Dokumente sicher im Griff

Sicheres Enterprise Rights Management

Foto: pixelio.de

Dokumente in der vernetzten Welt zu verwalten ist eine anspruchsvolle Aufgabe, die von diversen Softwarelösungen bereits gut umgesetzt wird. Kritische Dokumente und Daten dagegen sicher zu verteilen, zu verarbeiten und dabei zu schützen ist eine wesentlich kniffligere Aufgabe.

Vertrauenswürdiges Rechtemanagement ist eine elementare Forderung an die aktuelle Softwareentwicklung, damit Firmengeheimnisse geschützt weitergegeben werden und hochsichere Dokumente nicht auf einem Flurdrucker liegenbleiben und damit für jeden zugänglich werden. Die Trusted Computing Idee hilft in Verbindung mit einer Sicherheitsarchitektur Lösungen für diese Anforderungen zu schaffen.

Wissen schützen

In der heutigen vernetzten Wissensgesellschaft richtet sich der Sicherheitsanspruch vor allem an digitale Systeme, die kritische Daten verarbeiten. Die zu schützenden Daten sind vielfältig: Es handelt sich um Firmengeheimnisse, die zur Weiterverarbeitung an Mitentwickler verteilt werden müssen, wie in der Prototypenentwicklung der Automobilindustrie, oder auch um Auftragsangebote die verdeckt abgegeben werden. Es soll verhindert werden, dass Angebotsinhalte bei der Abgabe abgefangen und durch Spionage dem Konkurrenten zugänglich gemacht werden, wie beispielsweise im Fall TGV gegen ICE in Nordkorea 1993, wo TGV das Angebot des ICE-Konsortiums kannte und daher überbieten konnte. Die unlautere Verbreitung von Daten muss ebenfalls

unterbunden werden. Besonders bei Geschäftsmodellen, die sich auf den Handel mit Wissen beziehen. Die SAP AG verteilt beispielsweise Schulungsunterlagen an autorisierte (zahlende) Kunden.

In allen Fällen führt der Verlust der kritischen Informationen zu einem wirtschaftlichen Verlust oder Nachteil. Der Schutz von Wissen und Eigentum ist demnach die für den wirtschaftlichen Erfolg eines Unternehmens zentrale Komponente.

Heutige Systeme bieten für diese Anforderungen nicht die entscheidende Sicherheit. Auf zwei Ebenen muss hier eine Sicherheit gewährleistet werden, die mit herkömmlichen Systemen nicht zu erreichen ist.

Einerseits ist die Sicherheit von Betriebssystemen nicht ausreichend. Aktuelle Betriebssysteme, wie Windows und Linux, haben einen hybriden, beziehungsweise einen monolithischen Aufbau. Die negativen Folgen dieser Strukturen sind eine nicht strenge Speicherisolation und die Allmächtigkeit dieser Systeme. Ist ein Betriebssystem durch Malware kompromittiert worden, kann diese die Kontrolle über das gesamte System erlangen und erhält somit auch Zugriff auf sicherheitsrelevante Informationen und Dienste. Die Zahl der Angriffe auf Computersysteme durch Viren und Trojanische Pferde nimmt stetig zu. Angreifer durchbrechen die vorhandenen Sicherheitsmechanismen der Software- und Betriebssysteme, wie Virenscanner und Firewalls, und bisher standen keine effektiveren Maßnahmen zur Verfügung, die dieser Problematik entgegenwirken könnten. Somit sind alle Dokumente oder Identitätsdaten der betroffenen Anwender in Gefahr. Um sensible Daten vor unrechtmäßigen Zugriffen zu schützen, ist eine geräte- und netzübergreifende Vertrauens- und Sicherheitsbasis für die Zukunft unabdingbar. Mit herkömmlichen Rechnersystemen ist eine solche Basis jedoch nicht erreichbar, wie durch die Vielzahl an Sicherheits-Patches eindrucksvoll unterstrichen wird.

