

# COMPUTERWOCHE

NACHRICHTEN ♦ ANALYSEN ♦ TRENDS



**RECHT**

## Datenschutz ist Pflicht

Mit dem Datenschutz nehmen es viele Unternehmen – auch mangels behördlicher Kontrolle – nicht so genau. Doch das Risiko ist groß. **SEITE 43**



**SERVICEMARKT**

## Marktlücke Open Source

Immer mehr IT-Dienstleister bieten Open-Source-Services an. Richtig so, meint Techconsult-Analyst Denis Mrksa: Der Markt brummt. **SEITE 48**



**INTERVIEW**

## „Orks und Workaholics“

Für IBM-Querdenker Gunter Dueck sind Druck und „Stressfabriken“ ungeeignet, um IT-Beschäftigte zu Höchstleistungen zu animieren. **SEITE 53**

**COMPUTERWOCHE TV**

**CWTV** Professor Helmut Kremar, TU München  
Wem hilft eigentlich der Bachelor?

♦ **CA zieht sich aus dem Sumpf**

Thomas Leitner, Geschäftsführer von CA Deutschland, hat die Vergangenheit abgehakt.

♦ **Linguatec Voice Reader**

Die Software wandelt Text in Sprache um und ist gut in Office integriert.

**ZAHL DER WOCHE**

**60 Millionen** EU-Bürger (13 Prozent) verfügen über einen breitbandigen Internet-Anschluss. Das berichtet die EU-Kommission in ihrem ersten Jahresbericht zur europäischen Informationsgesellschaft. Europa liege jedoch in der IKT-Forschung weit hinter den USA, Japan und China zurück. Außerdem nutzten Firmen die Chancen durch moderne Informationstechnik zu wenig. „Insgesamt gibt es keinerlei Anzeichen für eine Trendwende oder eine beschleunigte IKT-Entwicklung, die ein dauerhaftes Wachstum und eine Wettbewerbsstärkung für die EU erwarten ließen.“

## Postbank übernimmt HVB-Zahlungsverkehr

Voraussichtlich ab Herbst dieses Jahres wird die Postbank den inländischen Zahlungsverkehr für die Hypovereinsbank (HVB) erledigen. In Rahmen des Outsourcing-Abkommens übernimmt sie wohl auch die derzeit 500 Köpfe starken HVB Payment Services (PAS). Die Details des Vertrags sind aber noch auszuhandeln. Ähnliche Deals hat die Postbank mit der Deutschen und der Dresdner Bank geschlossen. Auf diese Weise wickelte sie im vergangenen Jahr sechs Milliarden Zahlungsvorgänge ab. (qua) ♦

# Das größte Risiko ist der Anwender

*Von Viren, Würmern und Hackern ist viel die Rede, doch Experten sind sich einig: Das Problem sind die Menschen im eigenen Unternehmen.*

**D**as Thema Sicherheit treibt IT-Manager in Zeiten globaler Vernetzung mehr um als jedes andere. Die COMPUTERWOCHE startet mit dieser Ausgabe eine Serie zum Thema (siehe Seite 6). Im ersten Beitrag geht es um den vielleicht sensibelsten Punkt: Wie können Unternehmen das größte Sicherheitsrisiko beherrschen, den Anwender selbst?

Wie groß die Bedrohung ist, zeigt etwa eine Untersuchung des US National Reconnaissance Office (NRO), eine Behörde des amerikanischen Verteidigungsministeriums, die US-Unternehmen unter die Lupe genommen hat. Danach ist der Schaden, den Firmenmitarbeiter durch Fehlverhalten und andere sicherheitsrelevante Verstöße verursachen, um ein Vielfaches höher, als der durch externe Angreifer verursachte. Während Letztere durch ih-



re Aktivitäten jährliche Kosten von durchschnittlich 56 000 Dollar pro Unternehmen verursachen, schlagen absichtliche oder fahrlässige Fehler der Mitarbeiter mit rund zwei Millionen Dollar zu Buche.

Die Marktforscher von IDC bestätigen den Trend im Grundsatz. Allerdings, so die Marktforscher, scheinen die Unternehmen diese Bedrohung allmählich zu erkennen. Im November 2005 befragten sie IT-Verantwortliche in aller Welt und fanden heraus, dass diese ihre Mitarbeiter in diesem Jahr intensiv zur Einhaltung firmeninterner Sicherheitsrichtlinien anhalten wollen.

Zu den dringlichsten Aufgaben zählt dabei wohl der Umgang mit vertraulichen Passwörtern. Der britische Security-Spezialist Sophos sieht darin ein großes Problem: Unternehmen machen es sich bei der Vergabe zu einfach – und damit auch internen und externen Angreifern. (jm) ♦

## Allianz gegen Google

*Ebay und Yahoo haben eine Partnerschaft für E-Commerce vereinbart. Sie wollen damit Google unter Druck setzen.*

**D**ie beiden Unternehmen nannten als Gebiete ihrer Kooperation ganz allgemein E-Commerce, Online-Werbung und Suche. Konkret vereinbarten sie, dass Yahoo künftig die Suchfunktionen für das Auktionshaus anbieten wird und dort exklusiv kontextabhängige Werbung schalten darf. Umgekehrt wird Yahoo ausschließlich den zu Ebay gehörenden Bezahlservice „Paypal“ nutzen, um seine Dienstleistungen gegenüber den Kunden abzurechnen. Paypal soll außerdem in die Angebote von Partnern, etwa Händlern oder Content-Anbietern, integriert werden. Yahoo gibt im Zuge dessen sei-

nen eigenen erfolglosen Service „Paydirect“ auf. Zusätzlich beabsichtigt Ebay, die Suchfunktionen von Yahoo in seine Browser-Erweiterung („Toolbar“) aufzunehmen. Die Web-Companies wollen außerdem Möglichkeiten eruiieren, auf Basis von „Skype“ und „Yahoo Messenger“ bei der Internet-Telefonie zusammenzuarbeiten.

Nach allgemeiner Einschätzung richtet sich die Kooperation vor allem gegen Google, das Yahoo in den letzten Jahren erhebliche Anteile im Such- und Werbemarkt abgenommen hat.

**Fortsetzung auf Seite 4**

**DIESE WOCHE**



## IBMs Collaboration-Pläne

Auf der DNUJ ließ IBMs General Manager Mike Rhodin bezüglich der Zukunft von Notes und Workplace viele Fragen offen. **Nachrichten SEITE 8**

## Lünendonks Liste ist da

SAP behauptet sich als führendes Softwarehaus – dank einer neuen Erhebungsmethode allerdings nur noch knapp. **Business Report SEITE 12**

## Oracle bedient SAP-Anwender

Um dem Rivalen Kunden abzugewinnen, will Oracle künftig Supportleistungen für die SAP-Klientel bieten. **Nachrichten SEITE 13**

## Zeit für die Bestandsaufnahme

Wer seine IT auslagern will, sollte zuvor die Ausgangslage betriebswirtschaftlich bestimmen. „Baselining“ ist Pflicht. **Schwerpunkt SEITE 28**

## Mieses Klima in IT-Shops

In der IT gibt es viele Führungskräfte, die diese Bezeichnung nicht verdienen. Sie sind über ihr IT-Know-how in die Managerrolle geraten. **Karriere SEITE 50**



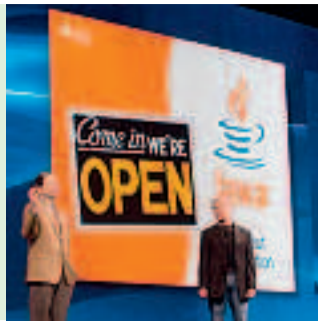


**Schlägt die Telekom zu? 5**

Telekom-Chef Kai-Uwe Rieke will angeblich bei der britischen BT Group einsteigen. Insbesondere die Service-sparte solle es dem Bonner Carrier angetan haben.

