

IBM Internet Security Systems – Produkte und Services

Highlights

- **Schutz kritischer Ressourcen und Kostensenkungen durch Abwehr von Gefahren aus dem Internet**
- **Schutz der gesamten IT-Infrastruktur und Entlastung Ihrer IT-Mitarbeiter, die sich auf Kerngeschäftsaufgaben konzentrieren können**
- **Abwehr von Angriffen ohne Beeinträchtigung der Netzwerkbandbreite und -verfügbarkeit**
- **Unterstützung unterbrechungsfreier Geschäftsabläufe durch Reduzierung von Ausfällen**
- **Höhere Mitarbeiterproduktivität durch Abwehr von Viren und Spam**
- **Management, Überwachung und Bewertung der unternehmensweiten Sicherheit zur Unterstützung der Einhaltung gesetzlicher Bestimmungen**

Bleiben Sie Gefahren immer einen Schritt voraus

Die Sicherheitsbedrohungen, mit denen wir heute konfrontiert sind, lassen wenig Raum für Fehler. Zur konsequenten Abwehr von Angreifern aus dem Internet, die intelligent und aggressiv vorgehen, ist ein Portfolio an Technologien und technischem Know-how erforderlich, das ständig weiterentwickelt wird. Doch nur wenige Unternehmen können es sich leisten, diese wesentlichen Bestandteile der unternehmensweiten Sicherheit in Eigenregie zu entwickeln und auf dem neuesten Stand zu halten.

Ein effektives Sicherheitsmanagement ist mit zahlreichen Herausforderungen verbunden. Es erfordert hoch qualifizierte Mitarbeiter, die nur mit hohem Kostenaufwand zu finden und zu halten sind. Außerdem müssen für das Sicherheitsmanagement die ohnehin knappen IT-Mitarbeiter von Kerngeschäftsaufgaben abgezogen werden, die für Produktivität und das Wachstum des Unternehmens entscheidend sind. Darüber hinaus

setzen immer strengere gesetzliche Bestimmungen, die ein bestimmtes Sicherheitsniveau vorschreiben, die Unternehmen zusätzlich unter Druck. Das Management der unternehmensweiten Sicherheit ist ein schwieriger Balanceakt: Ohne richtiges Sicherheitsmanagement wird nicht nur unerlaubter, sondern möglicherweise auch erwünschter Datenverkehr blockiert. Dies führt dazu, dass Transaktionen nicht zustande kommen oder sich verzögern, worunter die Kundenzufriedenheit und der Umsatz leiden. Und nicht zuletzt erschweren die ständig steigenden und oftmals unvorhersehbaren Kosten für die Sicherheit die Finanzplanung und Ressourcenoptimierung.

Um Unternehmen bei der Bewältigung dieser komplexen Herausforderungen zu unterstützen, bietet IBM Internet Security Systems (ISS) ein breites Spektrum an zentral administrierten präventiven Produkten und Services an, die auf Forschungsergebnissen zu Sicherheitslücken und mehrstufigen Sicherheitsmethoden basieren.

Schutz der gesamten IT-Infrastruktur

Die IBM ISS-Lösungen für präventive Sicherheit sind eng mit vorhandenen IT-Geschäftsprozessen verknüpft, um die gesamte Infrastruktur besser abzusichern – vom Gateway über den Kernbereich bis zu den entferntesten Endpunkten. Die Grundlage des ISS-Angebots bildet die IBM Proventia-Produktfamilie. Diese leistungsfähige und umfassende Plattform, bestehend aus Virenschutz, Firewall, VPN, Erkennung und Abwehr unbefugter Zugriffe, Anwendungsschutz, Spam- und Content-Filtern, basiert auf den Erkenntnissen des Forschungs- und Entwicklungsteams IBM ISS X-Force.

Die zentral gesteuerte Proventia-Produktfamilie beinhaltet folgende Angebote:

IBM Proventia Network Intrusion Prevention System – wehrt Angriffe auf das Netzwerk automatisch ab und stellt gleichzeitig die Netzwerkbandbreite und -verfügbarkeit sicher. Dieses auf der herausragenden Sicherheitsforschung des X-Force-Teams basierende Produkt bietet außergewöhnlich umfassenden Schutz vor unbekanntem Gefahren.

