

# Total Remote Management over IP: Kann der Administrator vor Ort wirklich ersetzt werden?

Dr. Christian Pätz  
Peppercon AG  
paetz@peppercon.com

## Zusammenfassung

*Nicht zuletzt bedingt durch die Diskussion über Total Cost of Ownership (TCO) wird dem Remote Management von IT-Geräten eine immer größere Bedeutung beigemessen. Während Remote Management Technologien in der Welt der großen Server schon von Beginn an integraler Systembestandteil waren, eröffnen eine Anzahl von Technologien nunmehr auch dem Rest der IT-Welt die Möglichkeiten des Remote Managements.*

*Dieser Beitrag versucht, einen Überblick über gegenwärtige Markttrends im Bereich von Remote Management Technologien und eine Ordnung der verschiedenen technologischen Ansätze zu geben.*

## 1 Einführung

System- oder Remotemanagement ist ein unscharf definierter Begriff. Er umfasst Architekturen, Protokolle, unterschiedlichste Programme, Prozesse und Szenarios, welche Wege und Möglichkeiten beschreiben, IT-Systeme aller Art optimal zu betreiben. Leistungskriterien sind zum einen eine hohe Verfügbarkeit der Systeme, zum anderen möglichst geringe Kosten. Die optimale Ausnutzung der vorhandenen Ressourcen an Personal, Hardware, Infrastruktur und Software steht dabei im Vordergrund der Bemühungen.

Die dezentrale und zugleich noch typischerweise heterogene Architektur heutiger IT-Lösungen erzwingt wiederum unter Kostenaspekten die Möglichkeit, IT-Systeme aus der Ferne über geeignete Netze managen und steuern zu können. In diesen Kontext fallen tägliche Administrationsarbeiten wie das Installieren von neuer Software oder das Hinzufügen neuer Nutzer ebenso wie das schnelle Reagieren bei Problemfällen.

Dieser Beitrag stellt *Remote Management Technologien* vor, die eine Kontrolle von Rechnern mittels IP basierter Netze ermöglichen und damit einen

weltweiten Zugriff realisieren. Konzentriert wird sich auf Zugriffstechnologien, die *alle* Funktionen eines Rechners entfernt anbieten und mit deren Hilfe dann problemorientierte Protokolle und Funktionen angewendet werden können, um die eigentliche Aufgabe zu lösen. Die Tatsache, dass dieses eine Herausforderung darstellt, wird deutlich, wenn man sich vorstellt, dass zur erfolgreichen Administration eben auch das Installieren eines neuen Betriebssystems, das Aus- und Einschalten von Systemen, das Verstellen von Bootcode- oder BIOS-Optionen oder auch das Umkonfigurieren von Routern gehört.

Um verschiedene Technologien und Begriffe richtig einordnen zu können, werden im zweiten Abschnitt einige klassifizierende Kriterien für die Beurteilung von Technologien benannt und ihre Bedeutung erläutert.

In den folgenden Abschnitten werden diese Kriterien auf heute verfügbare Technologien angewendet. Die Eignung verschiedener Techniken unter unterschiedlichen Randbedingungen wird herausgearbeitet. Gleichzeitig werden die technologischen Herausforderungen der jeweiligen Technologie aufgezeigt.

## 2 Bewertungskriterien

Um eine Vergleichbarkeit der verschiedenen Klassen zu ermöglichen, müssen Kriterien aufgestellt werden, die Rückschlüsse auf die Einsetzbarkeit und Leistungsfähigkeit der vorgestellten Technologien erlauben.

### **Unabhängigkeit vom Betriebssystem und Rechnerarchitektur:**

Heutige IT-Umgebungen sind in mehreren Betrachtungsweisen als heterogen anzusehen. Dies trifft sowohl die Kernfunktionalität des Rechners (Server, Universalrechner, IP-Router, ISDN Access-Router,...) zu als auch auf die zugrundeliegende Rech-

nerarchitektur, die verwendeten Betriebssysteme und nicht zuletzt auf die Hersteller dieser Geräte zu. Eine Remote Management-Technologie sollte hier ein Maximum an Freiheitsgraden besitzen, um in einem möglichst grossen Kontext einsetzbar zu sein. Detailliert lauten die Forderungen daher:

- Unabhängigkeit vom Betriebssystem; Im Falle eines defekten oder gar nicht vorhandenen Betriebssystems ist Remote Management zu gewährleisten.
- Unabhängigkeit von der Rechnerarchitektur; Heutige fernzusteuerte Rechner beruhen in der überwältigenden Mehrheit auf den Architekturen Intel-PC, Sun Sparc, Motorola/IBM Power PC. Eine Managebarkeit aller drei Architekturen ist daher sehr hilfreich.
- Unabhängigkeit von Herstellern; Eine Remote Management Lösung, welche auf proprietären Systemerweiterungen der Hersteller beruht, ist in der heutigen Zeit der offenen Standards nicht mehr akzeptabel.

