

COMPUTERWOCHE

NACHRICHTEN ♦ ANALYSEN ♦ TRENDS



KONFERENZ

BI ohne Kompromisse

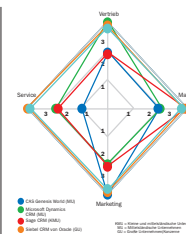
Die größten Konkurrenten von SAS Institute sind jetzt IBM, Oracle und SAP. Der Spezialist für Business Intelligence nimmt den Kampf an. **SEITE 9**



ANALYSE

Trends im Softwaremarkt

Software as a Service, Open Source und Globalisierung haben laut Gartner ihr Gutes: Die Softwarepreise werden fallen. **SEITE 10**



TEST

CRM-Produkte im Vergleich

Fünf Lösungen für das Customer-Relationship-Management (CRM) im Vergleich: Oracle/Siebel und Update zeigen Stärke. **SEITE 12**



◆ Outlook sichern

Mit „Planet Outlook Backup“ lassen sich E-Mails bequem zeitgesteuert sichern. Gut gelungen ist die Benutzerführung. Allerdings werden beim Restore immer alle Daten überschrieben, berichtet CW-Redakteur Frank Niemann.

ZAHL DER WOCHE

9.43 Uhr – zu diesem Zeitpunkt setzte am vergangenen Montag die Plattform für den elektronischen Aktienhandel, Xetra, für knapp eine Stunde aus. Auf Xetra findet der größte Teil des deutschen Aktienhandels statt. An das Computersystem sind Händler und Banken auf der ganzen Welt angeschlossen. Ursache der Panne soll ein fehlerhafter Start einzelner Prozesse auf einem der Server gewesen sein. Auch der Handel der Leipziger Strombörse und der irischen Börse waren betroffen – sie bauen ebenfalls auf dem Xetra-System auf.

Sun baut RZ in Kohlebergwerk

Gemeinsam mit elf anderen Unternehmen will Sun Microsystems ein Rechenzentrum tief unten in einem japanischen Kohlebergwerk einrichten. Dabei sollen 30 Spezialcontainer in der Erde versenkt werden. Hintergrund ist die Energieeffizienz: Die unterirdischen Rechner lassen sich mit Grundwasser kühlen, außerdem beträgt die Temperatur tief unter der Erde konstant 15 Grad Celsius. Damit soll sich der Stromverbrauch gegenüber einer Anlage an der Erdoberfläche um bis zu 50 Prozent senken lassen. (tc) ◆

Virens Scanner öffnen Hackern die Türen

Antiviren-Software kann – entgegen dem Sicherheitsgefühl, das sie vermittelt – zum Einfallstor für Schadcode werden.

Antiviren-Lösungen ermöglichen genau das, wogegen sie eigentlich schützen sollen: das Einschleusen und Ausführen von Schadcode. Sicherheitsexperten der N.runs AG haben in den vergangenen Monaten rund 800 Schwachstellen in Virenschutzprodukten aufgespürt, über die Angreifer Denial-of-Service-Angriffe (DoS) betreiben und Firmennetze mit Schadcode verschicken können.

Die Virens Scanner helfen sogar dabei, den Code auszuführen. „Von den Schwachstellen war jede am Markt befindliche Scan-Engine gleich mehrfach betroffen“, verdeutlicht Thierry Zoller, Security Engineer bei dem auf Sicherheitsanalysen von Applikationen spezialisierten IT-Dienstleister, die Tragweite der Testergebnisse.

Den Untersuchungen zufolge liegt die ungewöhnliche Vielzahl von Lücken in einer Kernfunktion der Antiviren-Lösungen, dem Parsen von Dateiformaten, begründet. Die Sicherheitsexperten führen die hohe Fehleranfälligkeit der Parser-Engines beim Zerlegen von Daten in

analysierbare Einzelteile auf die ständig steigende Zahl an Formaten zurück: Virens Scanner müssen sie verstehen und bearbeiten, um ihr primäres Ziel – möglichst viele Schädlinge zu erkennen – zu erfüllen. Laut Zoller stellt die in Teilen hochkomplexe

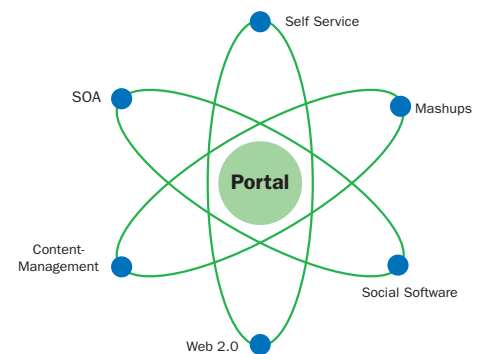
Analyse jedes einzelnen Formats im Prinzip eine potenzielle Fehlerquelle dar.

Verschärft wird die Situation nach Ansicht der Experten durch die von den Antiviren-Herstellern geforderte schnelle Reaktion auf neue Bedrohungen. „Die Antiviren-Industrie und deren Entwickler stehen unter enormem Zeitdruck: Hier geht es darum, wer am schnellsten neue Gefahren erkennt – was die Qualität des Codes nicht unbedingt steigert“, gibt Zoller zu bedenken.

Kritisch seien die Sicherheitslücken in Antiviren-Systemen aber auch, weil die meist mit hohen Rechten ausgestatteten Viren-Engines mittlerweile an nahezu allen zentralen Schaltstellen im Firmennetz laufen – genau dort also, wo die sensibelsten Daten eines Unternehmens gespeichert und verarbeitet werden. Den ausführlichen Bericht „Virens Scanner öffnen Hackern die Türen“ lesen Sie auf Seite 5. (kf) ◆



DIESE WOCHE



Comeback der Portale

Web-2.0-Themen wie Mashups, Wikis und Blogs hauchen den Unternehmensportalen neues Leben ein. **IT-Strategien SEITE 31**

Microsoft greift VMware an

Mit „System Center“ und „Windows Server 2008“ setzt der Softwaregigant jetzt auf Virtualisierung – vom Server bis zum Client. **Nachrichten SEITE 6**

Test: Sharepoint for Search

Die Suchmaschine von Microsoft zeigt Stärken bei Funktionsumfang und Verwaltung, sperrt sich aber gegen das Integrieren von Datenquellen. **Produkte & Technologien Praxis SEITE 18**

Berater rationalisieren

Mit vorkonfigurierten Eigenentwicklungen setzen immer mehr Beratungshäuser auf „industrialisierte Angebote“. **IT-Services SEITE 34**

Der CIO – das Alphanier?