IBM Proventia Network Multi-Function Security – schützt mehr Komponenten mit geringerem Kostenaufwand. Diese Lösung kombiniert Intrusion Prevention (Abwehr unbefugter Zugriffe) mit Firewall- und VPN-Funktionalität, verhaltens- und signaturbasiertem Virenschutz, Webfiltern und Spam-schutz. Diese UTM-Appliance (Unified Threat Management) schützt Ihr Unternehmen automatisch vor mehr als 1.000 Sicherheitslücken, mehr als 120.000 bekannten Viren, über 93 Prozent der unbekanntem Viren und weiteren kombinierten Gefahren sowie 95 Prozent Spam.

IBM Proventia Network Anomaly Detection System – verbessert die Netzwerküberwachung und -sicherheit durch Prüfung von Netzwerkverkehrsdaten von bestehenden Infrastruktureinheiten. Diese Lösung, die das Netzwerkverhalten analysiert, verschafft Ihnen einen präzisen Überblick über die Schwachstellen Ihres Netzwerks, indem sie automatisch aktive Sicherheitsbedrohungen, riskantes Benutzerverhalten, Leistungsprobleme und Verstöße gegen Sicherheitsrichtlinien erkennt.

IBM Proventia Network Enterprise Scanner – überprüft Ihr gesamtes Netzwerk, um die darin enthaltenen Ressourcen und möglichen Schwachstellen zu ermitteln. Die Lösung bietet Ihnen außerdem die Möglichkeit, Aktivitäten zum Schutz des Netzwerks zu priorisieren und Ihren Mitarbeitern zuzuweisen sowie Berichte zu den Ergebnissen zu erstellen. Die Lösung, die auf der umfangreichen, branchenweit anerkannten Schwachstellendatenbank des X-Force-Teams basiert, erlaubt das Management von Sicherheitslücken mithilfe nativer Trouble-Ticketing-Funktionen, die von Workflow-Funktionen unterstützt werden, um Managementaktivitäten in Ihrer gesamten Infrastruktur zu steuern.

IBM Proventia Web Filter – blockiert unerwünschte Webinhalte mittels einer ausgereiften Technologie, die eine Text- und Bildanalyse mit einer der weltweit größten URL- und Bilddatenbanken kombiniert. Diese leistungsstarke und präzise Lösung trägt dazu bei, die Produktivität zu erhöhen und Richtlinien zur Internetnutzung umzusetzen.

IBM Proventia Mail Filter – überwacht den Inhalt von E-Mails und blockiert automatisch Spam und weitere unerwünschte oder illegale Inhalte. Die Lösung nutzt hoch entwickelte Analysemethoden sowie eine Datenbank, die mehr als 200.000 relevante Beispiele von Spam und mehr als 20 Millionen Websites enthält. Sie erkennt harmlose E-Mails und leitet diese sofort weiter, während unerwünschte E-Mails abgeblockt werden.

IBM Proventia Server Intrusion Prevention System – kombiniert eine Firewall und Anwendungskontrollen mit präventiven Technologien zum Schutz vor Pufferüberläufen und zur Abwehr unbefugter Zugriffe. Diese mehrstufige Lösung empfängt automatische Updates von Sicherheitsinhalten, um Sicherheitslücken zu schließen, bevor Patches der entsprechenden Anbieter eingespielt werden, und schützt Server, auf denen Microsoft® Windows® oder Linux® läuft.

IBM Proventia Desktop Endpoint Security – ist eine Präventivlösung, die Angriffe abwehrt, bevor sie zu Ausfallzeiten und einer übermäßigen Anzahl an Anrufen beim Help-Desk führen können. Dieser einzelne Agent bietet eine Personal Firewall, Intrusion Prevention (Schutz vor unbefugten Zugriffen), Schutz vor Pufferüberläufen, Anwendungsschutz und Virenschutz. Damit stellt er sicher, dass Desktops geschützt sind und mit unternehmensinternen Standards übereinstimmen.