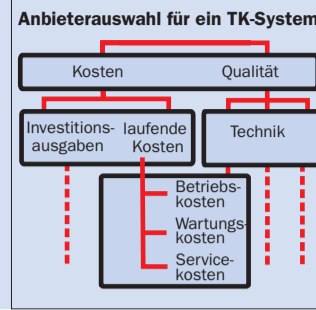
**Die Zukunft von Java 16**

Was Java EE 5 leistet und wie Suns Pläne für die Plattform in Bezug auf Trendthemen wie SOA, Web 2.0 und Open Source aussehen.



**Services lassen sich bewerten 28**

Betriebswirtschaftliche Methoden schaffen eine Basis für Outsourcing-Entscheidungen. Der Ist-Zustand (Baseline) dient als Referenzpunkt.



**NACHRICHTEN**

**Hummingbird wird geschluckt 5**  
Die Symphony Technology Group zahlt 465 Millionen Dollar für den Enterprise-Content-Management-Spezialisten.

**Salesforce.com lädt OEM-Partner ein 10**  
Der On-Demand-Pionier stellt seine technische Plattform gegen Gebühr zur Verfügung.

**WM 2006: Yahoo regiert im Web 15**  
Im Auftrag der FIFA will das Internet-Unternehmen die Infrastruktur für Milliarden Zugriffe schaffen.

**PRODUKTE & TECHNOLOGIEN**

**Unicenter aufgewertet 19**  
Mit der Clarity-Integration kommt eine Portfolio-Management- und IT-Governance-Lösung in die Suite.

**Zentrale Zugriffskontrolle 20**  
Secure Computing bringt eine Universal-Appliance für Identity- und Access-Management.

**Server für den VoIP-Einstieg 22**  
Die Telefonanlage von Tel2Web verbindet die Vorteile der Internet-Telefonie mit den Leistungsmerkmalen herkömmlicher TK-Installationen.

**Skalierbare Foundry-Switches 23**  
Die neuen Power-over-Ethernet-Modelle bieten laut Hersteller sehr flexible Upgrade-Möglichkeiten.

**PRODUKTE & TECHNOLOGIEN**

**PRAXIS**

**Ein Portal für SAP-Systeme 24**  
Warum das Stuttgarter Robert-Bosch-Krankenhaus Intrex statt Netweaver als Portallösung wählte und wie es seine R/3-Applikationen eingebunden hat.

**Microsoft DPM im Test 26**  
Der Data Protection Manager lässt sich als Kombination bekannter Konzepte der Datensicherung bezeichnen.

**CW-TOPICS: ERP**

**Wie SAP und Co ihre Plattformen öffnen und ausbauen. Eine Verlegerbeilage ab Seite 33**

**IT-STRATEGIEN**

**Datenschutzprüfung: mangelhaft 43**  
Viele Unternehmen wissen nicht einmal, welche Pflichten sie in Sachen Datenschutz haben. Das kann teuer werden.

**Flexibel durch Virtualisierung 46**  
Der Energieabrechnungs-Dienstleister Ista gewinnt Bewegungsfreiheit und spart Geld mit Hilfe einer virtualisierten Plattenspeicherumgebung.

**Funkchip am Krankenbett 47**  
Die Städtischen Kliniken Bielefeld experimentieren mit RFID-Technik, um die Auslastung ihrer Betten zu verbessern.

**IT-SERVICES**

**Open-Source-Anwender benötigen Hilfe 48**  
Der Trend, quelloffene Applikationen zu integrieren, erhöht die Komplexität von IT-Projekten.

**Provider müssen Technikwissen bieten 49**  
Immer seltener verpflichten Unternehmen externe Dienstleister, um Kosten zu sparen. Gefragt ist Unterstützung in technischen IT-Projekten.

**JOB & KARRIERE**

**Wenn Führungskräfte versagen 50**  
In vielen Unternehmen ist das Klima gestört. Statt an einem Strick zu ziehen, blockieren sich Vorgesetzte und Mitarbeiter gegenseitig.

**„Nur noch Orks und Workaholics“ 53**  
Der Zwang, ständig der Beste zu sein, fördert Depressionen und Burn-out.

**SCHWERPUNKT: BASELINING**

**Zehn Tipps für das Outsourcing 30**  
Jede IT-Dienstleistung ist nur so gut, wie sie in Auftrag gegeben wird. Wohl und Wehe einer Servicepartnerschaft entscheiden sich lange vor dem Start.

**Auslagern beginnt mit Benchmarks 31**  
Methoden des Baselineing helfen bei der Standortbestimmung, der Zieldefinition und der Entscheidungsvorbereitung.

**STANDARDS**

Impressum	47
Stellenmarkt	54
Zahlen - Prognosen - Trends	58

**COMPUTERWOCHE.de**

**HOTTOPICS**

- So gelingt die ERP-Einführung
- CW-Ranking: Die Top-IT-Unternehmen im April 2006
- Was ein Business-Notebook ausmacht

**Neuer Karriere-Ratgeber**



Ihre Fragen rund um die IT-Karriere beantwortet Frank Wuschech vom 1. bis 14. Juni im Online-Forum der COMPUTERWOCHE. Der Diplomkaufmann ist seit November 2004 Geschäftsführer des Softwareanbieters BasWare GmbH und verfügt über mehr als zwei Jahrzehnte Erfahrung in der IT-Branche.

[www.computerwoche.de/job\\_karriere/karriere\\_ratgeber](http://www.computerwoche.de/job_karriere/karriere_ratgeber)

**Frisch getestet: Jboss Portal 2.2.1**

Die Neuigkeiten im Portalprodukt von Jboss sowie Details zum Setup und zur Verwaltung hat der COMPUTERWOCHE Product Guide unter die Lupe genommen. [www.computerwoche.de/product\\_guide/plattformen](http://www.computerwoche.de/product_guide/plattformen)

**JETZT TESTEN! Neu mit COMPUTERWOCHE TV!**

**Mehr Infos, mehr Service, mehr Wissen**



Jetzt 4 Wochen kostenlos testen!  
[www.computerwoche.de/webtour](http://www.computerwoche.de/webtour)

Bei **COMPUTERWOCHE PREMIUM** auf [www.computerwoche.de](http://www.computerwoche.de) finden Sie alle wichtigen Informationen für die erfolgreiche Arbeit im IT-Business:

- 7 hoch informative Knowledge-Center zu den Bereichen ERP, Linux, VoIP, IT-Security, Wireless, IT-Services und RFID
- Ausgewählte Artikel der Printausgabe vorab online lesen.
- COMPUTERWOCHE Archiv
- Persönliches Archiv
- Marktübersichten
- Internationale News
- Kongressunterlagen der COMPUTERWOCHE Veranstaltungen
- Jeden Monat ein E-Books von Addison-Wesley, Pearson Studium oder Markt+Technik
- Ranking der 100 größten ITK-Unternehmen
- Whitepapers
- COMPUTERWOCHE TV
- u.v.m.