Auf der anderen Seite muss die Netzwerkkommunikation über das unsichere Medium Internet kontrollierbar und sicher sein. Dazu gehört nicht nur die Sicherheit auf dem Übertragungsweg. Vielmehr ist der Anspruch zu stellen, dass eine Sicherheit über den Kommunikationspartner herrscht. Das System mit dem kommuniziert wird, soll das „richtige“ System in einem vertrauenswürdigen Zustand mit dem „richtigen“ Anwender sein. Es ist heute nicht mehr ausreichend nur den Anwender am anderen Ende der Leitung zu kennen. Es ist wichtig den Zustand des Systems überprüfen zu können. Zusätzlich sollen Regeln, die an Dokumente gebunden sind, auf den entfernten Systemen durchgesetzt werden. Dies geschieht bestenfalls ohne dass der Geräteinhaber die Kontrolle über das eigene System verliert.

Die Anforderungen die bis zu diesem Punkt gestellt sind können durch reine Softwaresicherheit nicht mehr geleistet werden. Die Trusted Computing Technologie bietet den Einsatz von Hardwaresicherheit und die Möglichkeit ein System auf seine Vertrauenswürdigkeit zu überprüfen. Neue Betriebssystemarchitekturen – umgesetzt als Sicherheitskern – ermöglichen die strenge Isolation von Speicherbereichen und die vertrauenswürdige Durchsetzung von Rechten und Regeln. Außerdem können sichere und unsichere Bereiche parallel existieren.

Das Forschungsprojekt EMSCB (European Multilaterally Secure Computing Base) stellt mit Turaya eine Sicherheitsplattform zur Verfügung, die genau die geforderten Eigenschaften mitbringt und die Trusted Computing Technologie unterstützt. Turaya wird in einem Konsortium bestehend aus dem Institut für Internet-Sicherheit der FH Gelsenkirchen, der Ruhr-Universität Bochum, der TU Dresden und den Firmen Sirrix AG und escrypt GmbH entwickelt. Das Bundesministerium für Wirtschaft und Technologie fördert das Projekt und namhafte Industriepartner, wie die SAP AG und Bosch/Blaupunkt, unterstützen die insgesamt fünf Piloten. Im aktuellen Meilenstein Turaya.ERM wird zusammen mit dem Projektpartner SAP AG gezeigt, dass ein lauffähiges Enterprise Rights Management (ERM)- System realisierbar ist, das die geforderte Sicherheit und Vertrauenswürdigkeit erreicht. Ziel ist es mit Turaya eine Sicherheitsplattform mit offener Architektur und offenen Schnittstellen zu schaffen, die als Basis für vertrauenswürdige IT-Systeme dient.

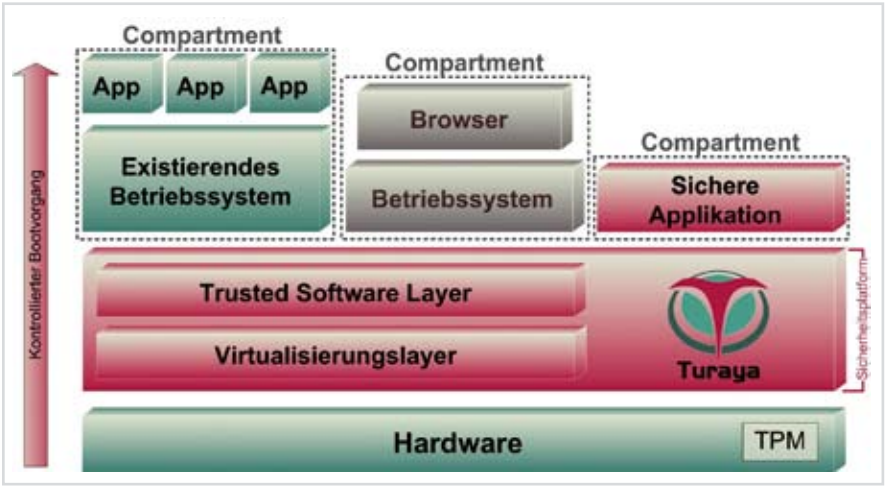

Bild 1: Diese Architektur ermöglicht strikte Isolation von Speicherbereichen.

Trusted Computing

Das Ziel von Trusted Computing ist die Erhöhung von Sicherheit und Vertrauen in IT-Systeme mit offenen Spezifikationen. Ein Industriekonsortium, die Trusted Computing Group (TCG), setzt sich aus über 160 namhafte Firmen zusammen, zu denen SUN, Intel, AMD, Microsoft, HP und IBM genauso gehören, wie die deutschen Hersteller Infineon, Utimaco und die Sirrix AG.