IBM Proventia Management SiteProtector System – steuert, überwacht und bewertet die unternehmensweite Sicherheit. Mit Berichten, die als Nachweis angemessener Sorgfalt dienen, unterstützt Sie das System bei der Einhaltung gesetzlicher Bestimmungen. Zudem stellt es Failover-Funktionen bereit, die unterbrechungsfreie Geschäftsabläufe sicherstellen. Durch Bereitstellung einer Konsole für das zentrale Management einer ganzen Palette von Sicherheitsprodukten entlastet das SiteProtector-System Ihr IT- und Sicherheitspersonal und sorgt für unternehmensweite Transparenz der Sicherheit.

Darüber hinaus hat IBM ISS zusätzliche Produkte im Angebot, die auf die Proventia-Produktfamilie abgestimmt sind und Ihr Unternehmen vor Gefahren schützen. Dazu gehören folgende Produkte:

IBM RealSecure Server Sensor – erlaubt die automatisierte Erkennung und Abwehr von unbefugten Zugriffen in Echtzeit. Das Produkt analysiert neben Ereignissen und Hostprotokollen auch den ein- und ausgehenden Netzwerkverkehr auf unternehmenskritischen Servern, um zu verhindern, dass böswillige Angriffe kritische Ressourcen beschädigen. Dieses leistungsstarke Angebot nutzt integrierte Signaturen und eine hoch entwickelte Protokollanalyse mit Verhaltensmustern und automatischer Ereigniskorrelation zur Abwehr bekannter und unbekannter Angriffe.

IBM RealSecure Network – enthält Funktionen für die Erkennung und Abwehr unbefugter Netzwerkzugriffe, die Netzwerksegmente innerhalb eines zentralisierten Betriebs- und Management-Frameworks überwachen. Dieses Produkt unterstützt eine außergewöhnlich hohe Netzwerksicherheit und überzeugt mit höchster Präzision bei der Erkennung von böswilligen Angriffen auf das Netzwerk.

Verringerung der Gefahren aus dem Internet für geschäftskritische Ressourcen

IBM ISS ergänzt seine Produktfamilie mit erstklassigen Sicherheitsservices, die Sie bei der Ausarbeitung, Implementierung und Aufrechterhaltung einer soliden Sicherheitsstrategie unterstützen.

Mit einer kompetenten Sicherheitsberatung versetzen die IBM Professional Security Services Unternehmen jeder Größe in die Lage, Risiken zu verringern, gesetzliche Bestimmungen einzuhalten, unterbrechungsfreie Geschäftsabläufe sicherzustellen und ihre Ziele in puncto Sicherheit zu erreichen. Die Berater von IBM Professional Security Services konzentrieren sich ausschließlich auf die Sicherheit und nutzen erprobte Consulting-Methoden, die auf den bewährten Sicherheitsverfahren des weltweit akzeptierten Standards ISO 17799 basieren. Unsere Sicherheitsexperten verwenden eigene

Tools, neueste Forschungsergebnisse zu Sicherheitsbedrohungen und intelligente Gegenmaßnahmen, um effektive Sicherheitsprogramme zu erstellen, die Geschäftsprozesse schützen und verbessern. Die folgenden Serviceangebote sind verfügbar:

IBM Penetration Testing – erkennt die Schwachstellen in Ihrem Netzwerk und bestimmt deren konkrete Risiken, indem heimliche, feindliche Aktivitäten, die typisch für Angriffe auf das Netzwerk sind, in einer sicheren und kontrollierten Übung demonstriert werden. Der Penetration Testing Service beinhaltet mehr als nur eine typische Analyse oder Netzwerkprüfung. Er gehört zu den branchenweit umfassendsten Tests seiner Art. Unsere kompetenten Berater nutzen ihr Know-how, um Ihr Netzwerk mit den Augen eines potenziellen Hackers zu sehen. Sie stellen Ihnen ausführliche Berichte bereit, die umsetzbare Maßnahmen zur Beseitigung der festgestellten Sicherheitslücken, geordnet nach Priorität, enthalten. Damit können Sie die Sicherheit in Ihrem Unternehmen verbessern.

IBM Application Security Assessment – umfasst eine detaillierte Prüfung und gezielte Codeprüfung Ihrer Anwendungen zur Erkennung von Sicherheitslücken und schützt Anwendungen, in denen geschäftskritische Daten gespeichert sind. Im Rahmen dieses Service erhalten Sie eine

detaillierte Aufstellung solider Empfehlungen zur Verbesserung der Anwendungssicherheit.