# MENSCHEN

## Stan Laurent verlässt AOL Europe



Hintergrund für den Rücktritt des COO ist einem Bericht des „Manager-Magazins“ zufolge die geplante Reorganisation des Unternehmens in Europa. Diese Rolle übernimmt jedoch Karen Thompson, bislang AOL-Chefin von Großbritannien. Laurent war erst Ende 2005 in die Europa-Zentrale von AOL nach Luxemburg gewechselt. Davor leitete der 37-jährige seit Oktober 2002 das Deutschland-Geschäft des Internet-Dienstleisters und führte es aus den roten Zahlen.

## Führungswechsel bei Nokia

Anfang Juni beginnt beim finnischen Handy-Riesen Nokia eine neue Zeitrechnung: Nach 14 Jahren an der Konzernspitze übergibt Jorma Ollila das Zepter an Olli-Pekka Kallasvuo (Foto) und zieht sich – mit 54 Jahren – in den Verwaltungsrat des Unternehmens zurück. Als Nokia-Veteran ist Kallasvuo für die Nachfolge Ollilas gut vorbereitet. Der 52-Jährige leitete in seinen 25 Dienstjahren unter anderem Nokia Americas, war Finanzvorstand und für die Handy-Sparte verantwortlich. Seit seiner Bestellung zum Thronfolger im Oktober vergangenen Jahres wurde er als Chief Operating Officer (COO) auf seine anstehenden Aufgaben als Nokia-Chef getrimmt.



## Surfcontrol verstärkt Marketing-Team



Daniel Heck übernimmt ab sofort bei dem Spezialisten für Internet-Sicherheit die Funktion des Marketing-Managers für Deutschland, Österreich und die Schweiz (Dach) sowie Osteuropa. Der 39-Jährige kommt von dem inzwischen vom Konkurrenten Autonomy übernommenen Knowledge-Management-Spezialisten Verity, wo er ähnliche Funktionen inne hatte. Davor arbeitete Heck als Leiter Kommunikation und Marketing bei Day Software.

## Ex-Siebel-Manager wird CEO von Polarlake

Auf seinem neuen Posten soll John Randles die Ausrichtung des Unternehmens auf die Bereiche Öffentliche Hand und Finanzdienstleister vorantreiben, gab der irische Business-Integration-Spezialist bekannt. Zuletzt war Randles bei Siebel Systems für die technische Entwicklung der Sparte Retail Banking in Amerika und der EMEA-Region (Europa, Nahost und Afrika) zuständig. Davor arbeitete der Ire als CTO bei Eontec, einem Anbieter von Java-basierenden Banklösungen. Das Dubliner Unternehmen wurde 2004 von Siebel übernommen.

## Pieper leitet AT&T-Vertrieb in Zentraleuropa

Als neuer Vice President Sales soll Frank Pieper den Vertrieb von AT&T für Deutschland, Österreich und die Schweiz von der Münchner Niederlassung aus steuern. Zu seinen zentralen Aufgaben gehört es, die größten Kunden des US-amerikanischen Carriers in allen Netzwerkbelangen zu unterstützen und global agierende Unternehmen in dieser Region zu betreuen. Pieper bringt weitreichende Branchenerfahrung mit: Zuletzt war er Director Global Accounts bei MCI (jetzt Verizon Business) in Zentraleuropa. Davor leitete er die weltweiten Geschäftsaktivitäten bei der UUNET Deutschland GmbH und Compuserve Network Services.



Personalmitteilungen bitte an [Menschen@Computerwoche.de](mailto:Menschen@Computerwoche.de)

Kolumne

## Open SOA – Suns neue Chance

Wann Sun die Kontrolle über Java in die Hände der Open-Source-Gemeinde legt, bleibt auch nach den jüngsten Ankündigungen offen. Die aufgeregte Debatte um eine quelloffene Plattform quittieren nicht wenige Java-Anhänger mit einem Schulterzucken. Die Diskussion sei nicht neu, am kollaborativen Entwicklungsmodell vieler Java-Projekte werde sich kaum etwas ändern. Anders beim Hypothema Service-orientierte Architekturen (SOA): Hier hat Sun Fakten geschaffen, und das ist tatsächlich neu. Die Kalifornier übergeben fast alle Kernkomponenten einer SOA der Community. „Wir sind der einzige Hersteller, der einen komplett quelloffenen SOA-Stack anbietet“, warb Senior Vice President Mark Bauhaus auf der Entwicklerkonferenz JavaOne (siehe Seite 16).

Mit seiner „Java Composite Application Platform“ (Caps) tritt Sun in Sachen SOA gegen die Großen der Softwarebranche an, dies allerdings mit einer klaren Open-Source-Strategie: Die Java-Company unterscheidet sich darin beispielsweise von IBM. Zwar offeriert der IT-Konzern mit der „Community Edition“ auch eine quelloffene Variante seines „WebSphere“-Application Server“. Doch die blauen Produktstrategen weisen stets darauf hin, dass dieser nicht in gleicher Weise für



Wolfgang Herrmann  
Redakteur CW

unternehmenskritische Einsätze geeignet sei wie das lizenzkostenpflichtige Pendant. Auch Bea Systems verfolgt mit seiner „Blended“-Strategie nur einen halbherzigen Open-Source-Kurs: Die Vermischung von quelloffenen Komponenten und eigenen proprietären Systemen diene dem Wohl des Kunden, argumentiert der Hersteller – und meint damit eher den eigenen Vorteil in Form verkaufter Softwarelizenzen.

Aus Kundensicht bleibt die Frage nach dem Support: Wer steht dafür gerade, dass quelloffene SOA-Komponenten

funktionieren und sich in bestehende IT-Umgebungen integrieren lassen? Wer garantiert regelmäßige Updates und die Wartung der komplexen Infrastruktur? Die Antwort haben professionelle Vermarkter von Open-Source-Softwarestacks längst gegeben. Zu ihnen gehören etwa die US-Anbieter Spikesource oder Sourcelabs, aber auch Jboss mit seiner quelloffenen Middleware-Suite.

Die Geschäftsmodelle dieser Unternehmen funktionieren. Wenn Sun sich mit Open SOA und produktnahen Dienstleistungen daran orientiert, besteht die Chance, die Abhängigkeit vom Hardwaregeschäft zu verringern. Das Führungsteam um CEO Jonathan Schwartz könnte damit auch kritische Investoren besänftigen, die seit langem eine Stärkung des Servicegeschäfts fordern.