#### **Unabhängigkeit vom Systemzustand des Rechners:**

Eine Abhängigkeit vom Systemzustand schränkt die Managebarkeit es entfernten Rechners ein. Eine solche Abhängigkeit entsteht regelmässig durch die Abhängigkeit vom Betriebssystem. Unabhängigkeit vom Betriebssystem ist eine notwendige, leider jedoch keine hinreichende Voraussetzung zur Erfüllung dieses Kriteriums.

#### **Sicherheit:**

Das Ziel von Remote Management ist es, weltweiten Zugriff auf ein Gerät zu ermöglichen. Dies bedeutet auch, dass ein Gerät mit seinen essentiellen und am meisten angreifbaren Schnittstellen global verfügbar wird. Damit ist klar, dass Sicherheitskonzepten einer Remote Management Lösung eine große Aufmerksamkeit gewidmet werden muss. Verschlüsselung, Authentifizierung und Zugriffskontrolle sind die gebräuchlichsten Technologien, die dafür benutzt werden.

#### **Management Software:**

Management Software dient der Bedienung des Management Systems. Ihre Funktionalität bestimmt in entscheidendem Maße die Funktionalität der Gesamtlösung. Es sind zwei Konzepte verbreitet:

1. Das Management System benutzt ein proprietäres Protokoll. Dies erfordert den Einsatz spezieller Software.
2. Das Management System benutzt ein Standardprotokoll, z.B. SNMP, so dass eine beliebige, standardkonforme Software genutzt werden kann.

Eine Lösung, die zwischen diesen beiden Ansätzen liegt, ist z.B. die Benutzung von *HTTP* oder *Telnet* als Kommunikationsprotokoll. Diese Protokolle sind standardisiert, es kann also eine Standardsoftware wie z.B. ein *Web-Browser* benutzt werden. Allerdings unterstützen sie nicht die Definition und den Austausch von Meta-Informationen, womit die Funktionalität der Lösungen beschrieben werden könnte. Das heißt, die eigentlichen Nutzerschnittstellen sind wiederum proprietär.

#### **Verbreitung**

Die Verbreitung einer Lösung gibt einen Hinweis darauf, wie praxisrelevant oder wie erprobt sie tatsächlich ist.

## **3 Technologien, Systeme und Initiativen**

Im folgenden werden einige Systeme genauer betrachtet.

### **3.1 IPMI**

IPMI<sup>1</sup> [6] ist eine Initiative von namhaften PC Herstellern. IPMI definiert ein low-level Interface, welches es ermöglicht, das physische Funktionieren eines Hostsystems zu überwachen. Darunter fallen verschiedene Parameter wie Temperaturen, Spannungen, CPU-Lüfterdrehzahl, Netzteile, Event-Log Einträge u.a. Zusätzlich beinhaltet IPMI Mechanismen für die Benachrichtigung in kritischen Systemzuständen, automatischen Restart, entferntes Ein- und Ausschalten sowie Reset.

IPMI in der Version 1.0 kann heute bei Serversystemen als Standard betrachtet werden. Sowohl die grossen Markenhersteller als auch Produzenten von Mainboards bieten eine derartige Schnittstelle an. Die Schnittstelle ist als IPMB serieller Zweidrahtbus nach der Spezifikation I2C verfügbar.

<sup>1</sup>Intelligent Plattform Management Interface

IPMI wird ab Version 1.5 über einen sogenannten BMC<sup>2</sup> auf dem Mainboard des Hostsystems implementiert. Wichtigstes Merkmal des BMC ist seine vom Mainboard unabhängige Stromversorgung. Damit ist sichergestellt, dass der BMC auch bei ausgeschaltetem System selbst noch ansprechbar und damit aktionsfähig bleibt. Der BMC implementiert auch den Zugriff zu BIOS-Einstellungen, welcher beim PC traditionell nur über die VGA-Console möglich war.