Über Personalführung lässt sich bekanntlich streiten. Drei Beispiele zeigen, wie CIOs in der Praxis vorgehen. **Job & Karriere SEITE 37**



„Verständnislücke“ behindert SOA 8



Business und IT haben nach Angaben des unabhängigen Analysten Wolfgang Martin oft unterschiedliche Vorstellungen von einer SOA: „Die Verständnislücke zwischen Business und IT ist noch längst nicht geschlossen.“

NACHRICHTEN UND ANALYSEN

SAP plant ohne Tomorrow Now 4
Die Unternehmenstochter, die sich mit der Wartung von Fremdsystemen beschäftigt, ist zum Risiko geworden.

Infors eigenwillige SOA-Strategie 7
Die einzelnen Programme sollen im Rahmen der Strategie „Open SOA“ integriert werden.

PRODUKTE & TECHNOLOGIEN

CRM-Systeme im Vergleich 12
Auf dem Prüfstand die Produkte von CAS Genesis, Microsoft, Sage, Siebel/Oracle und Update Seven.

Reddot auf Web-2.0-Kurs 17
Anwender sollen Inhalte aus Blogs und Wikis einbinden.

PRODUKTE & TECHNOLOGIEN

PRAXIS

Sharepoint-Suche im Test 18
Microsofts Suchmaschine für Firmen bietet viele Funktionen, doch für die Datenintegration müssen Anwender tief in die Tasche greifen.

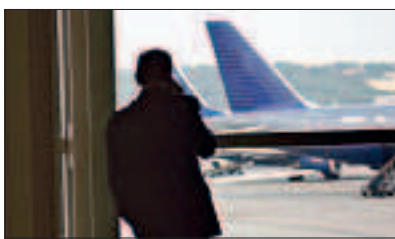
Ubuntu 7.10 macht Linux bunt 22
Das Desktop-Betriebssystem verfügt über viele Multimedia-Features, die Hardwareunterstützung weist jedoch Schwächen auf.

Kleine Helfer 22

SCHWERPUNKT: MOBILE SOLUTIONS

Mobilität kämpft noch mit Hindernissen 24
Bei der mobilen Kommunikation in Unternehmen klaffen Anspruch und Wirklichkeit weit auseinander.

Smartphones und PDAs verraten alles 26
Beim mobilen Einsatz gibt es vor allem zwei sicherheitsrelevante Schwachstellen: das Gerät und den Benutzer. Was Unternehmen tun müssen, um auf der sicheren Seite zu sein.



IT-STRATEGIEN

Portale – eine Renaissance 31
Statische Informationen waren gestern. Heute bilden die Unternehmensportale ganze Prozessketten ab.

Selbsttest für die IT 32
Booz Allen Hamilton und die CW bieten eine Organisations-Checkliste für IT-Abteilungen an.

IT-SERVICES

Die Softwarestrategie der Berater 34
Im Zuge der Industrialisierung entwickeln die Beratungshäuser zunehmend eigene, vorkonfigurierte Softwarelösungen, mit denen sich die Laufzeiten von Projekten verkürzen und Kosten einsparen lassen.

JOB & KARRIERE

Der CIO – Alphatier oder Kumpel? 36
Jeder zweite Beschäftigte schätzt klare Vorgaben. Ob dieses autoritär anmutende Rollenverständnis in modernen Unternehmen anzutreffen ist, beantworteten drei IT-Chefs.

Zuversicht im Projektmarkt 37
Die Stundensätze für Berater sind gestiegen, und auch die Zahl der Projektanfragen ist sehr hoch, wie der aktuelle Index für Freiberufler vom Hamburger Beratungshaus Geco zeigt.

CW-TOPICS: IT IN BANKEN

Kostendruck und Wettbewerb zwingen Banken, die Fertigungstiefe zu reduzieren. Verlegerbeilage ab Seite 27

STANDARDS

Impressum 25
Stellenmarkt 38
Zahlen – Prognosen – Trends 42
Im Heft erwähnte Hersteller 42

COMPUTERWOCHE.de

Die Highlights der Woche

Tipps und Tricks für Windows Vista

Das neue Windows-System macht es den Benutzern nicht gerade einfach. Im Wiki der COMPUTERWOCHE finden Sie hilfreiche Tipps zur Installation und zum Umstieg von XP. Außerdem erhalten Sie wertvolle Hinweise zur Konfiguration sowie Administration des Systems und erfahren, wie man der Software in Sachen Tempo auf die Sprünge hilft.



wiki.computerwoche.de

Das iPhone im Praxistest

COMPUTERWOCHE-Redakteur Thomas Cloer testet das iPhone mehrere Wochen lang und berichtet von Freud und Leid mit dem Kultgerät.

www.computerwoche.de/iphonetest

Orientierung im Markt für Navigationssysteme

Sie wollen nicht mehr als 300 Euro für ein Navigationsgerät ausgeben? Wir zeigen Ihnen in unserem Vergleichstest, welche Geräte in Frage kommen. Dabei spielen Kriterien wie Display, Kartenmaterial und Ausstattung eine Rolle. Noch wichtiger sind aber Navigation und Handhabung.



www.computerwoche.de/99747

Knowledge-Center Green-IT

Wie viel Energie verbrauchen Rechenzentren? Welcher Computerhersteller hat Probleme mit seinem Öko-Image? Seit wann müssen Rechnerbauer alte Geräte zurücknehmen und entsorgen? Überprüfen und erweitern Sie Ihr Wissen im Knowledge-Center Green IT.

www.computerwoche.de/knowledge_center/green-it/

Der Traum vom High Security Server

Etwa 18 000 Ergebnisse bekommt man in der Suchmaschine Google angezeigt, wenn man „unhackable server“ eingibt. Darunter sind in allen gängigen Sprachen rund 3800 Personen oder Gruppen, die behaupten, ihr Server sei gegen jegliche Angriffe gefeit. Security-Experte Alexander Tsolkas hat dazu eine eigene Meinung.

www.computerwoche.de/security-expertenrat

UMSONST Server,
UMSONST Anwendungen,

UMSONST Räume,
UMSONST Personal,

UMSONST Energie,
UMSONST Speicher...

Effizienzsteigerung auf ganzer Linie mit der revolutionären neuen Enterprise-Architektur

Ältere IT-Systeme haben einen Kühleffekt auf den gesamten Raum, doch die so vergebenden Energiekosten sind absolut unverantwortlich. Mit ihrer mitunter hoffnungslos überdimensionierten Auslegung werden sie den heutigen Anforderungen nicht mehr gerecht. Die unnötig verschwendeten Mittel fehlen dann für dringend erforderliche IT-Investitionen. Für ein einfaches Problem gibt es eine einfache Lösung: Sparen Sie Energiekosten und investieren Sie die freigesetzten Mittel in neue IT-Infrastruktur.

Einer Gartner-Studie zufolge werden 50 % aller vor 2002 entstandenen Datacenter aufgrund ihrer schlechten Energie- und Kühleffizienz 2008 schon überholt sein. Das Energie- bzw. Kühlproblem ist derzeit eine der größten Herausforderungen für Manager von Datacentern.

