

Mangelndes Vertrauen in einen jungen Markt

Unternehmen lagern Sicherheit ungern aus

MÜNCHEN (jha) – Das Auslagern von IT-Sicherheitseinrichtungen ist in Deutschland bislang ein Nischengeschäft. Der Markt ist nicht konsolidiert und der Erfahrungsschatz begrenzt. Allerdings steigen die Anforderungen, so dass es den Unternehmen zunehmend schwerer fallen dürfte, ihre IT in Eigenregie gegen unliebsame Gäste abzuschotten.

DAS SICHERHEITSBEWUSSTSEIN der IT-Verantwortlichen in deutschen Unternehmen steigt, gleichzeitig klagen sie über Personalmangel und schmale Security-Budgets – das ist ein Ergebnis einer Umfrage der Meta Group unter 209 hiesigen Anwenderunternehmen im vergangenen Februar. Ideale Voraussetzung für Anbieter von Managed Security Services (MSS), die die Sicherheitssysteme im Kundenauftrag pflegen und warten. Die Meta Group rechnet für Dienste wie Managed Firewall Services, Managed Virtual Private Networks (Managed VPNs), Managed Intrusion Detection Systems (Managed IDS) sowie Vulnerability Scanning in Deutschland mit einem Wachstum zwischen zehn und 15 Prozent. Der Markt für Security-Betriebsdienste wird somit deutlich stärker wachsen als der für Beratung und Systemintegration im IT-Sicherheitsumfeld.

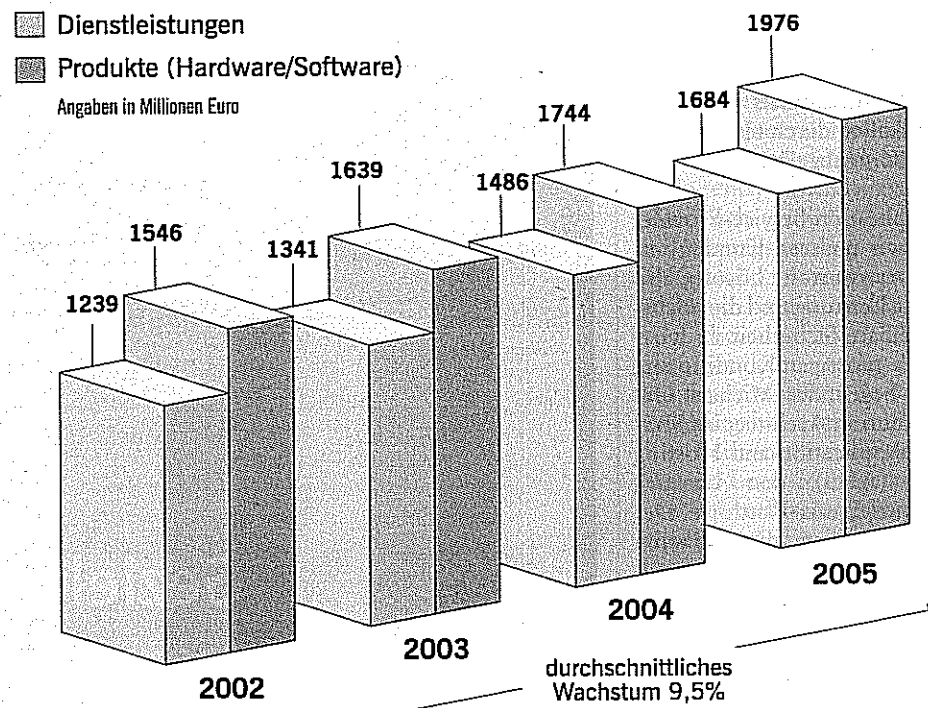
Zweistelliges Wachstum gilt als sicher

Noch optimistischer geben sich die Kollegen von Forrester Research. Sie sagen für die europaweit vertriebenen MSS-Offerten ein durchschnittliches Jahreswachstum von 37 Prozent voraus. Allerdings stecken die Forrester-Analysten den Rahmen etwas anders ab. Sie betrachteten das Geschäft mit Managed Firewalls, Managed IDS, Vulnerability Assessments sowie Managed Public Key Infrastructure (Managed PKI). Die stolzen Zahlen dürfen allerdings nicht darüber hinwegtäuschen, dass der Markt von einer sehr kleinen Basis aus startet. In Europa nehmen sämtliche MSS-Anbieter den Marktforschern zufolge in diesem Jahr zusammen rund 962 Millionen Euro ein. Das ist deutlich weniger als der Jahresumsatz von Symantec. Der Vertrieb von Security-Produkten und -Diensten brachte dem Anbieter im letzten Jahr rund 1,41 Milliarden Dollar ein. Damit legte Symantecs Geschäft im Jahresvergleich um 31 Prozent zu.