Die Hauptidee besteht darin, manipulationsgeschützte Sicherheitskomponenten in die Hardware zu integrieren. Sie sollen als vertrauenswürdige „Anker" für die Sicherheit sowohl die Integrität als auch die Authentizität des Rechnersystems garantieren und Software-basierten Angriffen entgegen wirken. Eine solche Sicherheitskomponente ist das „Trusted Platform Modul" (TPM).

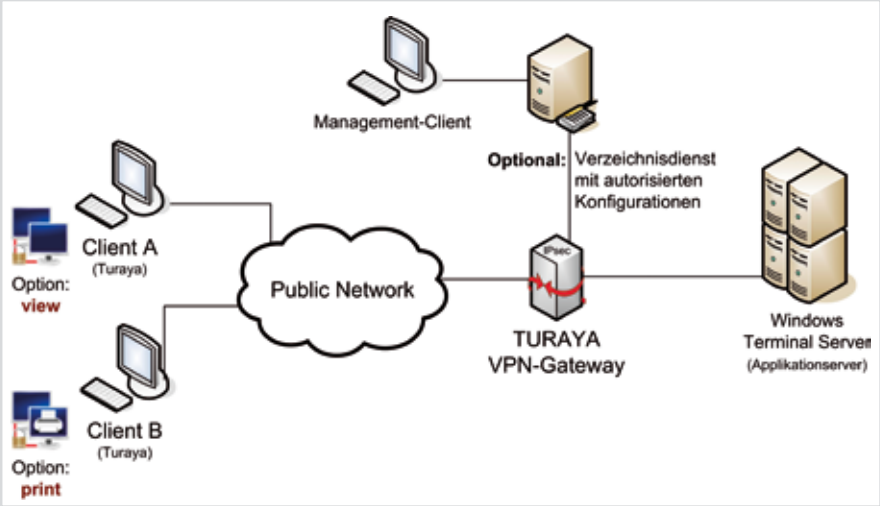

Bild 2: Über einen VPN Server wird bei vertrauenswürdiger Konfiguration ein Windows Terminal Server erreicht.

TPM

Das Trusted Platform Module ist ein kleiner passiver Chip, der fest mit der Systemplattform verbunden ist. Die Architektur des TPMs ähnelt der einer SmartCard. Der Chip beinhaltet einen Crypto-Coprozessor, einen Zufallszahlengenerator und das „Platform Configuration Register" (PCR), in dem die Hashwerte von Konfigurationszuständen gespeichert werden. Beim Bootvorgang (Secure Boot) eines Systems ermittelt man diese Hashwerte, die zur Erkennung von Änderungen an der Soft- oder Hardware-Konfiguration dienen. Ein Angriff oder ein anderer Einfluss verändert die Systemkonfiguration. Die Messwerte entsprechen dann eventuell nicht mehr den Vorgaben und sind nicht mehr als vertrauenswürdig einzustufen. Diese Information wird abgefragt und als Reaktion kann beispielsweise der Bootvorgang abgebrochen werden. So wird eine Aussage über die Vertrauenswürdigkeit eines Rechnersystems möglich.

Die Trusted Computing Funktion „Sealing" ermöglicht es außerdem Daten an eine Systemkonfiguration zu binden. Dieser Vorgang wird dem Anliegen von Anwendern gerecht, die eigenen Dokumente vor fremdem Zugriff zu schützen. Zusätzlich können Dokumente an ein anderes Rechnersystem übergeben werden, mit der Gewissheit dass nur das autorisierte entfernte Rechnersystem einen Dokumentenzugriff durchführen kann. Dieser Vorgang wird „Binding" genannt. Im Rahmen von ERM kann ein schützenswertes Dokument mit dem Hashwert einer vertrauenswürdigen Systemkonfiguration zu einem Datenpaket verbunden werden. So wird die vertrauensvolle Verarbeitung auf dem für das Datenpaket bestimmtem Rechnersystem garantiert.