## Allianz gegen Google

Fortsetzung von Seite 1

Erst kürzlich publizierte Zahlen belegen, dass der Branchenprimus weiter auf Kosten der Konkurrenz expandiert. Ebay hingegen wächst in seinem angestammten Business nur mehr moderat und möchte sich die kräftig sprudelnde Einnahmequelle der Online-Werbung erschließen. Der Internet-Auktionator fühlte sich zuletzt durch den neuen Kleinanzeigen-Service „Google Base“ in seinem Kerngeschäft angegriffen. Dieser enthält zudem einen Bezahlmechanismus, der von den Nutzern keine Provision verlangt und damit Paypal unter Druck setzt.

Der Deal zwischen den beiden E-Commerce-Riesen reiht sich ein in eine ganze Reihe ähnlicher Abkommen, mit denen sich die Schwergewichte die Online-Territorien aufteilen wollen. Fast gleichzeitig mit dem Abkommen zwischen Ebay und Yahoo gab

Google eine Kooperation mit Dell bekannt. Demnach wird der PC-Hersteller einige Softwarepakete von Google vorinstallieren und zudem dessen Suchmaschine im Web-Browser als Standard voreinstellen. Bereits im März investierte Google eine Milliarde Dollar in AOL, um dort weiterhin exklusiv seine Anzeigen und Suchdienste platzieren zu können.

### Microsoft buhlt um Amazon

Auch Microsoft, das verspätet in diesen Wettbewerb einstieg, nutzt seine prall gefüllte Kasse, um sich Marktanteile zu sichern. So verdrängten die Redmonder erst kürzlich Google bei Amazon und stellen mit „Live Search“ die Suchmaschine bei A9 und Alexa. Beobachter gehen davon aus, dass MSN mit „Adcenter“ die künftigen Werbeanzeigen für den Online-Händler zur Verfügung stellen wird.

Nach Berichten der New York Post verfolgt Bill Gates aber offenbar noch eine andere Option. Demnach verhandelt Microsoft seit mehreren Wochen mit Ebay über den Kauf des Auktionshauses. Allerdings befürchten beide Parteien Schwierigkeiten mit den Kartellbehörden. Microsoft lässt sich angeblich jedoch durch die Partnerschaft zwischen Yahoo und Ebay nicht beirren. (ws) ♦

## Mehr zum Thema

[www.computerwoche.de](http://www.computerwoche.de)

- 575633:** Amazon.com setzt auf Windows Live;
- 573594:** Google weitet seinen Bezahlendienst aus;
- 576753:** Dell installiert Google-Software auf PC;
- 574218:** Google steigt mit fünf Prozent bei AOL ein.

**FRAGE DER WOCHE**  
Dürfen Sie Spiele der Fußball-Weltmeisterschaft am Arbeitsplatz verfolgen?

41,0

Ich weiss nicht

21,0

Ja

38,0

Nein

Quelle: Computerwoche.de  
Angaben in Prozent, Basis: 207

Knapp die Hälfte der CW-Leser wird es zeitnah mitbekommen, wenn Ecuador unsere Klinsmänner am 20. Juni um 17:45 Uhr ins Achtelfinale verabschiedet.

# Schießt die Telekom auf BT?

Ein Zusammenschluss mit BT Global Services würde die Geschäftskundensparte T-Systems deutlich stärken.

Wie die Londoner Tageszeitung „Times“ unter Berufung auf Unternehmenskreise berichtet, soll die Deutsche Telekom verschiedene Machbarkeitsstudien erstellt haben, die alle eine Zerschlagung der britischen BT Group zum Thema haben. Offiziell wurde der Bericht allerdings weder von dem Bonner Ex-Monopolisten noch von BT Group kommentiert. Man nehme generell zu Marktgerüchten keine Stellung, hieß es in Bonn.

## Interesse an Global Services

Die Telekom soll laut „Times“ vor allem an BTs internationalem Großkundengeschäft interessiert sein: Demnach wäre die Sparte Global Services, die im vergangenen Geschäftsjahr 44 Prozent zu den Gesamteinnahmen der Briten beisteuerte, eine willkommene Verstärkung für T-Systems. Mit einer Übernahme könnte die Telekom den Dienstleistungsarm kräftigen und so die Abhängigkeit vom schwierigen Festnetzgeschäft reduzieren. Hier leiden die Deutschen – ähnlich wie BT – unter starker Konkurrenz und sinkenden Umsätzen. Marktbeobachter vermuten, dass die Sparte ebenso wie BTs Endkundengeschäft samt Händlernetz abgespalten werden könnte. Die auf mehr als 25 Milliarden Pfund (36,5 Milliarden Euro) geschätzten Kosten für die

## Telekom-Chef Ricke auf Werbetour



Kai-Uwe Ricke hatte bereits auf der diesjährigen Jahreshauptversammlung Anfang Mai angekündigt, dass sein Unternehmen einen aktiven Beitrag zum **Konsolidierungsprozess** im europäischen TK-Markt leisten werde. Wie groß dieser ausfallen kann, hängt **mangels** ausreichenden **Barvermögens** eng mit der Bewertung der Telekom-Aktie zusammen. In den vergangenen zwei Wochen rührte Ricke entsprechend bei institutionellen Anlegern dies- und jenseits des Atlantiks die Werbetrommel für das aus Telekom-Sicht **unterbewertete Papier**. Wegen der vermeintlich schlechten Perspektive, insbesondere des Festnetzgeschäfts, ist der Kurs seit August 2005 um fast 20 Prozent gesunken.

Übernahme müsste die Telekom möglicherweise nicht alleine aufbringen. Branchenkenner gehen davon aus, dass die Telekom-Aktionärin und Beteiligungsgesellschaft Blackstone Group Teile von BT erwerben könnte, die die Deutschen nicht wollen oder – aus regulatorischen Gründen – nicht kaufen dürfen. Ein Mobilfunknetz besitzt die BT Group seit der Abspaltung von O<sub>2</sub> im Jahr 2001 nicht mehr.

## Investoren wären begeistert

Am Aktienmarkt käme ein Engagement der Deutschen bei den Briten gut an. Dort wird derzeit eine langfristige Perspektive für die größten Telcos vermisst. Gleichzeitig würde ein solcher Deal im Nachhinein den im April

vollzogenen Einstieg des US-amerikanischen Investors Blackstone mit (untypischen) 4,5 Prozent bei der Telekom erklären. Bereits zuvor galt als sicher, dass verschiedene andere Private-Equity-Firmen BT als Übernahmekandidaten ins Auge gefasst haben.

Fraglich ist allerdings, wie die Bonner im Fall der Fälle ihren Beitrag zu der Übernahme aufbringen sollen. Zwar hat sich der Konzern von dem milliardenschweren Voicestream-Kauf zur Jahrtausendwende wieder einigermaßen erholt. Um das Wachstum im US-amerikanischen Mobilfunkmarkt beibehalten zu können, muss die Telekom jedoch in Kürze weitere Milliarden in den Erwerb von 3G-Lizenzen investieren. (mb) ◆

# AMD setzt auf Sachsen

Das Unternehmen baut für 2,5 Milliarden Dollar seine Dresdner Fabriken aus.