Gerade bei PC Systemen ist IPMI damit eine sehr interessante Initiative, welche den einheitlichen Zugriff auf Basis-PC-Funktionen ermöglicht, die bislang nur mit größerem technischen Aufwand gegeben war.

Leider ist eine größere Verfügbarkeit von Systemen mit IPMI V1.5 bisher nicht gegeben und ein eigentlich naheliegendes Produkt einer Schnittstellenkarte für IPMI über den IPMB Bus bisher von Marktteilnehmern nur angekündigt.

OS unabhängig	ja
Architektur-unabhängig	ja
Herstellerunabhängig	ja
Systemzustands-unabhängig	ja
Sicherheit	Authentifizierung
Clientsoftware	proprietär
Verbreitung	meist in Intel Servern

### 3.2 SNMP

SNMP<sup>3</sup>[5] ist ein Protokoll, dass zum Austausch von Management Informationen genutzt wird. Es ist einer der verbreitetsten de-facto Standards auf diesem Gebiet.

Die SNMP Spezifikation ist mittlerweile in der Version 3 verfügbar und besteht aus Definitionen zu folgenden Punkten:

- Einer formalen Sprache zur Datendefinition (ASN.1<sup>4</sup>)
- Den Definitionen von Management Informationen (MIB<sup>5</sup>)
- Der Protokoll Definition
- Den Sicherheits- und Administrations Definitionen

<sup>2</sup>Baseboard Management Controller

<sup>3</sup>Simple Network Management Protokoll

<sup>4</sup>Abstract Syntax Notation

<sup>5</sup>Management Information Base

SNMP definiert eine verteilte Managementarchitektur mit Managern und Agenten. Ein Manager kann Daten von Agenten nach dem Client-Server-Modell abfragen, auswerten und ändern. Ein Agent kann auch von sich aus Daten an einen Manager mittels eines sogenannten *Traps* senden. Das Modell lässt sich zudem mit Hilfe einer formalen Sprache sehr flexibel erweitern. Damit besticht SNMP durch seine Universalität und Einfachheit zugleich. Die Hersteller von Netzwerkkomponenten setzen uneingeschränkt auf SNMP zum Kontrollieren ihrer Produkte. Ebenso haben viele der hier erwähnten Remote Management Systeme ein SNMP Interface. Einer der wesentlichen Nachteile ist der, dass die sichere Version 3 bislang wenig verbreitet ist.

OS unabhängig	ja
Architektur-unabhängig	ja
Herstellerunabhängig	ja
Systemzustands-unabhängig	ja
Sicherheit	bis v2 nur einfache Authorisierung, ab v3 Authentifizierung, Verschlüsselung
Clientsoftware	jeder SNMP-fähige Software
Verbreitung	sehr große Verbreitung in Netzwerktechnik und Netzwerkmanagement

### 3.3 Remote Access Software

Um mit einer Remote Access Software einen Rechner fernzusteuern, müssen eine Reihe von Voraussetzungen erfüllt sein.

- Die Serverapplikation auf dem entfernten System muss korrekt arbeiten.
- Das darunterliegende Betriebssystem arbeitet stabil.
- Es wird keine Diagnosemeldung angezeigt (Blue Screen)
- Die Kommunikationsressource (Ethernetkarte, ISDN) wird nicht von einer anderen Applikation auf dem entfernten Rechner exklusiv genutzt.

Diese Voraussetzung lassen Remote Access Software nur für tägliche Administrationsaufgaben geeignet

erscheinen. Fehlerbehebung auf Systemebene ist damit ausgeschlossen.

Da die meisten Probleme heutiger IT-Technik jedoch auf Applikationsebene geschehen, ist der Einsatz dieser Softwarelösungen durchaus sinnvoll.

Ein Beispiel für Remote Access Software ist z.B. die freie Software VNC[7], welche für alle wesentlichen Systeme und Architekturen sowohl Server als auch Client Versionen bereitstellt. In modernen Betriebssystemen wie Linux (X11) oder WindowsXP (RDP) sind Fernsteuersoftwarepakete daher sogar integraler Bestandteil. Kommerzielle Lösungen kosten 100...300 EUR pro Rechner.