Begrenzte Energie- und Finanzressourcen

Wie viel Energie Sie zur Verfügung haben, sagt Ihnen der Verteilerschrank. Wie viel Geld Sie ausgeben können, sagt Ihnen Ihr Budget. Mit beidem müssen Sie möglichst sparsam

umgehen. Dabei unterstützt Sie Efficient Enterprise™ von APC.

Die skalierbare, modulare Lösung von APC lässt sich exakt an Ihre Bedürfnisse anpassen. Das Kapazitätsmanagement erleichtert die Planung von Investitionen in neue Server. Kühlung und Klimasteuerung werden durch dedizierte In-Row- und Wärmevermeidungskonzepte optimiert. Efficient Enterprise unterstützt Sie beim sparsamen, gezielten Einsatz Ihrer Ressourcen. Allein schon die Umschaltung von Raumkühlung auf Reihenkühlung bringt eine Einsparung der Stromkosten von durchschnittlich 35 %.

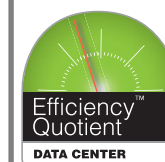
Unser System macht sich bezahlt

Ob Sie ein neues Datacenter einrichten oder die Effizienz der vorhandenen Systeme ermitteln möchten, an erster Stelle steht immer die Bestandsaufnahme. Unser Online-Dienst „Enterprise Efficiency Audit“ zeigt Ihnen, wie Sie sich die Vorteile eines integrierten, effizienten Systems nutzbar machen und mehr Leistung, Kontrolle und Rentabilität erzielen können.



Efficient Enterprise™ ermöglicht eine optimale Klimasteuerung und die Einsparung von Betriebskosten durch...

- 1 Ein eng gekoppeltes Kühlsystem.
- 2 Warmlufteindämmung.
- 3 Kapazitätsmanagement.
- 4 Optimal dimensionierte Komponenten.



Wie effizient arbeitet Ihr IT-System?
Nutzen Sie noch heute unseren Online-Dienst „Enterprise Efficiency Audit“ für eine Ist-Analyse.

Mehr online unter <http://promo.apc.com> Key Code 62788t
Tel: 0800 10 10067 • Fax: 089 51417-100



Legendary Reliability®

MENSCHEN

Lummitsch verlässt Sick AG



Nach nur neun Monaten hat Dietmar Lummitsch Ende September seinen Posten als CIO des Sensortechnologiekonzerns Sick AG wieder abgegeben. Gründe für die schnelle Trennung wurden nicht bekannt. Lummitsch hatte erst im Januar 2007 als IT-Chef und Mitglied der Geschäftsführung bei dem Unternehmen aus Waldkirch bei Freiburg angefangen. Davor arbeitete der 50-Jährige von April 2004 bis Ende 2006 als CIO bei dem Chemiekonzern Altana Pharma. Zuvor war er als CIO der TÜV Süddeutschland Holding und Geschäftsführer der TÜV Informatik und Consulting Services tätig.

Captiva-Gründer wird Dicom-CEO

Reynolds Bish ist seit Anfang vergangener Woche Chef der britischen Dicom Group. Der 55-Jährige tritt die Nachfolge von Rob Klatell an, der seit März 2006 – mit mäßigem Erfolg – die Leitung des Anbieters elektronischer Systeme zur Dokumentenerfassung innehatte. Bish ist seit mehr als 20 Jahren im Softwaremarkt tätig. 1989 hatte er den Dicom-Konkurrenten Captiva mitbegründet, als dessen CEO er auch fungierte. Als Captiva vor zwei Jahren von EMC übernommen wurde, blieb er bis Juni 2006 als Vice President bei dem Speicherriesen und legte dann sein Amt für eine berufliche Auszeit nieder.

Atos Origin findet Deutschland-Chef

Der französische IT-Dienstleister Atos Origin hat Peter t'Jong zum Vorstandschef seiner Deutschland-Tochter ernannt. Der 46-Jährige kam 2001 zu Atos Origin und trug bis zuletzt die Verantwortung für den Bereich Managed Operations in den Niederlanden. In seiner neuen Position berichtet t'Jong direkt an Wilbert Kieboom, Member of the Management Board und Senior Executive Vice President Operations. Die Position des Deutschland-CEO war seit dem Wechsel von Gerhard Fercho zum Konkurrenten CSC im November 2006 unbesetzt.



Lynx Consulting strukturiert Vorstand um

Die SAP-Beratungsfirma Lynx Consulting AG beabsichtigt umfangreiche Veränderungen in der Chefetage. In einem ersten Schritt wurde Karsten Noss, der bislang als externer Berater für Lynx tätig war, zum Mitglied des Vorstands berufen. Der 46-jährige Diplomkaufmann verantwortet mit sofortiger Wirkung die Bereiche Personal, Marketing, Finanzen, Organisation und Beteiligungen. Für den Vorstandsvorsitzenden Peter Hüsener ist zudem eine unternehmensinterne Nachfolge vorgesehen. Als aussichtsreichster Kandidat gilt Dirk Osterkamp (47), der aktuell die Tochterfirma Agremon GmbH leitet. Die Entscheidung über die Nachfolge will der Aufsichtsrat am 3. Dezember treffen.

Gorritz wird Daimler-CIO



Die Daimler AG hat die Nachfolge für die zum Ende des Jahres 2007 ausscheidende Sue Unger geregelt: In einer unternehmensweiten E-Mail wurde den Mitarbeitern Michael Gorritz als künftiger CIO vorgestellt. Offiziell hat Daimler die Personalie allerdings noch nicht bestätigt. Der gebürtige Spanier ist derzeit als CIO Business Systeme bei der Tochtergesellschaft Mercedes Benz Cars und Vans tätig. Zuvor hatte Gorritz Anfang 2005 – noch zu Zeiten von Daimler-Chrysler – den Posten des Vice President und CIO der Mercedes Car Group übernommen.

Personalmitteilungen bitte an Menschen@Computerwoche.de

Kolumne

Spätes Softwareglück

Die Gartner-Analysten sagen sinkende Softwarepreise voraus. Zwar werden sich diese Marktverhältnisse den Auguren zufolge erst im Jahr 2011 einstellen (siehe Seite 10), aber für viele kostengeplagte CIOs ist das auf jeden Fall eine gute Nachricht. Allerdings sind die Prognosen noch zu unkonkret und hängen von zu vielen Variablen ab, als dass sie sich im mittelfristigen Planungshorizont berücksichtigen lassen würden.

Für kommende Preissenkungen sprechen laut Gartner vor allem drei Argumente: das Aufkommen von Software as a Service (SaaS), die größere Macht der IT-Dienstleister und die rasante Entwicklung in Schwellenländern wie Indien und China.

Letzteres ist unumstritten. Indien ist schon heute ein Software-Powerhouse, China hat gute Möglichkeiten, sich dazu zu entwickeln. Wenn die SAPs und Microsofts dieser Welt dort mitspielen wollen, müssen sie ihr Preisniveau auf das der lokalen Konkurrenz absenken. Das wiederum wirkt sich kurzfristig auf die Margen der Anbieter aus und mittelfristig auf die Preise in Europa und USA.