Der Halbleiterhersteller AMD will seine Fertigungskapazitäten in den nächsten drei Jahren ausbauen. Im Rahmen von drei neuen Projekten werden am Standort Dresden zusätzliche Produktionskapazitäten für 300-Millimeter-Wafer geschaffen: Zum einen plant AMD, ein Halbleiterwerk mit dem Namen Fab 38 aufzubauen. Es soll durch eine grundlegende Neugestaltung des bisherigen Werkes Fab 30 entstehen. Die Produktion der neuen Fabrik soll auf 300-Millimeter-Wafer ausgerichtet sein und es erlauben, mehr als doppelt so viele Prozessoren auf einer Siliziumscheibe zu fertigen wie derzeit auf 200-Millimeter-Wafern.

Zudem wird AMD seine Kapazitäten in der Fab 36, der zweiten Fabrik in Dresden, erweitern. Außerdem errichtet das Unternehmen am sächsischen Standort ein neues Reinraumgebäude. Unternehmensangaben zufolge summieren sich die Investitionen auf rund 2,5 Milliarden Dollar, umgerechnet knapp zwei Milliarden Euro.

Die Pläne sehen vor, die 200-Millimeter-Fertigung in der zweiten Hälfte 2007 herunterzufahren. Derzeit laufen Vorbereitungen, um Ende 2007 mit dem Aufbau der neuen Produktion in Fab 38 zu beginnen. Ende 2008 soll die volle Ausbaustufe erreicht werden. (ajf) ◆

# Oracles CSO rügt Entwickler

Mary Ann Davidson kritisiert auch Universitäten.

Entwickler achten zu selten auf Sicherheit, wenn sie Anwendungen programmieren, kritisiert Oracles Chief Security Officer (CSO) Davidson. In einem Vortrag anlässlich der W3C-Conference in Edinburgh sagte die Managerin, dass fehlerhafte Software hohe finanzielle Schäden verursache. Dem amerikanischen National Institute of Standards and Technology (Nist) zufolge belaufen sich diese Kosten pro Jahr auf 22,2 bis 59,9 Milliarden Dollar.

Davidson schreckte auch vor Polemik nicht zurück: Wenn Architekten Brücken so bauten, wie Programmierer Anwendungen schrieben, würden viele Menschen allmorgendlich auf



„Fehlerhafte Software verursacht finanzielle Schäden“, meint Mary Ann Davidson, Chief Security Officer von Oracle.

dem Weg zur Arbeit die „Blue Bridge of Death“ zu sehen bekommen. Die Sicherheits-Managerin spielte damit auf die berühmten Blue Screens an, die einen Systemabsturz bedeuten.

An dem Dilemma seien Universitäten nicht ganz unschuldig. Sie lehrten keine sicheren Entwicklungsmethoden und seien nicht bereit, ihre Lehrpläne entsprechend zu ändern. (ave) ◆

# Sprint verklagt IBM

Ein mit mehreren Milliarden Dollar dotiertes Outsourcing-Abkommen wird vor Gericht verhandelt. Streitwert: lediglich 6,4 Millionen Dollar.

Die Unstimmigkeiten zwischen Sprint und IBM haben sich offenbar zu einem handfesten Streit entwickelt. Im Januar 2006 hatte der US-amerikanische TK-Anbieter Sprint angekündigt, ein umfangreiches Outsourcing-Abkommen mit IBM neu zu ordnen und einige Funktionen wieder unter eigener Regie zu betreiben. Der Beginn der Partnerschaft geht auf September 2003 zurück, als Sprint für die kommenden fünf Jahre die Anwendungsentwicklung und -wartung in die Hände von IBM legte. Im Juli 2004 wurde das Abkommen deutlich erweitert: IBM übernahm den Betrieb der Call-Center von Sprint. Der Wert des ersten Auftrags belief sich auf rund 400 Millionen Dollar, das zweite Paket hatte ein geplantes Volumen von mehreren Milliarden Dollar.

Doch die gemeinsame Zeit neigt sich dem Ende entgegen.

Die Differenzen scheinen derart groß, dass die Partner die Unstimmigkeiten nicht mehr ohne fremde Hilfe beheben können. Sprint beantragte vor einem Gericht in Kansas ein Gerichtsverfahren gegen IBM, weil Big

## Warum lässt es Sprint auf einen Streit mit IBM ankommen?

Blue es im vergangenen Jahr versäumt habe, vereinbarte Produktivitätssteigerungen zu realisieren.

Der Streitwert beläuft sich auf 6,4 Millionen Dollar, gemessen am Gesamtvolumen der Outsourcing-Verträge ist das ein kleiner Betrag. Doch gerade das nährt die Spekulation, die Partnerschaft sei grundlegend zerrüttet: Warum sonst lässt es ein Konzern von der Größe des TK-

Anbieters auf einen Streit mit IBM ankommen, wenn der Streitwert für beide Seiten „Peanuts“ ist?

Auslöser der Auseinandersetzung könnte ein Wechsel im IT-Management gewesen sein. Michael Stout, der als CIO von Sprint die Abkommen mit IBM unterschrieben hat, verließ das Unternehmen Ende 2005. Sein Nachfolger ist Richard LeFave, der von Nextel kommt. Die Abkommen mit IBM waren vor der Fusion von Sprint und Nextel unterschrieben worden. Möglicherweise haben sich die Geschäftsbedingungen derart verändert, dass die ursprünglichen Verträge nicht mehr haltbar waren. Ein Sprint-Sprecher bestätigte zwar, dass alle Abkommen mit IBM einer Revision unterzogen werden. Allerdings betonte er auch, man wolle weiterhin harmonisch zusammenarbeiten. (jha) ◆

# Hummingbird wird verkauft

Die Symphony TG übernimmt den kanadischen Enterprise-Content-Management-(ECM-)Anbieter.

Symphony TG, die sich als strategische Holding-Company bezeichnet, erwirbt den ECM-Spezialisten für 465 Millionen Dollar. Das entspricht einem Aktienpreis von 26,75 Dollar. An dem Deal beteiligt sich Tennenbaum Capital mit 135 Millionen Dollar.

Hummingbird gilt als kleinster der großen Fünf im ECM-Geschäft. Nach dem Kauf von Documentum durch EMC im Jahr 2003 verbleiben jetzt mit FileNet und Opentext nur mehr zwei unabhängige Spezialisten im führenden Quintett. Hummingbird selbst hatte zur Konsolidierung des Marktes durch die Akquisition von PC Docs und der deutschen Reddot AG beigetragen.

Die Kanadier fingen ursprünglich mit dem Verkauf von Connectivity-Software an, unter an-

derem mit Terminalemulationen und NFS-Servern. Sie stiegen erst Ende der 90er Jahre mit der Übernahme von PC Docs in das Dokumenten-Management ein. Der Kauf von Reddot 2005 sollte das Unternehmen vor allem beim Web-Content-Management verstärken und ihm den Zugang zu mittelständischen Kunden erleichtern.