Die Darstellung eines Systemzustands nach außen wird „Attestation" genannt. Die „remote-Attestation" stellt die Vertrauenswürdigkeit „entfernter" Rechnersysteme fest. Da die TPMs mit ihren Schlüsseln Einzigartigkeit gewährleisten, ist ein Rechnersystem mit Bezug auf seinen Integritätszustand eindeutig identifizierbar. Bei der Attestation wird nur ein Rechnersystem, das einen vertrauenswürdigen Zustand vorweist, als vertrauenswürdig eingestuft und in der Folge entsprechend wird eine Kommunikation zugelassen oder abgelehnt.

Sicherheitsarchitekturen

Die Trusted Computing Funktionen sind nicht eigenständig nutzbar. Eine Software muss die Funktionen steuern. Aktuelle Betriebssysteme können die genannten Funktionen aufgrund ihrer sicherheitskritischen Struktur wie bereits erläutert nicht vertrauensvoll anbieten. Eine Sicherheitsarchitektur macht jedoch sowohl die vertrauenswürdige Verarbeitung, als auch den Einsatz herkömmlicher Betriebssysteme möglich. Diese Architektur verfolgt einen Mikrokern-Ansatz mit strenger Isolation. Ein sehr klein gehaltener Sicherheitskern dient als Basis. Auf diesem Kern können virtualisiert und parallel komplette Betriebssysteme sowie einzelne Anwendungen in sogenannten Compartments betrieben werden. Bild 1 zeigt den architektonischen Aufbau.

Compartments

Die Compartments sind streng voneinander isoliert und können nur wenn eine entsprechende Berechtigung vorliegt über Interprozesskommunikation (IPC) miteinander interagieren. Alle sicherheitskritischen Vorgänge können vom un-

sicheren Betriebssystem gekapselt werden. Der Mikrokern-Ansatz minimiert durch die geringe Menge an Codezeilen die Fehleranfälligkeit und somit die Wahrscheinlichkeit, dass Sicherheitslücken entstehen.

Der entscheidende Punkt für ein Dokumentenmanagement ist, dass der Sicherheitskern vertrauenswürdig die Verwaltung der Ressourcen übernimmt und damit in der Lage ist Berechtigungen (Policies) zu bearbeiten und durchzusetzen. Er kann einem Compartment beispielsweise einen Zugang zur Netzwerkkarte erlauben oder verbieten, oder ein Dokument nur einem gemessenen und vertrauenswürdigen Compartment zur Verfügung stellen, aber dem herkömmlichen Betriebssystem den Zugang zum Dokument verwehren. Der Sicherheitskern ist vertrauenswürdig, da er beim Bootvorgang mitgemessen wird und damit überprüfbar ist. Es können beliebige Compartments in die Messung mit aufgenommen werden. Anhand des vierten Piloten des EMSCB Forschungsprojekts werden die ERM-Funktionalität und die Vorteile erläutert.

Enterprise Rights Management (ERM)

Laut Definition sorgt ERM dafür, dass geschäftskritische Informationen nur nach vorgegebenen Regeln von den definierten Akteuren auf definierten Rechnersystemen eingesehen oder bearbeitet werden können. Daten wie Dokumente erhalten durch ERM eine mögliche Einschränkung in ihrer Verwendung. So kann beispielsweise das Ausdrucken oder das Weiterversenden von Daten reglementiert werden.

Die Sicherheitsplattform Turaya zeigt mit dem vierten Piloten Turaya.ERM zusammen mit dem Projektpartner SAP, dass es möglich ist Dokumente vertrauensvoll zu reglementieren. Im SAP-Umfeld gehört die Ausgabe von Schulungsunterlagen für die unterschiedlichen Anwendungen, die im Firmenportfolio enthalten sind, zum Geschäftsmodell. Diese Unterlagen sind schützenswerte Daten. Ein Zugangsschutz mit Benutzername und Passwort ermöglicht eine anwenderabhängige Zugangskontrolle. Diese Daten sind jedoch schnell weitergegeben und somit erhalten auch nicht autorisierte Anwender Zugang zum System. Die Dokumente könnten auch ausgedruckt, kopiert und in Papierform verteilt werden. Um wirtschaftlichen Schaden abzuwenden, muss der Umgang mit den Dokumenten nach entsprechenden Berechtigungen ablaufen. Anforderung ist, dass ein Benutzer sich nur mit einem bestimmten Rechnersystem authentifizieren kann und keine Möglichkeit erhält die Dokumente über eine Schnittstelle weiterzugeben. Es gibt für dieses Szenario bereits reine Online-Lösungen, aber eine Offlineverarbeitung benötigt ein System, wie Turaya.ERM.