Noch nicht ausgemacht ist allerdings, dass SaaS wirklich zu niedrigeren Softwarepreisen für den Anwender führt. Als Argument für sinkende Preise führt Gartner die geringere Abhängigkeit der Anwender an und die auch dank SOA leichtere Kombinierbarkeit verschiedener Softwareprodukte. Doch je nach Ausgestaltung führt SaaS zu einer größeren Abhängigkeit. Schließlich bezieht der Kunde nicht nur seine Applikation vom Anbieter, sondern vertraut ihm auch die damit ver-



Christoph Witte
Chefredakteur CW

arbeiteten Daten an. Wer da nicht hundertprozentig aufpasst, kann noch schwerer wechseln als heute schon den Anbieter von Standardsoftware. Doch die Preise sinken nur, wenn sich die Abhängigkeit verringert.

Auch die größere Macht der Outsourcing- und BPO-Anbieter muss Software nicht unbedingt billiger machen. Sicher haben die Gartner-Berater Recht, wenn sie argumentieren, dass diese Dienstleister auf Dauer nicht mehr bereit sein werden, die hohen Margen der Softwareanbieter zu

bezahlen. Sie brauchen niedrigere Softwaregebühren, um ihre eigenen Renditeziele zu erreichen. Je stärker sich also der Trend zu Business Process Outsourcing durchsetzt, desto konsequenter werden die entsprechenden Dienstleister Software als einen Baustein ihres Service dem Kunden anbieten. Ob sie dabei die niedrigeren Preise an ihre Kunden weitergeben, hängt sehr davon ab, wie sich die Konkurrenz im Dienstleistungsmarkt entwickelt und wie stark der Kunde auf seinen BPO-Anbieter angewiesen ist.

Die Chancen auf sinkende Softwarepreise stehen insgesamt sicher nicht schlecht – vor allem der Druck aus Indien und China wird einiges bewirken –, aber es ist bei weitem noch zu früh, um darauf zu wetten.

Wie sehen Sie die Entwicklung der Softwarepreise? Sinken Sie tatsächlich, wie Gartner behauptet? Verhalten sich die Softwareanbieter in den Verhandlungen schon heute anders? Diskutieren Sie mit unter: <http://www.blog.computerwoche.de>

SAP will Tomorrow Now verkaufen

Der Rechtsstreit mit Oracle zwingt die Walldorfer zum Kurswechsel.

SAP hat die Strategie, Oracle-Kunden mit günstigen Wartungsangeboten zu locken und dann auf SAP-Produkte zu lotsen, aufgegeben. Das Management um Vorstandssprecher Henning Kagermann erwägt neben anderen Optionen den Verkauf der in Ungnade gefallenen Tochter Tomorrow Now. Teile von deren Führungsstab, darunter Firmenchef Andrew Nelson, haben ihren Hut genommen.

Mark White, der im Sommer als Executive Chairman eingesetzt wurde, soll die Geschäfte vorerst weiterführen. Hintergrund für den strategischen Schwenk ist eine Klage des Erzrivalen Oracle. Er wirft SAP vor, über die Tochter Tomorrow Now geheime Daten gestohlen zu haben.

Fehlverhalten eingeräumt

Die SAP-Konzernleitung musste danach ein Fehlverhalten der Firmentochter einräumen. Die Geschäftsprozesse von Tomorrow Now werden als Folge der Oracle-Klage seit Juli überprüft. Im Zuge dieser noch andauernden Untersuchungen wurden „nicht angemessene Downloads“ von Oracle-Servern festgestellt. Im Rahmen der internen Ermittlungen sam-

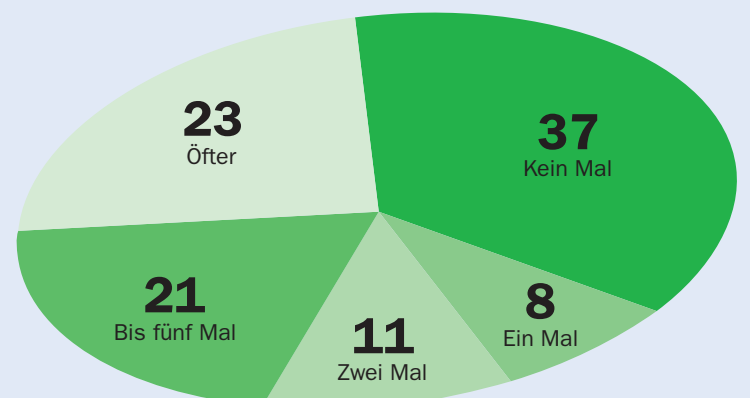
meln SAP-Mitarbeiter Material, das sie der US-amerikanischen Justiz zur Verfügung stellen müssen.

Wie der Rechtsstreit ausgeht, ist ungewiss. In etwa einem Jahr soll es in den USA den ersten Versuch einer außergerichtlichen Einigung geben.

SAP kann sich mit einem Verkauf des Tochterunternehmens keineswegs aus dem lästigen Rechtsstreit herauswinden. Der Konzern muss für Schäden auch dann geradestehen, wenn Tomorrow Now nicht mehr zur Firma gehört (siehe auch www.computerwoche.de/1848412). (fn) ♦

Frage der Woche

IT-Fachkräftemangel – wie oft wurden Sie 2007 von einem Headhunter kontaktiert?



Bei der gleichen Umfrage vor einem Jahr hatten 42 Prozent der Befragten keinen Kontakt mit einem Headhunter gehabt.

Quelle: Computerwoche.de; Angaben in Prozent; Basis: 556

Virens Scanner öffnen Hackern die Türen

Security-Experten haben eine Vielzahl von Fehlern in Antiviren-Lösungen (AV) entdeckt, durch die Virens Scanner - entgegen dem Sicherheitsgefühl, das sie vermitteln - zum Einfallstor für Schadcode werden können.

VON CW-REDAKTEURIN
KATHARINA FRIEDMANN

Sicherheitsexperten der N.runs AG haben kürzlich auf der Konferenz HackLu2007 in Luxemburg einen Proof-of-Concept demonstriert, laut dem AV-Lösungen genau das ermöglichen, wogegen sie schützen sollen: das Einschleusen und Ausführen von Schadcode. Die beiden Security-Forscher Thierry Zoller und Sergio Alvarez haben in den vergangenen Monaten Hunderte Schwachstellen in Virenschutzprodukten aufgespürt, über die Angreifer Denial-of-Service-Attacken (DoS) starten, Schadcode an der Sicherheitslösung vorbei ins Firmennetz schleusen und sogar mit Hilfe des AV-Programms zur Ausführung bringen könnten. „Von den Schwachstellen war jede auf dem Markt befindliche Scan Engine gleich mehrfach betroffen“, berichtet Zoller, Security Engineer bei dem auf Sicherheitsanalysen von Applikationen spezialisierten IT-Dienstleister. Laut N.runs handelt es sich um rund 800 dokumentierte Sicherheitslücken, die den betroffenen AV-Herstellern gemeldet wurden. Noch seien bei weitem nicht alle gepatcht.