Hummingbird erwirtschaftete im letzten Quartal bei einem Umsatz von 64,2 Millionen einen Gewinn von 4,9 Millionen Dollar. Im Vorjahresquartal hatte die Firma noch einen Verlust von 1,5 Millionen Dollar hinnehmen müssen. Symphony bietet dem Unternehmen nach Angaben des Managements nun die finanziellen Mittel, um sich auf seine traditionellen Geschäftszweige zu konzentrieren. (us) ◆

# Die Bedrohung kommt von innen

*Spam und Spyware, Phishing, Viren, Würmer, Hacker: Das Arsenal der Bedrohung, dem sich Computernutzer in Unternehmen und zu Hause ausgesetzt sehen, ist riesig. Das größte Sicherheitsrisiko aber ist – der Anwender.*

VON CW-REDAKTEUR JAN-BERND MEYER

Das hat verschiedene Gründe. Ein nur scheinbar widersprüchlicher ist der, dass PC-Benutzer sich einerseits in trügerischer Sicherheit wiegen. Dies gilt insbesondere dann, wenn sie glauben, durch die Sicherheitsvorkehrungen der firmeneigenen IT-Abteilungen von allem digitalen Unbill abgeschottet zu sein. Oder wenn sie sich irrigerweise vor den Fähigkeiten des Internet geübt zu wissen glauben. Andererseits bewegen sich viele Anwender sehr unsicher im Cyberspace und ohne Kenntnisse über die Fallstricke des WWW. Sie kommen mit neuen Techniken nicht zurecht und provozieren so erst Gefahrensituationen.

## Denn sie wissen, was sie tun

Wie groß das Sicherheitsrisiko Anwender ist, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) ermittelt. Dessen Präsident Udo Helmbrecht sagt, in einer repräsentativen Studie habe das BSI festgestellt, dass jeder vierte Deutsche ohne aktuellen Virenschutz im Internet unterwegs ist und mehr als die Hälfte der deutschen Surfer keine Firewall einsetzt, „und das, obwohl die Befragten wissen, dass im Internet Gefahren lauern“.

In den Unternehmen ergebe sich ein zusätzliches Problem, so Helmbrecht: „Neue Technologien und mobile Endgeräte, also beispielsweise Laptops, USB-Sticks oder Internet-Telefonie, erhöhen die Zahl möglicher Fehlerquellen.“ Der Teufel steckt dabei einerseits in der Technik selbst. Neue Geräte und Applikationen provozieren aber andererseits auch Fehlverhalten beim Anwender. „Die Einführung ungewohnter Techniken muss daher immer gepaart sein mit einer Sensibilisierung der Anwender für deren Gefahrenpotenziale.“

## Zu sicher

Raimund Genes, der beim Security-Anbieter Trend Micro als Chief Technology Officer (CTO) für Anti-Malware zuständig ist, macht einen weiteren Grund für die Gefährdung der Unternehmens-IT durch Mitarbeiter aus. In einer Studie von 2005 habe sein Unternehmen herausgefunden, dass sich insbesondere Großkonzerne, zunehmend aber auch mittelständische Firmen, über die Bedeutung abgesicherter PC-Arbeitsplätze im Klaren seien. „Genau um diese Sicher-

heit besorgen sie sich folgerichtig auch“, sagt Genes. Ironischerweise lässt diese vermeintliche Sicherheit Mitarbeiter erst unvorsichtig handeln.

Die Bedeutung dieses Sachverhalts kann gar nicht überschätzt werden. Denn das hauptsächliche Sicherheitsrisiko für Firmen kommt aus den eigenen Reihen. Konstatiert Norbert Pohlmann, Leiter des Instituts für Internet-Sicherheit an der FH Gelsenkirchen und Vorstandsvorsitzender von Teletrust Deutschland e.V.: „Die Mehrzahl der Sicherheitsverstöße wird durch Innetäter verursacht“. Vorsatz, Versehen, Übereifer, Neugierde und mangelndes Problembewusstsein seien die häufigsten Ursachen für Sicherheitsvorfälle.

Das Problem „Innetäter“ kommt Firmen dabei richtig teuer zu stehen. Sagt Armin Stephan, Security-Experte bei Computer Associates (CA) in Darmstadt: „Die Angriffe von „Insidern“ nehmen ständig zu. Da sie meist einfacher auf kritische Informationen zugreifen können als Externe, sind Angriffe und Fehlverhalten von innerhalb der Firma oft kostspieliger als Attacken von außen.“

Stephans These wird durch Ergebnisse einer Untersuchung untermauert, die das US National Reconnaissance Office (NRO) bei US-Firmen anstellte. Angriffe, die von außen gegen eine Firma gestartet werden, kosten Konzerne pro Jahr durchschnittlich 56 000 Dollar. Schäden durch Aktionen aus der eigenen Firma liegen um ein Vielfaches höher. Das NRO beziffert sie auf durchschnittlich mehr als zwei Millionen Dollar jährlich.

CA-Mann Stephan zitiert zudem die Studie „The InfoPro's Information Security Study“ vom Februar 2006. Diese kommt,

die Erkenntnisse des NRO flankierend, zu dem Ergebnis, dass 72 Prozent aller Unternehmen die Bedrohung der Sicherheit durch interne Kräfte mindestens so hoch einschätzen wie die Gefährdung durch externe Attacken.

Thomas Rickert, Rechtsanwalt bei der Bonner Schollmeyer & Rickert Rechtsanwalts-gesellschaft mbH, hat ebenfalls die Erfahrung gemacht, dass die Mehrzahl der Sicherheitsverstöße von Firmenangehörigen ver-

übt wird. Nicht immer aber sei Vorsatz zu vermuten. „In kleinen und mittelständischen Unternehmen sind die

PC-Anwender meist auf sich allein gestellt und sind sich der Risiken oft gar nicht bewusst“,

sagt Rickert, in Personalunion auch Vertreter des Eco Ver-

bands der deutschen Internetwirtschaft aus Köln.

Für Unternehmen bleibt das Risiko. Und sie wissen

das auch, wie die Marktforscher von IDC in der Untersuchung „Worldwide Outbound Content Compliance 2005 – 2009 Forecast and Analysis: IT Security Turns Inside Out“ vom November 2005 ermittelt haben. Die für die IT-Studie befragten IT-Verantwortlichen gaben an, dass eine ihrer größten Herausforderungen in den kommenden zwölf Monaten darin bestünde, ihre Mitarbeiter anzuhalten, die firmeninternen Sicherheitsrichtlinien zu befolgen.

Warum nur, warum?

Die Frage, weshalb dem Faktor Mensch so zentrale Bedeutung beim Thema Sicherheitsrisiko zukommt, beantwortet Joachim von Gottberg ernüchternd. Der Sprecher der Initiative „Deutschland sicher im Netz“, die im Januar 2005 gegründet wurde, erklärt:

„Die meisten Nutzer wis-

sen zwar um die Risiken im World Wide Web, gehen aber dennoch davon aus, dass sie selbst nicht Opfer von Internet-kriminalität werden.“

Und so verhalten sie sich nach einer Internet-Umfrage des britischen Sicherheitsspezialisten Sophos dann auch. 41 Prozent von 500 an der Untersuchung teilnehmenden Computernutzern aus Unternehmen verlässt sich beispielsweise darauf, mit einem einzigen Passwort alle Applikationen am PC und im Internet abzusichern. Nur 14 Prozent verwenden für jede Anwendung einen anderen Zugangscode. Die restlichen 45 Prozent variieren diesen zumindest teilweise. „Wer heute dasselbe Passwort für Online-Banking wie für den Zugriff auf die Website mit den neuesten Fußball-Ergebnissen verwendet, macht es Hackern nur allzu leicht“, warnt der in Diensten des Softwareunternehmens stehende Senior Technology Consultant Jens Freitag.