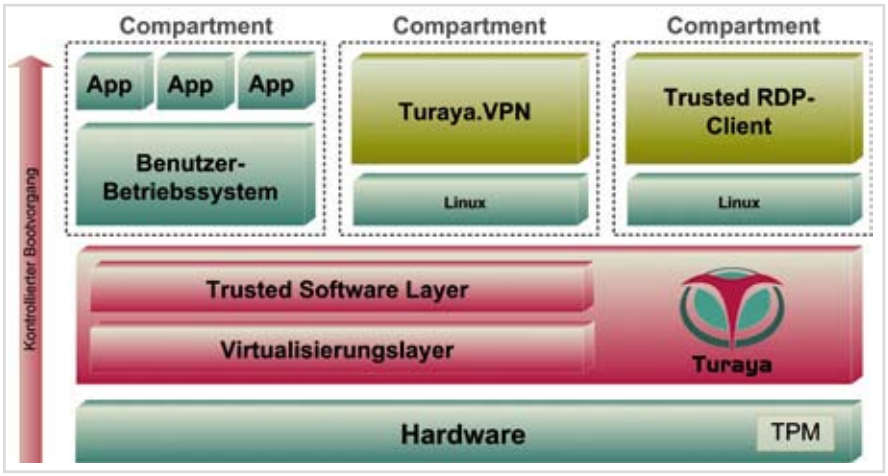

Bild 3: Die Kontrolle über die Ressourcen ermöglicht die Durchsetzung von Regeln.

Schlüssel und Daten

Im Beispiel Turaya.ERM baut der Anwender eine Verbindung zu einem entfernten Terminal-Server auf, um Dokumente zu bearbeitet. Im ersten Schritt benötigt Turaya einen Schlüssel für den Aufbau eines VPN-Tunnels zur sicheren Übertragung und Verbindung (siehe Bild 2). Der Schlüssel ist an die Plattform „gesealt". Er kann nur entschlüsselt und verwendet werden, wenn das Rechnersystem mit der korrekten Konfiguration gestartet wurde. Damit ist das System als vertrauenswürdig einzustufen. Der Schlüssel gelangt aber niemals in das herkömmliche unsichere Betriebssystem, sondern steht nur dem Compartment zur Verfügung, das die sichere VPN-Verbindung initiiert (siehe Bild 3). Durch das etablierte VPN kann jetzt eine Verbindung zu dem Windows Terminal Server (WTS) aufgebaut werden und eine Anmeldung erfolgen. Wenn ein Dokument auf dem Terminal-Server gedruckt wird, wird es an den lokalen Drucker weitergeleitet, sofern die Berechtigung dazu vorliegt. Neben dem VPN-Schlüssel wurde auch eine Berechtigung (Option) für den Anwender im Bezug auf die Verbindung zum WTS übergeben, die beispielsweise das Drucken verbietet. Der Sicherheitskern verarbeitet diese Anweisung und trennt das Compartment, das mit dem Terminal-Server verbunden ist (siehe Bild 3:Trusted RDP-Client) vom Zugriff auf den Drucker. Es können weitere Berechtigungen an Schlüssel und Daten gebunden werden die beispielsweise das Drucken erlauben oder das Weiterleiten von Daten unterbinden. In Bild 2 haben zwei Clients einen Zugriff auf den WTS. Beide befinden sich in ei-

nem vertrauenswürdigen Zustand. Client A besitzt die Option „View“. Dies berechtigt ihn lediglich zum Ansehen von Dokumenten. Client B besitzt die Option “Print“ und hat damit das Recht auch Dokumente zu drucken. Turaya etabliert also eine Verbindung zwischen dem WTS, beziehungsweise dem Trusted RDP-Client-Compartment und dem lokalen Drucker.