IBM Information Security Assessment – überprüft die gesamte Sicherheit in Ihrem Unternehmen. Dies schließt sowohl Sicherheitsrichtlinien, -verfahren, -kontrollen und -mechanismen als auch physische Sicherheit, Netzwerke, Server, Desktops und Datenbanken mit ein. Diese umfassende Analyse ermöglicht Ihnen die Ermittlung von Schwachstellen in Ihrer IT-Infrastruktur und von Lücken bei Kontrollen, Richtlinien und Verfahren. Nach der Analyse erhalten Sie einen Plan zur Verbesserung der gesamten Sicherheit in Ihrem Unternehmen, der auf bewährten Verfahren basiert.

IBM Payment Card Industry Assessment – unterstützt Sie dabei, die Vorgaben des Payment Card Industry (PCI) Data Security Standard einzuhalten. IBM ISS wird vom PCI Security Standards Council als Qualified Security Assessor (QSA) und Approved Scanning Vendor (ASV) anerkannt. Die PCI-Analysen werden von speziell dafür zertifizierten Beratern durchgeführt. Eine Analyse von Zahlungsanwendungen ist ebenfalls verfügbar. Sie wird von

Consultants durchgeführt, die als Qualified Payment Application Security Professionals (QPASPs) zertifiziert sind.

IBM Emergency Response Services – beinhalten Leistungen für die Abwehr von Sicherheitsbedrohungen, die Vorbereitung auf künftige Sicherheitsverstöße und forensische Analysen, die von unseren Sicherheitsexperten durchgeführt werden. Die Services sind sowohl auf Subskriptionsbasis als auch auf Abruf verfügbar. Das Emergency Response-Team reagiert schnell auf Angriffe und erarbeitet gemeinsam mit Ihrem Unternehmen maßgeschneiderte Pläne für Notfallmaßnahmen, mit denen sich die Auswirkungen künftiger Attacken minimieren lassen. Unsere Sicherheitsexperten unterstützen Sie außerdem mit forensischen Analysen beim Auffinden und bei der strafrechtlichen Verfolgung der für Angriffe auf die Informationssicherheit verantwortlichen Täter.

IBM Policy Development – definiert die Strategie und Richtlinien, auf denen wichtige Entscheidungen in Bezug auf Prozesse, Technologien, Management und Administration zum Schutz Ihrer IT-Ressourcen und zur Einhaltung gesetzlicher Bestimmungen basieren.

IBM Network Architecture Design Services – ist ein Serviceangebot, bei dem wir Ihre bestehende Netzwerkarchitektur prüfen und gemein-

sam mit Ihren Mitarbeitern eine detaillierte Sicherheitsarchitektur für den Schutz Ihrer IT-Umgebung entwerfen.

IBM Technology Implementation Planning – bietet Ihnen die Chance, das Potenzial Ihrer Sicherheitstechnologie bestmöglich auszunutzen. Wir erarbeiten einen Plan für die Implementierung von Sicherheitslösungen mit minimaler Beeinträchtigung des Netzwerkbetriebs. Darüber hinaus unterstützt Sie der Service bei der Planung des Managements und der Wartung Ihrer Sicherheitslösung.

IBM Deployment Consulting – trägt dazu bei, den Wert Ihrer Investitionen in IBM ISS-Lösungen zu maximieren. Die IBM ISS-Sicherheitsexperten begleiten Sie bei der Installation, Konfiguration und Optimierung sowie der Migration auf neue ISS-Lösungen.

IBM Staff Augmentation – ergänzt Ihre eigenen Mitarbeiter durch IBM ISS-Sicherheitsexperten. Die IBM ISS-Consultants erweitern Ihr eigenes Team und stellen Ihnen kosteneffizientes Sicherheits-Know-how bereit. Ihre Mitarbeiter können sich so ganz auf die Sicherstellung der regulären Geschäftsabläufe konzentrieren.

IBM Vertical & Regulatory QuickStart Programs – analysieren Abweichungen zwischen der bestehenden und der von branchenspezifischen und gesetzlichen Bestimmungen vorgeschriebenen Sicherheit. Dazu gehören folgende Bestimmungen: Supervisory Control and Data Acquisition (SCADA), Sarbanes-Oxley, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act und Federal Information Security

Management Act (FISMA). Diese Programme stellen Ihnen detaillierte Empfehlungen zur Einhaltung gesetzlicher Bestimmungen und zur Verbesserung der Sicherheit bereit.