**Top-Priorität: Aufklärung**

„Umso wichtiger ist es, fundierte Aufklärungsarbeit zu leisten und an die Verantwortung der Nutzer zu appellieren“, fordert von Gottberg. BSI-Präsident Helmbrecht sieht es genauso und moniert: „Der Anwender muss hinsichtlich der IT-Risiken noch stärker als bisher sensibilisiert werden. Einige User sind blauäugig und ohne Risikobewusstsein im Internet unterwegs. Dem kann man durch Aufklärungskampagnen abhelfen.“

Oft wüssten Anwender aber auch nicht, welche technischen Möglichkeiten sie haben, um das Niveau der IT-Sicherheit zu steigern – beispielsweise, wie sich ohne Administratorenrechte ein Nutzerprofil einrichten lässt. „Hier muss Wissen vermittelt werden.“ Das BSI tue dies mit seinem Bürger-Portal (siehe Kasten „Links“).

## 3. tecCHANNEL-Security-Konferenz

Sie wollen mehr zum Thema Security erfahren? Die dritte tecCHANNEL-Security-Konferenz am **29.06.2006 in München** informiert Sie über aktuelle Trends und Technologien, um Ihr Unternehmen gegen Angriffe abzusichern. Alle Informationen unter: [www.tecchannel.de/tecsecurity](http://www.tecchannel.de/tecsecurity)

Sehr wichtig sei auch, dass Anwender Informationen über neue Sicherheitslücken – etwa in Betriebssystemen – erhalten, fährt Helmbrecht fort. „Hier ist entscheidend, wie schnell der Anwender die Information bekommt, dass eine Sicherheitslücke besteht, und ob sein System und seine Software überhaupt betroffen sind und was er dagegen tun kann.“

Entsprechende Auskünfte liefert der E-Mail-Warnservice des Bürger-CERT (siehe Kasten „Links“). Muss der Anwender erst langwierig nach Informationen suchen, ist es oft schon zu spät. „Die Zahl der Zero-Day-Exploits nimmt zu“, begründet der BSI-Präsident. Gemeint ist die Summe der Attacken, die Hacker unmittelbar starten, nachdem Sicherheitslücken rufbar werden.

Pohlmann von Teletrust warnt in diesem Zusammenhang: „Meiner Meinung nach versuchen sich Gesellschaften gerade einmal in

## Die größten IT-Bedrohungen

1. Risikofaktor Anwender
2. Spam
3. Phishing
4. Hacker
5. Viren + Würmer
6. Spyware

den ersten Schritten, um mit den neuen Herausforderungen des Internet fertig zu werden. Ähnlich wie im Straßenverkehr müssen wir angemessene Sicherheitsmechanismen erst noch erlernen.“

Gut gebrüllt Löwe, könnte man sagen – und zu Recht gebrüllt, wie Magnus Kalkuhl, Virusanalyst bei Kaspersky Lab, schon fast ungehalten bestätigt: „Es gibt immer wieder Computerbesitzer, die mit stolz geschwellter Brust behaupten, keinerlei Schutzsoftware zu benötigen. Dabei belästigt ihr Rechner längst unbemerkt die PCs anderer User als Spam-Schleuder.“

In größeren Unternehmen würde die allgemeine Sicherheitsbedrohung zwar durch den Einsatz von Virenschaltern auf Mailservern und Arbeitsplatzrechnern etwas entschärft, „aber auch Sicherheitsgurte und Airbags können nur noch wenig zur Schadensbegrenzung beitragen, wenn jemand mit 200 Stundenkilometern im Auto fröhlich die Gegenfahrbahn entlang rast.“

### Ideale Beute

Das Thema Sicherheitsrisiko Anwender ist dabei aktueller denn je. Die Frage, ob diese Problematik größer oder kleiner geworden sei, beantwortet etwa Rickert vom Eco-Verband unmissverständlich: „Eindeutig größer! Die Systeme sind komplexer geworden und durch die Konvergenz

## Top-Sicherheitsratschläge der Experten

- Lebensnotwendig: Personal Firewall (Zwei-Wege-Firewall) und Virenschutzprogramme mit aktuellen Signaturen;
- Niemals als Administrator mit umfassenden Rechten im Internet surfen;
- Ständig Informationen über aktuelle Gefahren und neu entdeckte Sicherheitslücken sammeln auf einschlägigen Internetseiten und weitergeben;
- Generell Vorsicht walten lassen und ein wenig misstrauisch sein;
- Sicherheitsaktualisierungen zu Software (Betriebssysteme, Browser etc.) bei Verfügbarkeit sofort aufspielen;
- E-Mail-Adresse nie im Klartext im Internet angeben und für öffentliche Foren und Newsletter eine spezielle E-Mail-Adresse einrichten, die ausschließlich dort benutzt wird;
- Starkes Passwort wählen und nicht auf einem Zettel unter der Tastatur deponieren;
- Risiken reduzieren durch gesunden Menschenverstand;
- Backup, Backup, Backup ...

der Medien haben sich die potenziellen Gefahren vermehrt.“ Für die meisten User seien E-Mail und Web-Browser die beiden wichtigsten Anwendungen: „Und genau hier lauern auch die Gefahren.“

Kalkuhl von Kaspersky Lab zeichnet das Bild noch etwas drastischer: „Es gibt immer mehr Menschen, die erst jetzt – sei es beruflich oder privat – mit dem Thema Internet in Berührung kommen. Die sind eine geradezu ideale Beute für die Malware-Szene.“

### Hersteller in der Verantwortung

Und Pohlmann von Teletrust macht an einem Beispiel klar, wie einfach der Daten-GAU heutzutage zu fabrizieren ist: „Jemand will seine auf einem USB-Stick gespeicherte Präsentation auf Ihrem Rechner oder Laptop vorführen: Kommen Sie da sofort auf die Idee, dass vermittels dieser kleinen Hardwareerweiterung Ihre Festplatte en passant abgegrast und Daten gespeichert oder gar gelöscht werden könnten?“

Ein gerüttelt Maß latenten Misstrauens scheint deshalb das Gebot der Stunde zu sein. BSI-Präsident Helmbrecht kommt dabei sofort ein Szenario in den Sinn, das heutzutage verbreitet ist: Social Engineering. Die Bezeichnung verharmlost die dem Phänomen innewohnende Brisanz. Helmbrecht: „Mit der psychologischen Ansprache, dem Social Engineering, im Massenmedium Internet zielen Cyberkriminelle genau auf die Schwachstelle Mensch.“ Da würden vermeintlich persönliche Botschaften schnell geöffnet, Einladungen zu Klassentreffen etwa, und rasch habe man sich im Dateianhang ein trojanisches Pferd eingehandelt.