Wachstum und Umsatz sind demnach nur bedingt aussagekräftig, selbst die Meta Group räumt ein, dass die Durchdringung des Marktes mit verwalteten Sicherheitsdiensten dürftig ist. Lediglich die Firewall-Verwaltung ist ein gut akzeptierter Service in Deutschland, ihn nutzen immerhin 40 Prozent der befragten Unternehmen. Zu ihnen zählt Gerhard Büchner, IT-Leiter beim Personaldienstleister und -vermittler DIS Deutscher Industrie Service AG, Düsseldorf: „Wir haben unsere 85 Niederlassungen via VPN an ein zentrales Data-Center angeschlossen. Den Betrieb und das Management der zentralen und dezentralen Firewalls verantwortet die SHE AG aus Ludwigshafen.“ Bislang sind derartige Outsourcing-Projekte allerdings noch die Ausnahme. Das Gros der von der Meta Group befragten Anwender betreibt die Security-Anlagen noch selbst und plant dies auch weiterhin.

Wenig geschäftsfördernd ist vermutlich auch

IT-Security In Deutschland: Wachsendes Outsourcing wider Willen



Quelle: Meta Group

CW 33/03-tp

Der Markt für IT-Security-Dienstleistungen umfasst das Beratungs-, Systemintegrations- und Outsourcing-Geschäft. Letzteres Marktsegment wird laut Einschätzungen der Meta Group überdurchschnittlich wachsen.

das anhaltende Verwirrspiel um die Inhalte. Vor allem unter dem MSS-Label werden zahlreiche Dienste vertrieben, etwa auch automatische Virens Scanner. Nicht zuletzt die unterschiedlichen Ausführungen der Marktexperten verdeutlichen anschaulich, dass es keinen einheitlichen MSS-Begriff gibt. Für die Meta Group ist der Betrieb eines Virtual Private Network (VPN) integraler Bestandteil der MSS-Definition, bei Forrester spielen diese Angebote im Rahmen der eigenen MSS-Bezeichnung keine Rolle. Andernorts werden das Security-Outsourcing und die Managed Security Services synonym verwendet, wogegen sich Wolfram Funk verwehrt: „Managed Security Services ist ein Teilbereich des Security-



„In der Vergangenheit sind viele junge Unternehmen mit Angeboten rund um Managed Security Services gestartet und gescheitert.“

Wolfram Funk, Meta Group Deutschland

Outsourcing. Hierzu gehören im weiteren Sinne auch Managed Services für Virenschutz und Content-Filtering. Diese werden aber direkt von den Produktanbietern erbracht. Typische Outsourcing-Themen neben den Managed Security Services sind Trust-Center-Dienstleistungen im Zusammenhang mit der elektronischen Signatur sowie klassische Hochverfügbarkeitsthemen“, erklärt der Meta-Berater, der für die Bereiche IT-Dienstleistung und -Sicherheit verantwortlich ist.

Das Votum der Anwender für den Eigenbetrieb lässt sich aber auch als mangelndes Ver-

trauen in einen relativen jungen Markt interpretieren, und Skepsis scheint in der Tat angebracht: „Beim Outsourcing sollten sich Anwender immer die Frage stellen, ob der Anbieter die Leistungen dauerhaft erbringen kann. In der Vergangenheit sind viele junge Unternehmen mit Angeboten rund um Managed Security Services gestartet und gescheitert. Der Markt konsolidiert sich“, warnt Funk.

Die Anbieter, die durchkommen, hoffen auf einen Sinneswandel der Anwender, weil Sicherheit ihrer Meinung zufolge kaum noch in Eigenregie zu schaffen ist. Die weltweite Vernetzung sowie die tiefe Integration der Partner und Zulieferer in die IT der Unternehmen stellen hohe Ansprüche. Unbefugten muss der

Zutritt verwehrt, Kunden, Mitarbeitern und Partner hingegen Zugang zu unterschiedlichen Ressourcen und Bedingungen gewährt werden, und zwar rund um die Uhr. Das ist teuer und erfordert häufig einen Dreischichten-Betrieb, denn Firewall, Netzwerk-Layer, Betriebssystem und

Router wollen permanent überwacht und angepasst werden. „Ein Drei-Schicht-Betrieb ist bei uns nicht zwingend erforderlich. Um die Sicherheit der IT-Systeme selbst zu gewährleisten, hätten wir aber zwei bis drei weitere Mitarbeiter einstellen müssen, da wir die entsprechende Kompetenz nicht im Haus haben“, räumt DIS-Manager Büchner ein. Die Systeme müssen beispielsweise ständig aktualisiert werden, um gegen neue Bedrohungsszenarien gewappnet zu sein. Änderungswünsche der Fachabteilungen, weil etwa eine neue Applikation angeschafft oder Niederlassungen eröff-

net wurden, tun ein Übriges, um die Sicherheitsexperten zu beschäftigen.