Speziell im Übertragen von graphischen Bildschirmhalten lassen Softwarelösungen ihre später zu beschreibenden Hardwarekollegen weit zurück, da sie auf wesentlich mehr und präzisere Informationen für die effiziente Bildkodierung zurückgreifen können. Gepaart mit günstigen Kosten ist das Preis-Leistungsverhältnis von Softwarelösungen meist ungeschlagen. Beim Ausfall des Betriebssystems ist eine reine Softwarelösung jedoch machtlos.

OS unabhängig	nein
Architektur-unabhängig	nein
Herstellerunabhängig	ja
Systemzustands-unabhängig	nein
Sicherheit	Authentifizierung, A uthentifizierung und Verschlüsselung
Clientsoftware	meist Windowsclients
Verbreitung	stark, auch durch GPL Software wie vnc
Preis	100 ... 350 EUR

### 3.4 Remote Management Boards

Remote Management Boards [8] sind PCI-Einsteckkarten und werden hauptsächlich für PC-Systeme hergestellt. Sie rüsten einen Host ebenso wie IPMI mit erweiterten und betriebssystemunabhängigen Schnittstellen aus, die einen Zugriff auf den PC aus der Ferne gestatten. Ihr Ziel ist, einem Administrator aus der Ferne mindestens die Funktionalität zur Verfügung zu stellen, die er bei einer Arbeit direkt vor Ort hätte. Dies sind insbesondere

- Der durchgängige und betriebssystem- sowie betriebssystemzustandsunabhängige Zugriff auf die

Console, d.h. auf Bildschirm, Tastatur und gegebenenfalls Maus.

- Das Auslösen eines Kaltstartes mittels System-Resets.
- Das Einschalten und Ausschalten des Systems.
- Temporäres Aktivieren eines externen Speichermediums, u.a. zum
  - Nachladen von Betriebssystembestandteilen.
  - Ausführen von Test und Analysesoftware, die nicht auf den Plattenspeichern des Systems verfügbar sind.
  - Starten eines Notfall-oder Backupbetriebssystems von einer Floppy Disk oder CD-ROM

Durch ihre tiefe Integration in das Zielsystem können Remote Management Boards je nach der Architektur des entfernten Systems weitere Informationen über den Systemzustand ermitteln. Sie bedienen sich hier meist der IPMI Schnittstelle der Mainboards.

Remote Management Boards verfügen über alternative Stromversorgungswege oder eine Batteriepufferung. Nur so ist ein unabhängiger Zugriff bei jedem Systemzustand sichergestellt. Kommunikationsschnittstellen sind heute neben Ethernet auch analoge Modems oder sogar ISDN on board.

Remote Management Boards sind in allen bekannten Fällen als autonome Rechner implementiert und damit selbst komplexe embedded Rechner. Die meisten Funktionalitäten eines solchen Boards lassen sich auch mit anderen Mitteln erreichen aber bei weiten nicht mit dieser Einfachheit. Remote Management Boards überzeugen also durch ihre *Easiness of Use*. Von allen in diesem Artikel vorgestellten Systemen implementieren sie den komplettesten und "natürlichsten" entfernten Rechnerzugriff mittels einer einfachen *Plug 'n Play* Lösung. Das begründet auch ihre Beliebtheit für das Management von PC-Systemen. Voraussetzung für das erfolgreiche Arbeiten von Remote Management Boards sind detaillierte Kenntnisse der Systemarchitektur. Um hier flexibel zu sein, basieren Remote Management Boards daher in der Regel auf standardisierten Schnittstellen wie USB oder PCI.

Die technische Herausforderung bei Remote Management Boards ist die Übertragung des Bildschirmsignals. Diese Übertragung stellt einen nicht unerheblichen kodiertechnischen Aufwand dar, müssen doch

zum Beispiel, um ein einigermaßen flüssiges Bild mit 5 Frames/s bei einer Farbtiefe von 24 Bit und einer Bildschirmauflösung von 1024x768 Pixel zu übertragen, fast 12 MByte pro Sekunde an Daten verarbeitet werden. Noch komplexer ist die Ermittlung dieser Daten aus dem PC heraus. Hier existieren drei konkurrierende technische Ansätze:

- Mittels eines PCI-Bus-Sniffing (Ablauschen des PCI-Buses und Dekodieren von Daten, die für andere PCI-Targets bestimmt sind) werden Daten, die von der System-CPU zum Grafikkadapter gesendet werden, zum Rechnerkern des Remote Management Boards kopiert. Dieses Verfahren funktioniert jedoch nur, wenn innerhalb der PCI Bushierarchie sowohl Grafikkadapter als auch Remote Management Board an einem physischen PCI Bussegment angeschlossen sind. Selbst dann führt dieses Bussniffing meist zu einer Verletzung des PCI Busstandards. Diese Lösung wird von den Herstellern Agilent, Dell und Siemens favorisiert. Da ein Sniffing mit hoher Bitrate meist aus systemtechnischen Gründen nicht möglich ist, unterstützen zusätzliche Gerätetreiber diese Remote Management Boards, indem von der System-CPU Grafikkprimitive direkt in den Speicher des Managementboards geschrieben werden. Der Forderung nach Systemunabhängigkeit kann damit jedoch nicht mehr entsprochen werden.
- Der VGA Adapter befindet sich direkt auf dem Remote Management Board. Das Problem des Bussniffings entfällt damit. Problematisch ist lediglich die Festlegung auf eine spezielle Grafikkarte. Für einen Einsatz in einem Server mit reduzierten Grafikanforderungen ist ein derartiger Ansatz durchaus opportun. Einschränkend wirkt jedoch, dass eine eventuelle bereits vorhandene Grafikkarte im System deaktiviert werden muss. Remote Management Boards mit dieser Technologie werden von Compaq, American Megatrends und Peppercon angeboten.
- Das Remote Management Board liest über PCI-Busmasterzyklen aktiv Grafikdaten aus dem VGA-Controller des Systems. Dabei kommt es zum einen zu einer Belastung des System-Busses durch diese zusätzlichen Bustransaktionen mit entsprechend negativen Auswirkungen auf die Gesamtleistungsfähigkeit des Systems bei Remote Zugriffen. Zum anderen ist dieser Ansatz nur

in Systemen brauchbar, deren PCI Bridges derartige Lesezyklen überhaupt erlauben. Bei allen AGP<sup>6</sup>-basierten Systemen ist dies nicht der Fall. Mit IBM und Dell bieten nur noch zwei Hersteller ein Board mit diesem Technologieansatz an.

Die oben beschriebene Notwendigkeit, detaillierte Kenntnisse über Systeminterna besitzen zu müssen, um ein Remote Management Board in ein System integrieren zu können, führt dazu, dass die meisten Hersteller ihre Boards nur für eigene Serversysteme zur Verfügung stellen und dabei teilweise sogar eigens dafür definierte proprietäre Schnittstellen nutzen. Lediglich das deutsche Unternehmen Peppercon bietet mit eRIC eine herstellerübergreifende Remote Management Lösung an, die jedoch teilweise durch Spezialadapter an die proprietären Gegenheiten einzelner Zielsysteme angepasst werden muss. Preislich liegen Remote Management Boards zwischen 500 und 800 EUR.

OS unabhängig	nur Compaq RemoteInsight[3] und Peppercon eRIC[1], sonst nein
Architekturunabhängig	basieren auf PCI Busstandard
Herstellerunabhängig	nur Peppercon eRIC, sonst nein
Systemzustandsunabhängig	ja
Sicherheit	Authentifizierung, Autorisierung, Verschlüsselung
Clientsoftware	meist Webbrowser
Verbreitung	5...10 % aller verkauften Server werden mit einem Remote Management Board ausgerüstet.
Preis	500 ... 800 EUR

### 3.5 Console Server

Serielle Consolen werden sehr häufig als universelle Management-Schnittstellen eingesetzt. Traditionell werden sie von RISC-Servern, Switches, Routern und UPS<sup>7</sup>en unterstützt. Ein entscheidender Vorteil der seriellen Consolen ist ihre technische Einfachheit, ihre weite Verbreitung und ihre lange Tradition. Die

<sup>6</sup>Accelerated Graphics Port

<sup>7</sup>Uninterrupted Power Supplies

den seriellen Consolen zugrundeliegenden Standards RS232 und V.24 gelten als eingeführt und technisch wenig herausfordernd.

Console Server oder Console Management Server zielen darauf ab, das zeichenorientierte serielle Schnittstellenprotokoll auf einen TCP/IP-Netzwerkzugang zu konvertieren, so dass einerseits der Zugriff auf eine Vielzahl von Servern von einem einzigen Punkt aus möglich wird und andererseits dieser Zugang global zur Verfügung gestellt werden kann.