IBM Security Awareness Training – unterstützt Sie bei der Schulung Ihrer Mitarbeiter in bewährten Sicherheitsverfahren und -richtlinien über ein Onlineschulungsprogramm. Zusätzlich zum Awareness Training bietet IBM ISS eine Vielzahl weiterer Schulungen an, die an Ihrem eigenen oder einem anderen Standort durchgeführt werden. Damit helfen wir Ihnen dabei, sich größtmöglichen Ertrag aus Ihren Investitionen in IBM ISS-Lösungen zu sichern.

Sicherheitsmanagement in Echtzeit und rund um die Uhr

Nur sehr wenige Unternehmen verfügen über die nötigen Ressourcen, um mit den immer neuen Gefahren aus dem Internet, die ihre Geschäftsabläufe und Gewinne bedrohen, Schritt zu halten. Die Sicherheit eines Unternehmens muss rund um die Uhr gewährleistet sein. Wachsende Anforderungen beim Patch-Management, der Betrieb von Geräten in einer aus unterschiedlichen Komponenten

bestehenden IT-Landschaft und die Umsetzung von Sicherheitsrichtlinien, die sich auf Mitarbeiter, Auftragnehmer und Kunden auswirken können, sind nur einige Herausforderungen, die es zu meistern gilt.

Die IBM Managed Security Services bieten umfangreiche Outsourcing-Lösungen für das Sicherheitsmanagement in Echtzeit, einschließlich Systemüberwachung, Einleitung von Maßnahmen im Notfall und Schutz rund um die Uhr – und das zu einem Bruchteil der Kosten, die normalerweise für eigene Sicherheitsressourcen anfallen. Die folgenden Managed Security Services sind verfügbar:

IBM Managed Protection Services – werden mit einem herausragenden leistungsbasierten Service-Level-Agreement (SLA) angeboten, das die einfache und sichere Übertragung der Verantwortung für den Schutz des Netzwerks an einen verlässlichen Partner erlaubt. Diese Lösungen gehen über die Ereignisüberwachung und das Management von Geräten hinaus. Zum Leistungsumfang der Managed Protection Services gehören

in Echtzeit und rund um die Uhr verfügbare Überwachungs-, Management- und Eskalationsservices für eine Vielzahl verschiedener Plattformen und Betriebssysteme für Netzwerke, Server, Desktops und Wireless-Anwendungen.

IBM Managed and Monitored Firewall Services – sind umfassende, rund um die Uhr verfügbare, kompetent erbrachte Services für Überwachung, Management und Analyse von Firewallprotokollen zur Erkennung, Vermeidung und Abwehr immer neuer Gefahren. Der Service ist in einer Vielzahl verschiedener Optionen erhältlich, sodass Sie vorhandene Investitionen in die Sicherheit maximieren können – zu einem Bruchteil der Kosten einer in Eigenregie betriebenen Lösung.

IBM Managed IDS & IPS Services – schützen Netzwerke und Server vor Angriffen von innerhalb und außerhalb des Netzwerks – mit deutlich geringerem Kostenaufwand als beim Einsatz einer in Eigenregie betriebenen Lösung für die Erkennung und Abwehr unbefugter Zugriffe. Dieses Serviceangebot beinhaltet umfassende, rund um

die Uhr verfügbare Leistungen für Überwachung, Management und Analyse unbefugter Zugriffsversuche. Es erlaubt Abwehr- und Eskalationsmaßnahmen in Echtzeit und bietet Unterstützung bei forensischen Analysen und bei der Wiederherstellung nach Sicherheitsvorfällen.