Parsing – die Achillesferse der AV-Systeme

Bei der Inspektion des AV-Programmcodes fanden die Forscher heraus, dass die ungewöhnliche Vielzahl von Lücken auf eine Kernfunktion der AV-Lösungen zurückzuführen ist – das Parsen von Dateiformaten, also die Zerlegung der Daten in analysierbare Einzelteile. Bei diesem Vorgang verlassen sich Anwendungen – so auch Virens Scanner – häufig auf die mehr oder weniger gut dokumentierten Formatvorgaben der jeweiligen Hersteller, so dass das Kopieren von Daten in den Arbeitsspeicher ohne weitere Überprüfung des Inhalts oder seiner Länge erfolgt. Das kann Fehlberechnungen zur Folge haben und bietet damit Raum für Manipulationen. „Durch Fehlannahmen beim Parsen entstehen Konstellationen, die es ermöglichen, Exploit-Code einzuschleusen und zur Ausführung zu bringen“, beschreibt Zoller die grundsätzliche Problematik.

Durch die entdeckten Parser-Fehler könne ein Angreifer das Format einer Datei beispielsweise derart verändern, dass die AV-Software sie unanalysiert passieren lässt, der Endanwender das File aber sehr wohl öffnen und ausführen kann. Den Tests zufolge

lässt sich die AV-Software etwa mit Hilfe einer via E-Mail verschickten, präparierten ZIP-Datei aber auch dazu bringen, speziell für eine Lücke im Programm geschriebenen Exploit-Code im Zuge des Parsing-Vorgangs auszuführen – und zwar oft mit höchsten Rechten. „Das Betriebssystem



„Die große Vielfalt von Formaten und Spezifikationen macht es fast unmöglich, alle korrekt zu unterstützen.“

Thierry Zoller, N.runs AG

bemerkt also keinen Unterschied, ob hier ein Angreifer am Werk ist oder die Scan-Engine ihren Dienst verrichtet“, erläutert Zoller. Auf diesem Weg könnte ein Angreifer etwa die Kontrolle über den zentralen Mail-Server erlangen – und sich damit nicht nur Zugriff auf die gesamte elektronische Kommunikation des Unternehmens, sondern auch Zugang zu anderen kritischen Netzsegmenten und Systemen verschaffen.

Last, but not least sei es möglich, die AV-Lösung lahmzulegen oder mit ihr – je nach Implementierung – das Betriebssystem zum Absturz zu bringen. Für die Dauer der Störung bedeute dies, dass das Unternehmen entweder schutzlos ist oder, im zweiten Fall

„Es gibt vermehrt Versuche, den Virens Scanner auszuhebeln.“

Jens Freitag, Sophos

etwa bei einem E-Mail-Server, während dieser Zeit keine elektronische Post erhält, so Zoller. Den Experten zufolge lassen sich Virens Scanner aber auch dahingehend manipulieren, dass sie ständig „grünes Licht“ geben, ein Systemzugriff von außen demnach unbemerkt bleibt.

Wer viel parst, macht auch viele Fehler

Schon allein aufgrund der ständig steigenden Zahl an Dateiformaten, die AV-Software verstehen und bearbeiten, spricht „parsen“ muss, um ihr primäres Ziel – die

Erkennung möglichst vieler digitaler Schädlinge – zu erfüllen, ist ihre Fehleranfälligkeit entsprechend hoch. „Die große Vielfalt von Formaten und Spezifikationen macht es fast unmöglich, alle korrekt zu unterstützen“, so Zoller. Die in Teilen hochkomplexe Analyse jedes einzelnen

Format stelle eine potenzielle Fehlerquelle dar. Andererseits gelte im AV-Markt zwangsläufig: Je mehr Dateiformate eine Virenschutzlösung unterstützt (bei einigen Herstellern bis zu 3000 Formaten), desto besser ist der durch sie erzielte Schutz. „Die AV-Industrie und deren Entwickler stehen unter enormem Zeitdruck: Hier geht es darum, wer am schnellsten neue Gefahren erkennt – was die Qualität des Codes nicht unbedingt steigert“, gibt Zoller zu bedenken. Kritisch sei die Fehlerfülle in AV-Systemen aber auch, weil Virens Scanner heute nicht mehr nur auf dem PC, sondern in der Regel an allen zentralen Schaltstellen im Firmennetz laufen, wo die wichtigsten Daten gespeichert und verarbeitet werden. Nach Meinung der Experten ist der als „Best Practice“ propagierte Ansatz, dass die Hintereinanderschaltung mehrerer unterschiedlicher AV-Engines die Sicherheit per se erhöhe, nicht haltbar. Vielmehr gerate dieses Vorgehen, irrtümlich als „Defense in Depth“ verstanden, zum Paradoxon: „Unternehmen gehen davon aus, sich umfassend zu schützen, vergrößern aber in Wirklichkeit mit jeder zusätzlichen AV-Engine die Angriffsfläche“, so Zoller.

Auch für andere Sicherheitsspezialisten haben die Parser-Schwachstellen in Virenschutzlösungen besondere Tragweite. So wertet Wolfgang Kraft die Vielzahl der in den vergangenen Monaten publizierten Lücken in AV-Systemen als deutliches Indiz für eine Schwäche der Engines. Der auf Prozess- und Systemsicher-

Hacker suchen nach neuen Angriffswegen

heit spezialisierte IT-Berater achtet insbesondere den funktions- und wettbewerbsbedingten Spagat der AV-Hersteller als Quelle immer neuer Fehler. „Das Parsen könnte ausgefeilter sein, wären die Programmierer nicht gezwungen, jede Möglichkeit wahrzunehmen, den Prozess abzukürzen oder den Speicherbedarf zu optimieren“, verweist Kraft auf die Zwickmühle der Anbieter. So erwarte der Kunde einerseits, dass seine AV-Lösung einen neuen Schädling innerhalb von Stunden nach dem ersten Auftreten erkennt, andererseits soll der Virens Scanner vom Nutzer möglichst unbemerkt arbeiten.

Das Parsen könnte ausgefeilter sein, müssten die Programmierer den Prozess nicht abkürzen.

ihm diese verschafft – die AV-Software“, prophezeit der Consultant. Allerdings sieht Kraft hier weniger das Risiko von Massenattacken als gezielter Einbrüche.