Wie beim klassischen Rechenzentrums-, Netzwerk- oder Desktop-Outsourcing spielen die Kosten eine große Rolle bei der Entscheidungsfindung, doch bei den bisher abgeschlossenen MSS-Verträgen hat sich gezeigt, dass die Anwender mehr noch als bei anderen Auslagerungsprojekten auf das Fachwissen, die Ressourcen und Kapazitäten der externen Dienstleister bauen. „Wir sind wiederholtes Ziel von Viren- und Hacker-Attacken“, schildert Bib Spencer, Chef der IT-Abteilung der britischen Handelsbank Lloyds TSB, der die Sicherheitsanlagen des Hauses von Unisys betreiben lässt. „Der Unisys-Dienst bringt uns zwar keine Kostenersparnis, er räumt uns aber Zugriff auf Spezialwissen ein, das wir intern nicht aufbauen können. Zudem haben wir stets aktuelle Hinweise auf mögliche Angriffe.“

Security bleibt in Eigenverantwortung

Das Security-Outsourcing unterscheidet sich in einem weiteren Punkt von herkömmlichen Auslagerungsverträgen. Weil Sicherheitsthemen in großem Maße Vertrauen erfordern, haben viele Kunden Bedenken, ihre Geräte einem externen Dienstleister zu überlassen. Während beim Übergang von Rechenzentren komplette Anlagen und Systeme den Eigentümer wechseln, sind die Anwender beim Thema Sicherheit



„In den Unternehmen sprießt allmählich die Erkenntnis, dass Sicherheit auch einen Mehrwert für das Geschäft liefern kann.“

Peter Wirnsperger, Deloitte & Touche

diesbezüglich sehr viel zurückhalten. „Viele Unternehmen würden ihre Security-Installationen niemals außer Haus geben“, schildert Urs Brawand, CEO des Sicherheitsspezialisten und Security-Dienstleisters Celeris AG in Hinwil, Schweiz. „Sie wollen ihren Datenverkehr nicht über eine gemeinsam mit anderen Unternehmen genutzte Firewall vermitteln.“ Technisch ist dieser Wunsch ohne weiteres zu erfüllen, Celeris verwaltet beispielsweise per Fernzugriff überwiegend Security-Geräte, die in den Räumen der Kunden stehen und ihnen gehören. „Den Unternehmen ist es wichtig, rasch und unbürokratisch den Betreiber zu wechseln, sollten sie mit ihm unzufrieden sein“, erläutert Brawand. IT-Leiter Büchner bestätigt diese Einschätzung: „Sämtliche Firewalls, Router und Server gehören der DIS AG. Wir sind zwar sehr zufrieden mit unserem Service-Provider, wollen aber unabhängig bleiben und in der Lage sein, jederzeit den Anbieter zu wechseln.“

Anwender sollten umdenken

Die Frage nach dem Eigentümer der Geräte ist für Peter Wirnsperger von der Deloitte & Touche GmbH in Hamburg hingegen zweitrangig. Der Senior Manager der Security Services Group befürwortet sogar das Outsourcing an einen zuverlässigen Betreiber, solange die Prozesse noch im eigenen Haus zusammengehalten werden. Denn die so eingesparte Arbeitszeit der Mitarbeiter lässt sich besser nutzen. Statt mit routinemäßigen Wartungsdiensten sollten die Unternehmen ihre Fachkräfte besser damit beschäftigen, strategische IT-Projekte weiterzubringen und beim Entdecken und Ausweiten neuer Geschäftsfelder einen aktiven Part zu spielen. „In den Unternehmen sprießt allmählich die Erkenntnis, dass Sicherheit nicht allein dazu da ist, Schlimmes zu verhindern; sie kann auch einen Mehrwert für das Geschäft liefern.“

Das setzt allerdings zwischen Service-Provider und Kunde eindeutige Schnittstellen, Absprachen und Abläufe voraus. Auftraggeber und -nehmer sollten Klarheit darüber haben, wie ein Prozess angestoßen wird und wer wann welche Aufgaben zu erledigen hat, um etwa Änderungswünsche schnell und verbindlich umzusetzen. „Ab Eingang des Änderungsauftrags garantieren wir im Rahmen der Service-Level-Agreements (SLAs), dass die Arbeiten innerhalb von 30 Minuten gestartet werden“, verspricht Celeris-Manager Brawand. Ähnliche Zeitrahmen gelten für außergewöhnliche Zwischenfälle. Bei Attacken, Virenbefall oder Ausfall wichtiger Komponenten geht spätestens nach 30 Minuten eine Alarmmeldung an den zuständigen Mitarbeiter des Kunden. Dazu sind für jedes denkbare Ereignis detaillierte Prozesse dokumentiert, wie die Beteiligten sich zu verhalten haben.