Wie das Sicherheitsniveau schon an der Basis angehoben werden könnte, darüber scheinen Experten einer Meinung. Genes von Trend Micro fordert stellvertretend für seine Zunft: „Die Einführung eines Internet-Führerscheins in Schulen wäre wünschenswert, um der kom-

mende Generation schon im Kindesalter verschärft vor Augen zu führen, welche Untiefen sich im Internet verbergen können und was man dagegen tun kann.“

Pohlmann, Leiter des Instituts für Internet-Sicherheit an der FH Gelsenkirchen, bläst ins gleiche Horn: „Selbstverständlich sollte Sicherheitsbewusstsein schon in den Schulen vermittelt werden. Informatikunterricht ohne Berücksichtigung der Sicherheitsaspekte ist schier unvorstellbar.“

So sieht es auch Helmbrecht vom BSI: „Medienkompetenz und IT-Sicherheitskultur sind Themen, die auch in den Schulalltag gehören, nicht erst, seitdem Gewaltvideos auf Handys von Schülern entdeckt wurden.“



Der BSI-Präsident teilt aber auch gegen die Hersteller aus: „Je mehr die IT unseren Alltag durchdringt, desto bedeutungsvoller ist das Thema Sicherheit. Diese Erkenntnis sollte sich auch in der Qualität der IT-Produkte und -Programme widerspiegeln. Die hohe Zahl der Nachbesserungen und Patches

## Links

- <https://www.sicher-im-netz.de/?sicherheit/ihre/checklisten/default>
- [http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html)
- [www.buerger-cert.de](http://www.buerger-cert.de)
- [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)
- <http://polizei-beratung.de>
- [www.internauten.de](http://www.internauten.de)
- [http://de.trendmicro-europe.com/enterprise/about\\_us/spreuse.php?lstPages=9&id=136](http://de.trendmicro-europe.com/enterprise/about_us/spreuse.php?lstPages=9&id=136)
- <http://www.theinfo.pro.net/>
- <http://www.idc.com/getdoc.jsp?containerId=34260>
- <http://www.nro.gov/index.html>

wäre sicherlich reduzierbar, würde im Vorfeld der Herstellung mehr Sorgfalt walten. Hier sind insbesondere die Hersteller gefordert.“

Pohlmann pflichtet dem bei: Anwender müssten auf sichere Infrastrukturen, Rechner, Betriebssysteme und Anwendungen vertrauen können. „In diesem Zusammenhang sollte die Produkthaftung für Software gestärkt werden.“

### Organisierte Kriminalität

Individuelles Sicherheitsbewusstsein und kontinuierliche Schulungen auch in Unternehmen sind dabei das A und O, um heutigen Gefahren entgegenzuwirken. Kalkuhl von Kaspersky Lab deutet auf eine wesentliche Veränderung in der Welt des WWW hin, die zum erhöhten Gefahrenpotenzial maßgeblich beiträgt: „In den letzten Jahren hat sich die Malware-Szene vom Just-for-fun-Virenschreiben verabschiedet und ihren Platz in der mit handfesten finanziellen Interessen operierenden organisierten Kriminalität gefunden. Warum einen Menschen auf offener Strasse überfallen, wenn man PINs und TANs direkt abgreifen kann und so Zugriff auf die Konten der Opfer hat?“

BSI-Mann Helmbrecht sieht es genau so: „IT-Bedrohungen sind zunehmend kriminell motiviert. Die Cyberkriminalität setzt immer raffiniertere Methoden ein – nicht nur in der technischen Umsetzung.“

Einig sind sich die Sicherheitsexperten zudem darüber, dass Kriminelle im Internet zunehmend intelligenter agieren. Zudem würden gezielte, personalisierte Angriffe Anwendern das Leben schwer machen. Plumpe Phishing-Aktionen sind nicht mehr State of the Art. „Es wird nicht mehr nur via E-Mail nach Kontonummern, PINs und TANs gefragt. Verstärkt werden Trojaner eingesetzt, die etwa in der Lage sind, beim Online-Banking unbemerkt den Geldbetrag einer Überweisung und das Empfängerkonto zu manipulieren“, sagt Helmbrecht.

Genes sieht im DNS-Poisoning und -Pharming eine Betrugsvariante, die zurzeit en vogue ist. Hierbei muss der Anwender nicht mehr auf einen E-Mail-Hyperlink klicken, um auf eine Phishing-Seite geleitet zu werden.

Vor allem aber stehe heutzutage ganz klar das kommerzielle Interesse der Malware-Writer im Vordergrund, das sich unter dem Deckmäntelchen des „guten“ Social Engineering einschleicht. Als Beispiel zitiert Genes den wenige Wochen zurückliegenden Vorfall, als Internetpiraten einen „FIFA-Spielplan“ durch das WWW pumpten. Diese Malware transportierte Software (trojanische Pferde), die TCP-Ports öffnet, um über diesen Einfallsweg einen infizierten Rechner fern- und fremdzusteuern (so genannte Haxdoor-Software).

Sowohl der private Anwender wie auch Computernutzer in Unternehmen hinken dabei immer den neuesten Malware-Entwicklungen hinterher. Rechtsanwalt Rickert: „Die Themen wechseln ständig. Heute Phishing, morgen Bot-Netze. Das bedeutet, Sicherheit stellt keinen statischen Zustand dar, sondern einen sich ständig verändernden Prozess.“

Firmen, so der Vertreter des Eco-Verbands, müssten deshalb erkennen, dass Ausgaben für IT-Sicherheit so überlebensnotwendig sind wie die für Hard- und Software. Der Rechtsanwalt sagt: „IT-Sicherheit ist Chefsache und muss vorgelebt werden.“

Es sei auch nicht damit getan, „Mitarbeitern bei der Einstellung eine Mappe mit Richtlinien zur Sicherheit in die Hand zu drücken, die am Ende doch nicht befolgt werden“, assistiert Kalkuhl. Im Idealfall sollte jeder

## Basis-Check zur Sicherheit

Die Firma Computer Associates (CA) hat unter dem unten angeführten Link einen Basis-Check zur Optimierung der Sicherheit insbesondere von Rechnern privater Anwender und von kleinen Unternehmen veröffentlicht. Hier gibt es Handlungsempfehlungen und sieben Individual-Checks zu praxisrelevanten Themen wie Medienkompetenz und Kinderschutz, Online-Banking und E-Mail-Kommunikation.

<https://www.sicher-im-netz.de/default.aspx?sicherheit/ihre/checklisten/default>

Mitarbeiter auf wenige Punkte hin gezielt geschult werden. Das dauere nicht länger als einen Nachmittag, „wenn überhaupt“, und spare dem Unternehmen unter Umständen sehr viel Geld: „Denn durch das Training ist es vor kostspieligen Systemausfällen und dem Verlust von Betriebsgeheimnissen besser geschützt.“

### Menschenverstand, gesunder

Wichtig sei allerdings, solche Schulungen in regelmäßigen Abständen immer wieder durchzuführen – denn mit neuen Technologien tauchten auch neue Risiken auf. Kalkuhl: „Das Sicherheitsrisiko von Handviren beispielsweise ist zur Zeit noch vergleichsweise überschaubar. In einem Jahr kann das schon ganz anders aussehen.“

Trotz der permanenten Gefahrensituation, in der sich Anwender bewegen, ist die Lage nicht hoffnungslos. Es gebe ein ganz probates Mittel, meint Kaspersky-Experte Kalkuhl, um sich der größten Gefahren der Internet-Kriminalität zu erwehren: „Gesunder Menschenverstand“ sei sehr hilfreich. ♦