Die AV-Industrie zeigt sich im Hinblick auf die von ihren Produkten ausgehende Problematik gelassen. Über die grundsätzliche Fehleranfälligkeit der Parser-Engines herrscht weitgehend Konsens. „Hundertprozentig ausschließen kann man nicht, dass es da mitunter Bugs geben kann“, räumt etwa Magnus Kalkuhl, Virenanalyst bei Kaspersky, ein. „Wir prüfen bei einem neuen Format immer, wie weit sich der jeweilige Interpreter in die Enge treiben lässt, wenn ihm absichtlich falsche Daten zugeführt werden.“ Das Gros der Schwachstellen, etwa beim Umgang mit gepackten Dateien, hält Kalkuhl jedoch für keine wirkliche Bedrohung, da sie im schlimmsten Fall dazu führten, dass der Rechner einfriert. „So ärgerlich ein Rechnerabsturz auch ist, wirklich ge-

fährlich ist die unbemerkte Infektion mit einem Schädling“, argumentiert der Virenanalyst. Eine solche Lücke im AV-Scanner, die sich ausnutzen lässt, um Code auszuführen, sei zwar theoretisch denkbar, aber extrem selten und erfordere erhebliches Know-how vom Angreifer.

Sophos wiederum bestätigt, dass Virens Scanner ein Angriffsziel sind. „Wir haben in unseren Labors mit Hilfe unserer Honey-pots festgestellt, dass es vermehrt Versuche gibt, den Virens Scanner auszuhebeln“, berichtet Jens Freitag, Senior Technology Consultant bei Sophos. Die Parsing-Funktionalität des Scanners sei gleichzeitig eine Schwachstelle, die schon in der Vergangenheit dazu geführt habe, dass sich dieser außer Gefecht setzen ließ. Daher habe Sophos die eigene AV-Lösung weiterentwickelt, um derartigen Angriffen entgegenzuwirken. Ein erster Schritt sei hier die „Buffer Overflow Protection“, die überwache, ob ein Programm versucht, den Stack zu überschreiben.

Symantec hat vermehrt Versuche festgestellt, mit dem AV-Scanner den ganzen Rechner lahmzulegen. „Das Thema beschäftigt uns seit geraumer Zeit, und wir bemühen uns darum, unser Produkt als Applikation sicherer zu machen, damit es nicht ausgehebelt oder missbraucht werden kann“, berichtet Michael Hoos, Technical Director Central EMEA bei Symantec. Dafür sorgten viele Selbstschutzmechanismen in der Symantec-Software und ein automatisierter Quality-Assurance-Prozess beim Testen von Virendefinitionen gegen alle gängigen Dateien. „Aber: Es ist Software! Wenn ein Angreifer sich hinsetzt und partout unser Produkt verwenden will, um etwas lahmzulegen, wird ihm das – wie bei jeder anderen Software – irgendwann gelingen“, so Hoos.

Nachdem sich die grundsätzliche Fehleranfälligkeit der AV-Lösungen beim Parsen aus genannten Gründen kaum beheben lässt, der Erkennungsmechanismus bei der Bekämpfung digitaler Schädlinge aber nicht zu ersetzen ist, gibt es nach Ansicht von N.runs nur eine Lösung: eine weiterhin hohe Erkennungsrate von Viren, allerdings eingebettet in eine sichere Architektur, die erfolgreiche Angriffe auf AV-Produkte verhindert. Die Sicherheitsexperten entwickeln daher eine Lösung (Codename „Parsing-safe“), die die AV-Hersteller als Technikpartner einbindet. ◆

Microsofts Masterplan für Virtualisierung

Das Teched IT-Forum vergangene Woche in Barcelona hatte ein Leitmotiv: Mit „System Center“ und „Windows Server 2008“ plant Microsoft die totale Virtualisierung – vom Server bis zum Client.

VON WOLFGANG MIEDL*

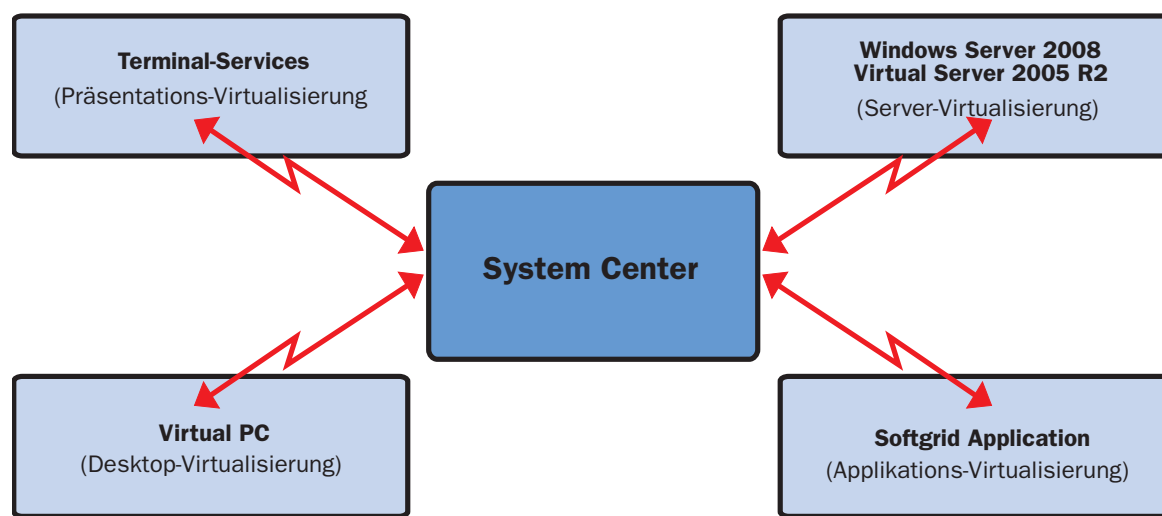
Mit der Ankündigung seines ersten Hypervisor-Produkts „Hyper-V“ präsentierte Microsoft auf seiner Kundenkonferenz ein schlagzeilenträchtiges Thema. Genau ein halbes Jahr nach der Premiere von Windows Server 2008 wollen auch die Redmonder eine zeitgemäße Server-Virtualisierung liefern. Der Druck ist offenbar enorm, wie dem Kommentar eines deutschen IT-Managers zu entnehmen war, der nicht genannt werden möchte: „Microsoft muss sich beeilen, wenn das Unternehmen beim Thema Virtualisierung noch einen Fuß in die Tür kriegen will.“ In seiner Eröffnungsrede blies Corporate Vice President Bob Kelly denn auch zum Angriff gegen Marktführer VMware: „VMware bietet weder ein robustes Software-Ökosystem noch ein integriertes System-Management, das die virtuelle und die physische IT-Umgebung unter einen Hut bringt.“

Um künftig auf der Virtualisierungswelle zu surfen, setzen die Redmonder genau hier an. Da ein Feature-Wettlauf mit der Konkurrenz um den besten Hy-

