekturen (SOA). Dabei spielen auch Elemente des Identity-Managements eine wichtige Rolle, die unter anderem den internen und externen Missbrauch von Nutzerrechten verhindern sollen.

Weitere Herausforderungen liegen in der zunehmenden Relevanz regulatorischer Anforderungen in Deutschland und den entsprechenden Anforderungen an die Automatisierung und Dokumentation von Compliance-Prozessen. Insgesamt tun sich die Unternehmen bei der Priorisierung von Sicherheitsinvestitionen schwer – hier müssen regelmäßige Risk-Assessments zum Standard werden.

„Reaktionsfähigkeit auf dem Prüfstand“

Michael Hoos, Technischer Direktor Central Emea, Symantec

Eine Entwicklung, die Unternehmen zunehmend Sorgen bereitet, ist die Professionalisierung der Internet-Kriminalität. Es geht nicht mehr nur um wahllose Attacken durch E-Mail-Würmer, die Netze überlasten oder lahm legen, vielmehr werden Firmen gezielt unter Androhung von Denial-of-Service-Attacken oder der Verschlüsselung wichtiger Firmendokumente erpresst. Während auffällige Virusattacken oft schnell erkannt und Gegenmaßnahmen eingeleitet werden konnten, arbeiten Internet-Kriminelle heute subtiler, so dass die Reaktionsfähigkeit der Unternehmen auf die Probe gestellt wird. Proaktive Maßnahmen wie eine umfassende Security-Richtlinie und Maßnahmen, um die Konformität der Endgeräte mit den aufgesetzten Policies sicherzustellen, sind daher heute besonders wichtig. Durch ein strategisches Business-Continuity-Management ist es zudem möglich, Sicherheitsstrukturen zu implementieren, mit denen im Ernstfall nicht unnötig Zeit verloren geht.

Eine weitere, aktuelle Herausforderung ist der Umgang mit Instant Messaging (IM), dem derzeit am schnellsten wachsenden Kommunikationsmedium. Bei IM erfolgt nicht nur die Kommunikation in Echtzeit: Sobald auch nur ein Computer infiziert ist, kann sich Schadcode rasant im gesamten IT-Netz verbreiten. Die Zunahme der IM-Sicherheitsvorfälle um mehr als 1600 Prozent im Jahr 2005 spricht eine klare Sprache. Nur durch die Implementierung eines ganzheitlichen Enterprise-Messaging-Managements können Unternehmen auf diese Bedrohungen reagieren.

„Das Rückgrat des Unternehmens schützen“

Klaus Lenssen, Senior Business Development Manager Security and Government Affairs, Cisco Deutschland

Datenschutz oder neu-deutsch „Data Leakage Prevention“ zählt heute zu den größten Herausforderungen der Unternehmen – insbesondere vor dem Hintergrund, dass sie immer mehr gesetzlichen Regelungen (Compliance) unterworfen sind. Angriffe auf Firmennetze zielen heute nicht mehr darauf ab, die IT-Infrastruktur auszuschalten oder willkürlich Schäden zu verursachen. Vielmehr geht es Hackern darum, sich unbemerkt in funktionierende Infrastrukturen einzuklinken, um dort Informationen abzugreifen. Der klassische Perimeter, wie von Cheswick und Bellowin in ihrem Firewall-Klassiker definiert, existiert eigentlich nicht mehr. Firmennetze sind heute Netze von Netzen ohne klare Begrenzungen – durch die Wireless-Technologie oftmals sogar ohne physische. Das alles verbindende Netz bildet jedoch das Rückgrat des Unternehmens. Da hierbei jedes Element ein potenzielles Angriffsziel ist, sollte es entsprechend geschützt werden und möglichst zum Schutz anderer beitragen.

IT-Sicherheit kann heute aber nicht mehr nur im Netz oder nur auf Anwendungs- oder Endgeräteeite realisiert werden. Schwachstellen auf dem Endgerät bieten Angriffsflächen für Malware, die dann den Rechner kapern und in einen „Bot“ verwandeln kann. Im Verbund stellen diese Bots eine Gefahr für das Netz und damit das gesamte Unternehmen dar. Nur durch eine integrierte Betrachtung des Themas Sicherheit und die Einbindung entsprechender Maßnahmen in ein intelligentes Netz können sich Firmen angemessen schützen und Datenschutz sowie Compliance realisieren.

ung des Themas Sicherheit und die Einbindung entsprechender Maßnahmen in ein intelligentes Netz können sich Firmen angemessen schützen und Datenschutz sowie Compliance realisieren.