IBM Security Event and Log Management Services – ermöglichen Unternehmen die Zusammenfassung unterschiedlicher Sicherheitstechnologien in einer nahtlos integrierten Plattform für die Archivierung, Analyse, Korrelation und Verfolgung von Sicherheitstrends und Netzwerkereignissen, während gleichzeitig Abläufe zur Abwehr und Beseitigung von Sicherheitslücken koordiniert werden. Zudem haben Sie die Möglichkeit, Protokolle aus Anwendungen und Betriebssystemen auf vielen unterschiedlichen Geräten über eine gemeinsame

Schnittstelle abzufragen. Dadurch können Sicherheitsanalysen auf einer Vielzahl von Einheiten sehr viel schneller durchgeführt werden. Zudem übernimmt IBM ISS auch die Archivierung dieser Protokolldaten, sodass Abläufe zur Einhaltung gesetzlicher Bestimmungen deutlich verbessert werden.

IBM Vulnerability Management Service – automatisiert die verschiedenen Phasen des Managements von Schwachstellen und sorgt für mehr Transparenz in jedem Bereich potenzieller Risiken. Dieser sofort einsatzbereite Service sorgt durch das Management und die Analyse von Servern, Firewall, Switches und anderen Komponenten in Echtzeit für unterbrechungsfreie Geschäftsabläufe. Er kombiniert außerdem Managed Scanning Services mit kompetentem Workflow- und Vorfallmanagement, um Ihre Netzwerkinfrastruktur vor unbefugten Zugriffen zu schützen, die Ihrem Unternehmen schaden könnten.

IBM ISS X-Force Threat Analysis Service – liefert Ihnen individuell angepasste Informationen über eine Vielzahl verschiedener Bedrohungen, die sich auf die Sicherheit Ihres Netzwerks auswirken könnten. Der Service

kombiniert qualitativ hochwertige Echtzeitdaten über Sicherheitsbedrohungen, die aus dem internationalen Netz der IBM ISS Security Operations Center (SOCs) stammen, mit den Forschungsergebnissen des X-Force-Teams. Er bietet detaillierte und maßgeschneiderte Analysen globaler Internetgefahren.

Überwachung von Sicherheitsoperationen über eine zentralisierte Befehlszentrale

Mit dem IBM ISS Virtual-Security Operations Center (Virtual-SOC) können Sie sämtliche Sicherheitsoperationen, managed oder unmanaged, von IBM ISS oder von anderen Anbietern, anzeigen und verwalten – über das Virtual-SOC-Portal, eine einheitliche webbasierte Konsole. Das Virtual-SOC vereint die Kompetenz von sechs globalen IBM Internet Security Systems SOCs und verschafft Ihnen Zugang zu Folgendem:

- *Sicherheitsforschung des renommierten X-Force-Teams*
- *Überwachung und Management rund um die Uhr*

- *Umfassende IBM ISS Consulting-Services*
- *Trouble-Ticketing, Verfolgung, Alarmierung, Eskalation und Einleitung von Maßnahmen*
- *Berichterstellung, Archivierung und Abruf*
- *Zusammenarbeit in Echtzeit mit den Sicherheitsexperten von IBM ISS*

Warum IBM Internet Security Systems?

Präventive Sicherheit erfordert erstklassige Forschungsarbeit, einen Blick für neue Trends und Techniken bei Sicherheitsbedrohungen und eine optimierte und kostengünstige Plattform für die Bereitstellung innovativer Sicherheitslösungen auf Wissensbasis. IBM ISS verfügt über umfangreiches Know-how, innovative Forschungsmethoden und komplexe Technologien, die für den Schutz Ihres Unternehmens erforderlich sind.

Unsere erfahrenen und zertifizierten Berater, Architekten, Projektleiter und Experten sind dafür gerüstet, Ihrem Unternehmen eine umfassende Plattform präventiver Sicherheitsprodukte und -services anzubieten, die Ihre gesamte IT-Infrastruktur – vom Netzwerk-Gateway bis zum Desktop – schützen.

Weitere Informationen

Wenn Sie mehr über die Produkte und Services von IBM Internet Security Systems erfahren möchten, vereinbaren Sie einen Gesprächstermin mit Ihrem IBM ISS-Ansprechpartner oder besuchen Sie uns unter:

ibm.com/services/de/iss



IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

IBM, das IBM Logo und ibm.com sind eingetragene Marken der IBM Corporation.

Proventia, RealSecure, SiteProtector und X-Force sind Marken der IBM Corporation in den USA und/oder anderen Ländern.

Linux ist eine Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenames können Marken anderer Hersteller sein.

Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern. Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

© Copyright IBM Corporation 2007
Alle Rechte vorbehalten.