Duet 3.0

Neuigkeiten gab es auf dem Teched IT-Forum auch zu „Duet“, jenem **gemeinsam mit SAP** initiierten Projekt, das den Zugriff auf SAP-Systeme aus Microsoft Office heraus vereinfacht. In den letzten 16 Monaten sollen dafür 280 Kunden gewonnen und 770 000 Lizenzen verkauft worden sein. Microsoft kündigte für das zweite Quartal 2008 Duet 1.5 an, das neben **weiteren Szenarien** wie Einkaufs- und Recruitment-Management auch **neue Plattformen** wie Office 2007, Vista und Exchange 2007 unterstützt. Darüber hinaus gewährte der Konzern einen Ausblick auf die nachfolgende Version, die 3.0 heißen soll. Das **Integrationsprodukt** soll auf die kommende Office-Version zugeschnitten sein, geplant sind erstmals branchenspezifische Szenarien, ein eigenständiges Softwareentwicklungs-Kit sowie **Sharepoint als tragende Säule** im Microsoft-seitigen Backend anstelle des Duet-Servers. Auf SAP-Seite wahren die involvierten Komponenten Netweaver, ESA und Business Suite nach derzeitigem Stand Kontinuität. Ein Erscheinungstermin für Duet 3.0 wurde nicht genannt.

End-to-End-Virtualisierung



Quelle: Microsoft

Analysten zufolge bringt Virtualisierung nur etwas, wenn ein gutes System-Management dahintersteckt.

pervisor ohnehin kaum zu gewinnen sein dürfte, hebt der Software-Ökosystem noch ein integriertes System-Management, das die virtuelle und die physische IT-Umgebung unter einen Hut bringt.“

Um künftig auf der Virtualisierungswelle zu surfen, setzen die Redmonder genau hier an. Da ein Feature-Wettlauf mit der Konkurrenz um den besten Hy-

pervisor ohnehin kaum zu gewinnen sein dürfte, hebt der Software-Ökosystem noch ein integriertes System-Management, das die virtuelle und die physische IT-Umgebung unter einen Hut bringt.“

Um künftig auf der Virtualisierungswelle zu surfen, setzen die Redmonder genau hier an. Da ein Feature-Wettlauf mit der Konkurrenz um den besten Hy-

pervisor ohnehin kaum zu gewinnen sein dürfte, hebt der Software-Ökosystem noch ein integriertes System-Management, das die virtuelle und die physische IT-Umgebung unter einen Hut bringt.“

Der virtuelle Windows-Client

Fundamentale Veränderungen stehen auch beim einstigen Flaggschiff, dem Windows-Fat-Client, ins Haus. Bisher waren die Anwender auf Deployment- und Terminal-Produkte von Drittanbietern angewiesen, um ihre Fat-Client-Landschaften in den Griff zu bekommen. Nun präsentiert der Software-Ökosystem noch ein integriertes System-Management, das die virtuelle und die physische IT-Umgebung unter einen Hut bringt.“

Um künftig auf der Virtualisierungswelle zu surfen, setzen die Redmonder genau hier an. Da ein Feature-Wettlauf mit der Konkurrenz um den besten Hy-

pervisor ohnehin kaum zu gewinnen sein dürfte, hebt der Software-Ökosystem noch ein integriertes System-Management, das die virtuelle und die physische IT-Umgebung unter einen Hut bringt.“

hinlänglich bekannt, wobei hier als Nachteile vor allem die problematische Lastverteilung zwischen konkurrierenden Benutzern sowie potenzielle Anwendungsincompatibilitäten mit dem Server-Betriebssystem gelten.

Vista-Instanz für jeden User

Derartige Probleme lassen sich mit der „Desktop Virtualisierung“ umgehen, indem jeder Endanwender eine eigenständige XP- oder Vista-Instanz erhält. Diese residiert jedoch nicht am PC, sondern wird von einer virtuellen Server-Maschine oder auf einem Blade-PC im Rechenzentrum bereitgestellt und per RDP-Terminal-Protokoll an die jeweiligen Thin Clients publiziert

Applikations-Virtualisierung wiederum basiert auf der mit der Firma Softricity erworbenen Softgrid-Streaming-Technik. Diese bildet innerhalb eines Windows-Systems eine abgeschottete Laufzeitumgebung und sorgt dafür, dass Anwendungen und Benutzereinstellungen den Client unangetastet lassen – jegliche Zugriffe auf Dateisystem und Registrierdatenbank werden auf temporäre Ziele umgelenkt. Im Praxiseinsatz ergeben sich daraus mehrere Vorteile: Auf Terminal-Servern laufen auf diese Weise auch untereinander inkompatible Anwendungen wie Word 97, Word 2000 oder Word 2003 parallel und voneinander sauber getrennt. Weitere Einsatzszenarien

sind plattenlose PCs oder Client-Umgebungen, die aus Gründen der Wartbarkeit und Ausfallsicherheit manipulationsicher eingerichtet werden sollen. Applikationen wie Benutzereinstellungen liefert hierbei stets der Streaming-Server, der die jeweils benötigten Daten- und Programm-Bits in nahezu Echtzeit an die Clients überträgt. Die für Mitte 2008 angekündigte Version mit dem Namen „Microsoft Application Virtualization 4.5“ soll die entsprechende Integration in System Center sowie einige neue Funktionen erhalten.

Alter Name – neue Technik

Wohl um die Kunden ob dieser Vielfalt nicht zu verwirren, fasst Microsoft all diese Spielarten der Client-Bereitstellung unter dem altbekanntesten Namen „Windows Client“ zusammen. Ein erstes entsprechendes Lizenzmodell steht bereits seit Juli für Großunternehmen in Form des „Vista Enterprise Centralized Desktop“ zur Verfügung. Weitere Lizenzierungsangebote sollen folgen, doch will Microsoft wie viele andere Hersteller erst noch Erfahrungen mit Lizenzmodellen in virtuellen Umgebungen sammeln, wie Klaus von Rottkay, verantwortlich für das Server-Geschäft bei Microsoft Deutschland, gegenüber der COMPUTERWOCHE erläuterte. (ue)



*WOLFGANG MIEDL ist freier Fachjournalist in Erding bei München.

Initiative zum Breitbandausbau

Gemeinsam wollen VATM sowie der Gemeinde- und Städtetag Gebiete, in denen es kein DSL gibt, mit alternativen Internet-Zugangstechniken versorgen.

Auf einen „Masterplan“ als Ratgeber in Sachen alternative Breitbandzugangstechnologien haben sich der Verband der Anbieter von Telekommunikations- und Mehrwertdiensten sowie der Deutsche Städte- und Gemeindetag geeinigt. Der Plan soll Kommunen, die nicht mit DSL versorgt werden können, bei der Suche nach anderen Access-Technologien wie etwa Wimax oder Satellit helfen.