Die gestellten Anforderungen an ein ERM-System sind damit erfüllt. Nur ein vorher definiertes und als vertrauenswürdig eingestuftes Rechnersystem erhält Zugang zu einem Dokumentenmanagementsystem, das in diesem Beispiel durch den WTS dargestellt wird. Außerdem können Berechtigungen (Optionen/Policies) an Dokumente und Applikationen gebunden werden. Festgelegte Berechtigungen zu dem jeweiligen Vorgang werden vertrauensvoll durchgesetzt und können nur äußerst schwer manipuliert werden. Alle sicherheitskritischen Informationen, wie Schlüssel und Zugangsdaten sind vor dem unsicheren Benutzerbetriebssystem durch Isolation geschützt. Die Weitergabe von Zugangsdaten oder Schlüsseln ist zwecklos, da diese Informationen nur mit dem autorisierten Rechnersystem entschlüsselt werden können.

Fazit

Mit einer Sicherheitsplattform wie Turaya und der Unterstützung durch Trusted Computing können Dokumente vertrauenswürdig geschützt werden. Diese Technologien ermöglichen Lösungen für Firmen wie SAP oder beispielsweise für die Autoindustrie im Rahmen von Plagiatsvermeidung und Schutz von Firmengeheimnissen. Die grundlegenden Konzepte sind die Isolation von Anwendungen, die Überprüfbarkeit der Hard- und Software auf Vertrauenswürdigkeit und die Minimalisierung des Sicherheitskerns zur Vermeidung von Sicherheitslücken. Turaya ist in diesem Forschungsgebiet weltweit eine führende Entwicklung und kann von der deutschen Industrie genutzt werden, um Produkte dafür zu entwickeln. Die Sicherheitsplattform ist Open Source und plattformunabhängig konzipiert und bietet somit einen weiten Rahmen von Einsatzmöglichkeiten beispielsweise auch im Embedded-Bereich.

Die weiteren Piloten, Informationen und den Source Code von Turaya finden sie auf www.emscb.de. Weitere Informationen zu Trusted Computing erhalten sie unter www.trustedcomputinggroup.org

Dipl.-Ing. Niklas Heibel
Dipl.-Inform. Markus Linnemann
Prof. Dr. Norbert Pohlmann

Impressum

Chefredakteur:
Ulrich Parthier

Redaktion:
Carina Pradler

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH
Rudolf-diesel-Ring 32, D - 82054 Sauerlach
Tel.: +49 8104 6494-0
Fax: +49 8104 6494-22
www.it-verlag.de

Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949:
100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Alle Autoren erreichen Sie über die Redaktion.
Wir reichen Ihre Anfragen gerne an die Autoren weiter.
Manuskripteinsendungen: Für eingesandte Manuskripte wird keine Hhaftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung: Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programmteilen führen, übernimmt der Verlag keine Haftung. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

Druck:
gebr. Geiselberger Druck
www.geiselberger.de

Objektleitung:
Ulrich Parthier (-14)

Erscheinungsweise: zweimonatlich

Verkaufspreis:
Einzelheft € 20,– (Inland)
Jahresabonnement € 100,– (Inland) bzw. € 110,– (Österreich, Schweiz) bei Zustellung per Normalpost.

Bankverbindung:
VRB München Land eG,
BLZ 701 664 86, Kontonummer 25-23752

Abonnementservice:
Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Bezugsgelder.

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 7
gültig ab Januar 2007

Anzeigenverkauf:
Deutschland:
Nicola Heidrich
Rudolf-Diesel-Ring 32
82045 Sauerlach
Tel.: +49 8104 6494-17
Fax: +49 8104 6494-22
Mobil: +49 1788885691
E-Mail: heidrich@it-verlag.de

USA:
Global Ad-Net
Mr. Ed Ware
80 Elm Street, Suite #2, Peterborough, NH 03458
Phone: 603-924-1040
Fax: 603-924-1041
E-Mail: ed@globalad-net.com

United Kingdom:
GCA Greg Corbett Associates Ltd.
International Media Sales,
Ms Ceri Thacker
5 Lower Belgrave Street, London SW1W ONR
Phone: 044 2077306033
Fax: 044 2077306628
E-Mail: gca@gca-international.co.uk