Die Meta Group hingegen bezweifelt, dass das Gros der Anbieter konkret umsetzbare und verbindliche SLAs in der Schublade hat. Technische Meßgrößen wie Firewall-Uptime sowie Verfügbarkeit, Kapazität und Durchsatz von Intrusion-Detection-Systemen, ergänzt durch operative Anhaltspunkte wie Antwortzeiten bei Änderungsanfragen, Reaktionszeit auf Sicherheitsalarme sowie Zeitbedarf für Updates von Antivirus- und IDS-Signaturen, sollten zwar Bestandteil eines Outsourcing-Vertrags im Sicherheitsbereich sein. Die Meta

Group plädiert jedoch für einen ganzheitlichen Ansatz, der technische und operative Messgrößen sowie das Risk-Assessment, also die regelmäßige Kontrolle der Sicherheitseinrichtungen, umfasst. Der Anbieter sollte regelmäßig ein detailliertes Reporting liefern.

Diesen Empfehlungen sind die Partner SHE und DIS mit ihren Vereinbarungen relativ nahe gekommen: Der Dienstleister liefert regelmäßige Reports und informiert via Ticket-System über mögliche Bedrohungsszenarien. Zudem werden die DIS-Mitarbeiter zeitnah über Vorfälle verständigt. „Wir haben uns bewusst für einen kleinen Anbieter entschieden, um flexibel reagieren zu können. Die Prozesse sind nicht festgezurrt, gewöhnlich arbeiten die DIS-Administratoren partnerschaftlich mit den Betriebsmitarbeitern von SHE zusammen.“ Dennoch baute Büchner eine weitere Kontrollstufe ein, immerhin schicken die Niederlassungen via VPN häufig kritische Kunden- und Mitarbeiterdaten, es käme einer Katastrophe gleich, sollten diese Informationen in fremde Hände gelangen. Deshalb überprüft ein weiterer unabhängiger Dienstleister turnusmäßig die gesamte Sicherheitsanlage auf Verlässlichkeit.

Angestoßen wurde das Sicherheitsprojekt bei DIS durch den hohen Virenbefall. Bevor die Filialen via VPN vernetzt wurden, gab es keine einheitliche Lösung. Nachdem der zentrale Mail-Server dann vom in Konkurs geratenen Dienstleister nicht mehr gepflegt wurde, brach die Virenplage über die DIS-Systeme herein. „Damals wurde der Entschluss gefasst, eine zentrale Sicherheitslösung zu installieren“, so der IT-Chef.

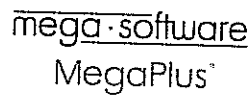
Wie funktioniert der CW-MARKTPLATZ?

Ganz einfach! Sie schalten über einen Zeitraum von 1/4 Jahr bzw. 1 Jahr Ihre Marktplatz-Anzeige in der entsprechenden Rubrik. Potentielle Kunden finden auf Anhieb Ihre Anzeige. Mit Ihrer Buchung sind Sie für Ihre Kunden automatisch auch online präsent – in den Standard-Online-Seiten des CW-Marktplatzes mit einem zusätzlichen Link zu Ihrer Homepage. Ihr Vorteil: Optimale Werbewirkung und zeitgemäße Kommunikation zu minimalen Kosten. Nähere Informationen erhalten Sie jederzeit unter:

Telefon: 0180/5236868

ANWENDUNGS-SOFTWARE

Mega Software GmbH
Über 600 mittelständische und große Unternehmen setzen MegaPlus erfolgreich und effizient ein.
• Finanzbuchhaltung
• Kostenrechnung
• Anlagenbuchhaltung
• Lohn und Gehalt
• Personalzeiterfassung
• Warenwirtschaft
• Integration Branchensysteme
Server: Unix, Linux, Windows
Datenbanken: Oracle, Informix, MySQL
Mega Software GmbH, Hauert 1, 44227 Dortmund
Tel.: 0231/9749-153, Fax: 0231/9749-157
www.mega-software.de, info@mega-software.de