„Achillesferse Applikationen“

Stefan Strobel, Geschäftsführer, Cirosec

Eine der größten Herausforderungen für die IT-Sicherheit in Unternehmen ist die zunehmende Öffnung von Applikationen für externe Partner, Kunden und Lieferanten über das Internet.

Der klassische Fokus auf die Perimeter-Absicherung mit Firewalls und Virenschutz-Gateways führt zu einem trügerischen Gefühl von Sicherheit. Oft werden komplizierte und teure DMZ-Strukturen aufgebaut, aber die Bedrohungen auf der Applikationsebene aus Unkenntnis der modernen Angriffstechniken vernachlässigt. So lassen sich beispielsweise mit Methoden wie SQL Injection, Cross Site Scripting oder Session Fixation Portalsysteme hacken, die nur für eine kleine Benutzergruppe gedacht sind und über starke Authentisierung verfügen. Dabei kann ein Angreifer meist auf vertrauliche Daten aus den Backend-Systemen zugreifen.

Selbstverständlich ist dies nur ein Beispiel für eine aktuelle und wichtige Bedrohung der IT und trifft nicht auf jede Organisation zu. Wer keine Applikationen mit Web-Zugriff betreibt, für den existiert diese Bedrohung auch nicht. In diesem Fall sind dann eventuell andere Bedrohungen etwa für interne vertrauliche Daten viel wichtiger.

Eine allgemeingültige Top-Ten der wichtigsten Bedrohungen für die IT ist demnach nur statistisch begründet und lässt sich nicht auf einzelne Organisationen übertragen. Wer seine eigenen gefährlichsten Bedrohungen kennen möchte, der kommt um eine individuelle Bedrohungs- und Risikoanalyse nicht herum.

„Web-basierende Gefahren auf dem Vormarsch“

Rainer Link, Senior Security Specialist Anti-Malware, Trend Micro

Das aktuelle Bedrohungsszenario stellt sich besonders variantenreich dar, zugleich sind die Angriffe heute zielgerichteter als früher.

Neben der klassischen Verbreitung von Malware via E-Mail – sei es durch eine eigene Verbreitungsroutine oder das so genannte Spamming/Seeding – nimmt die Anzahl der Web-basierenden Bedrohungen immer mehr zu. Dies können Angriffe sein, die Sicherheitslücken in Browsern ausnutzen, oder Attacken mit Hilfe gefälschter oder nachgemachter Web-Seiten (Stichwort: Phishing) – oder, als aktuelles Beispiel, ein gefälschter Wikipedia-Artikel, der einen modifizierten Microsoft-Patch zum Herunterladen anbietet.

Möglich sind auch Kombinationen der beschriebenen Bedrohungen: Auf den ersten Blick landet man auf einer typischen Phishing-Web-Seite. Über eine Sicherheitslücke wird jedoch gleichzeitig versucht, heimlich im Hintergrund Ad- oder Spyware auf dem System zu installieren, die sich dann über ein Rootkit noch möglichst tief ins System eingräbt. Als Vertreter komplexerer Web-basierender Malware wären etwa die „Gromzom“- oder „Stration“-Familie zu nennen. Darüber hinaus stellen Bot-Netze eine anhaltende Gefahr dar – die Anzahl steigt ständig, und vielfach bleibt unbemerkt, dass Computer als „Zombies“ bereits Teil eines Bot-Netzes sind.

Fortsetzung auf Seite 8



Michael Hoos, Technischer Direktor Central Emea, Symantec.



Klaus Lenssen, Senior Business Development Manager Security and Government Affairs, Cisco Deutschland.



Stefan Strobel, Geschäftsführer, Cirosec GmbH.



Rainer Link, Senior Security Specialist Anti-Malware, Trend Micro.



Karsten Weronek, Senior Executive Manager Corporate Information Management, Fraport AG.



Reinhard Bertram, Leiter Competence Center Security Services, SBS.