In einem ersten Schritt sollen hierzu topografische und auch soziodemografische Daten sowie Informationen zu Interconnection-Punkten erfasst werden, um anhand der gewonnenen Informationen besser beurteilen zu können, welche Technik sich für welches Einsatzszenario eignet

und rechnet. Dieser Ansatz geht damit über die Informationen des Breitbandatlas hinaus, der vom Bundeswirtschaftsministerium herausgegeben wird. Zudem definiert der VATM Breitband anders als der Breitbandatlas, der darunter jede Verbindung versteht, die schneller als 128 Kbit/s ist.

Berater als Mittler

Ebenso sollen im Zuge des Masterplans unabhängige Berater gewonnen werden, die dann etwa die Bürgermeister in den Gemeinden beraten. Möglicherweise werden sie die lokalen Politiker nicht nur über alternative Zugangstechnologien aufklären, sondern auch über Fördermittel aus den diversen EU- und Bundes-Töpfen. Ferner könnten

die Berater später bei der Implementierung eines entsprechenden Systems den Gemeinden zur Seite stehen.

Enthusiasten, die nun hoffen, auch im letzten Winkel der Republik Breitbandzugänge zu DSL-Kampfpreisen zu erhalten, nimmt man beim VATM gleich den Wind aus den Segeln. Die alternativen Angebote würden in diesen Gebieten immer etwas teurer sein. Zudem fordert der Verband für seine Mitglieder von der Politik eine Art Investitionsschutz: Es könne nicht angehen, dass die Telekom eine Gemeinde jahrelang aus wirtschaftlichen Gesichtspunkten nicht mit DSL versorge, dann aber – wenn die Konkurrenz investiere – plötzlich mit günstigen DSL-Tarifen locke. (hi)

Infor koppelt Altprodukte per SOA

Mit „Open SOA“ verspricht der Anbieter den Kunden, die ERP-Software zu öffnen.

Anders als Softwarehäuser wie SAP und Oracle investiert Infor nicht in umfangreiche Middleware, um die eigenen Produkte SOA-fähig (SOA = Service-orientierte Architektur) zu machen. Vielmehr sollen die einzelnen Programme im Rahmen der Strategie „Open SOA“ Schnittstellen erhalten, die eine Integration in andere Infor-Produkte sowie mit Drittsystemen über standardisierte Geschäftsdokumente erlauben. Ein Enterprise Service Bus („Infor ESB“) sorgt dabei für die Kommunikation.

Auf diese Weise können ERP-Kunden Erweiterungssysteme von Infor einbinden. Die „Business Information Services“ beispielsweise erlauben es Nutzern, Berichte und Kennzahlen abzu-

(vormals AS/400) laufenden Geschäftsanwendungen. Dazu zählen unter anderem Applikationen von Brain und Mapics. Um Zusatzbausteine auch in die auf

RPG basierenden Programme einzubinden, muss Infor jedoch in den Quellcode eingreifen.

Neben den für den Kunden kostenlosen Erweiterungen plant

Infor darüber hinaus kostenpflichtige Zusatzbausteine. Laut Infor-Chef Jim Schaper soll es eine Variante von „Infor CRM Epiphany“ für Baan- und ERP-COM-Nutzer geben. Unlängst für Europa freigegeben hat Infor die ebenfalls optionale Produktfamilie „Performance Management 10“.

Mitte nächsten Jahres soll eine CRM-Software für die verschiedenen AS/400-basierenden Produkte von Infor auf den Markt kommen. Die Lösung geht auf Entwicklungen von Geac („System 21“) zurück.

Weitere Informationen zum Thema finden Sie unter www.computerwoche.de/1848143. (fn) ♦



Kunden können neue Module andocken. ERP-eigene Komponenten pflegt Infor weiter, verspricht Bruce Gordon, CTO.

rufen, Aufgaben zu verwalten und auf Ereignismeldungen zuzugreifen. Als Frontends dienen neue, interaktive Web-Seiten („Homepages“). Auf den Homepages verweilt der Anwender jedoch nicht dauernd: Sobald er eine ERP-Funktion aufruft, zum Beispiel zum Erfassen eines Auftrags, erscheint die bekannte Benutzerschnittstelle. Dass Infor alte und neue Oberflächen vermischt, hat wirtschaftliche Gründe. „Es wäre viel zu aufwändig, sämtliche Masken von Baan IV und V umzuprogrammieren“, so Bruce Gordon, Chief Technology Officer des Softwarehauses.

Gemeinsames Hauptbuch

Weitere Entwicklungen zielen darauf ab, bestehende ERP-Module durch angeflanschte SOA-Komponenten zu ersetzen. Mit einem „Multibook“ können Unternehmen ihre Systemumgebungen für die internationale Rechnungslegung fit machen. Das externe Rechnungswesen könnte ein Baan-Kunde ebenfalls über den Infor ESB einbinden und somit das interne Hauptbuch umgehen, wenn er dies wünscht.

Anhand des Multibooks wird die Stoßrichtung von Infor deutlich. Die Softwarefirma bietet vermehrt moderne Funktionsbausteine an, die Anwender alternativ zu bestehenden ERP-Modulen nutzen können. Statt vieler Hauptbücher in den jeweiligen Systemen muss Infor irgendwann nur noch das Multibook verwalten, das sich an alle ERP-Softwareprodukte andocken lässt.


Modernisieren will Infor auch die auf der System-i-Plattform

DER FOUNDRY-VORTEIL FÜR UNTERNEHMEN:
**SIE UND UNSER SWITCH
 HABEN ETWAS GEMEINSAM.**
**SIE BEIDE SIND
 FÜR DIE
 ZUKUNFT GERÜSTET**
 HEUTE DIE SKALIERBARSTE POE-LÖSUNG AUF DEM MARKT
 BEREIT FÜR DAS IPV6-NETZWERK VON MORGEN.

Copyright © 2007 Foundry Networks, Inc. Alle Rechte vorbehalten.

ÜBERZEUGEN SIE SICH SELBST

Sicher. Skalierbar. Fit für künftige Anforderungen. Nennen Sie es, wie Sie wollen. Wenn Sie heute einen Foundry-Switch installieren, sind Sie für die Zukunft bestens gerüstet. Unsere Enterprise-Lösungen gibt es in kompakten Modulen für höchste Ansprüche – einschließlich Unterstützung von 10 GbE, Advanced Layer 2, IPv4, IPv6 und PoE. Foundrys umfassendes Angebot an Lösungen für die Zugangskontrolle mit integrierten Sicherheitsfunktionen wie Closed-Loop-Betrieb schützen Ihr Netzwerk effektiv vor internen und externen Angriffen. Und weil wir einen offenen Standard verwenden, genießen Sie freie Auswahl bei den besten Lösungen anderer Händler. Wenn Sie für Ihren nächsten Switch bereit sind, dann sollte Ihr Switch bereit für die Zukunft sein. foundrynet.com/believer


**FOUNDRY
 NETWORKS**
The Power of Performance™