PAYMENT-ANBIETER

ebs Electronic Billing Systems AG
Internet-Zahlungssysteme, Elektronische Lastschrift, Kreditkartenclearing, Finanzmanagement, Risikomanagement.
Lilienthalstraße 5
85399 Hallbergmoos
www.ebs-ag.de
info@ebs-ag.de
Tel. 0811/5546-300
Fax 0811/5546-399



PAYMENT-ANBIETER

Wire Card AG
Risikomanagement-Lösungen, Payment & Integration, elektr. Zahlungseinzug und Auszahlungen, Risk-Management, Optimierung aller Finanzprozesse
Lilienthalstraße 5
85399 Hallbergmoos
www.wirecard.com
info@wirecard.com
Tel. 0811/5546-400
Fax 0811/5546-499



SAP BW UND SEM

s2s AG
Wir von s2s AG bieten Ihnen kompetente Unternehmensberatung mit folgenden Schwerpunkten:
• Geschäftsprozessanalyse und -optimierung
• mySAP.com BW und SEM
• Beratung und Entwicklung für SAP R/3
• Releasewechsel auf Enterprise/ 4.7
Unsere Berater verbinden umfassendes betriebswirtschaftliches Know-how mit fundierten Kenntnissen der Informationstechnologie für Ihren Projekterfolg. Fordern Sie unser Unternehmensprofil mit Referenzen an.
s2s AG
Theresienstr. 114
80333 München
Tel.: 089/52 057 280
Mail: service@s2s.de
www.s2s.de



ASSET-MANAGEMENT & HELPDESK

OMEGA Software GmbH
Asset-Management; HelpDesk; Leistungsverrechnung; Kosten- und Vertragsverwaltung; datenbankunabhängig. Anbindung an SAP, SMS, HP, Mail, uvm.
Schloß Weiler
74182 Obersulm
vertrieb@omegasoft.de
www.omegasoft.de
Tel. 07130/4006-0
Fax 07130/4006-40



CALLCENTER

Konzept Telemarketing Service GmbH
Telefonmarketing - Kompetent mit Herz und Verstand. Im Inbound oder im Outbound. Sie setzen die Prioritäten - Unser Know-how bringt den Erfolg.
Insterburger Straße 7
56564 Neuwied
Tel. 02631/944-400
Fax 02631/944-411

DIREKTMARKETING

Konzept Marketing Service GmbH
Zielgruppenorientiertes Dialogmarketing u. effektive Verkaufsförderung für die EDV-Branche. Adreßmaterial, Konzeption, Produktion, Versand u. Warehousing
Insterburger Straße 7
56564 Neuwied
Tel. 02631/944-100
Fax 02631/944-111

PASSGENAUE SOFTWARELÖSUNGEN

Schettler Consulting KG – Ihr innovativer Partner
• Anwendungsbezogene Lösungen
• Zusammenführung heterogen gehaltener Daten
• Eigener Taskmanager / Dienst auf Windows 2000, XP
• Replikation so zeitnah wie nötig
• Fachgerechtes Reengineering von Altsystemen
• Realisierungen auf Client-Server und Mainframe
• Volle Gewährleistung, Projektübernahme zum Festpreis
Sommeraktion 2003: Profitieren Sie von unseren günstigen Konditionen.
Brüder Allee 1
91207 Lauf a. d. Peg.
www.schettler-consulting.de
info@schettler-consulting.de
Tel.: (0 91 23) 96 29 9-0
Fax.: (0 91 23) 96 29 9-99



SCHULUNGEN

ORDIX AG
Softwareentwicklung, Schulung, Beratung, Systemintegration. Durchführung von öffentlichen und Inhouse-Seminaren zu den Themen ORACLE, INFORMIX, BMC PATROL, UNIX, JAVA, OO, INTERNET, PERL, IT-Projektmanagement.
Kreuzberger Ring 13
65205 Wiesbaden
training@ordix.de
http://training.ordix.de
Tel.: 06 11 / 778 40 00
Fax.: 06 11 / 778 40 11



WEITERBILDUNG

Technische Akademie Esslingen (TAE)
Geschäftsfeld Informationstechnologie
Durchführung von Trainings in Form von öffentlichen und Inhouse-Seminaren zu den Themenbereichen:
• Betriebssysteme / Zertifizierungen
• PC-Endanwendersoftware / IT-Anwendungen
• Softwareengineering / Softwareentwicklung
• Telekommunikation / Vernetzung
• Internet, Intranet, E-Business
• CAD / CAM
An der Akademie 5
73760 Ostfildern / Nellingen
www.tae.de
info@tae.de
Tel. 0711/34008-76
Fax 0711/34008-30