Als Client Software von Console Servern werden verbreitete Terminalemulationen eingesetzt, die im Falle von *telnet* oder *ssh* mit entsprechenden TCP/IP Protokollstapeln gebündelt und auf nahezu allen Rechnern bereits verfügbar sind.

Ein Console Server lässt sich im Prinzip mittels eines einfachen PCs realisieren, der über einen TCP/IP Stack sowie eine Ethernet und eine RS232 Schnittstelle verfügt. Professionelle Geräte bestehen jedoch durch eine sehr hohe sogenannte *Port-Dichte* und einen niedrigen Preis pro Port.

In eine 19 Zoll Höheneinheit können heute bis zu 48 serielle RS232 Schnittstellen integriert werden. Damit sind Console Server prädestiniert für Rechenzentren und Service Provider, die eine große Zahl von Servern ohne graphische Benutzeroberfläche und andere Geräte wie Router oder auch Klimaanlage kostengünstig und einheitlich kontrollieren möchten.

Zugriffssicherheit in Console Servern wird über normale Login/Password-Vergabe realisiert. Ein verschlüsselter Zugriff mittels SSH gilt nur bei besseren Geräten als Standard.

Der Markt für Consoleserver wird von den vier US-amerikanischen Anbietern Digi International, Lantrox, Cyclades und Equinox bestimmt. Die Preise variieren zwischen ca. 40 EUR bei Geräten mit vielen Ports und 400 EUR bei Einzelportgeräten.

OS unabhängig	nur graphische Nutzerschnittstelle
Architektur-unabhängig	ja
Herstellerunabhängig	ja
Systemzustands-unabhängig	nein, kein Powermanagement
Sicherheit	Authorisierung, teilweise Verschlüsselung
Clientsoftware	meist Webbrowser
Verbreitung	sehr stark im UNIX-Bereich, kaum im Windows-Umfeld
Preis	40 ... 400 EUR (je nach Portdichte des Gerätes)

### 3.6 KVM via IP Geräte

KVM<sup>8</sup> via IP Geräte sind ähnlich gewöhnlichen KVM-Extendern lediglich "Verlängerungen" der wesentlichen externen Schnittstellen eines Rechners. Diese wesentlichen Schnittstellen sind, wie der Name bereits verrät, Tastatur, Bildschirm und Maus. Im Gegensatz zu KVM-Extendern, welche die Signale durch geeignete Modulationsverfahren auf analogem Wege über eine räumlich sehr begrenzte Länge (10-100m) übertragen, findet bei KVM via IP Geräten eine komplette Umwandlung in IP-Pakete statt. Während dies für Keyboard und Maus Signale einfach möglich ist, erfordert die Redigitalisierung eines analogen VGA Signals erheblichen Aufwand. Technisch handelt es sich hier um eine Funktionalität, die von handelsüblichen Framegrabberkarten für geringes Geld angeboten wird. Im Unterschied zu diesen Framegrabberkarten, die auf SVHS oder Fernsehsignale mit 1000\*625 Bildpunkten und 50 Hertz Bildwiederholrate optimiert sind, müssen die Redigitalisierungseinheiten von KVM via IP Geräten bis zu 1280\*1024 Bildpunkte mit einer Bildwiederholrate von 60...85 Hz verarbeiten können. Eine weitere technische Herausforderung liegt in dem Redigitalisierungsrauschen, dass in Form leichter Farbverschiebungen einzelner Pixel äußerst negative Auswirkungen auf die Kompressionsmöglichkeiten des Datenstromes hat. Die Kompression derart hoher Datenvolumina (1280\*1024\*3 Bit Farbtiefe pro Frame) ist nur dadurch möglich, dass unveränderte Bereiche des Bildes erkannt und daher nicht permanent übertragen werden. Das erwähnte Redigitalisierungsrauschen sabotiert diesen Kompressionsansatz sehr wirkungsvoll.

<sup>8</sup>Keyboard Video Mouse

Bisher ist es noch keinem Marktteilnehmer gelungen, die Videoqualität und Videogeschwindigkeit bei KVM via IP-Lösungen auf ein Remote Management Boards vergleichbares Niveau zu heben, obwohl verschiedene Hersteller aus den USA, Deutschland und Israel derartige System vorgestellt haben, die zwischen 3500 und 7000 EUR angeboten werden.

Eine weitere Herausforderung von KVM via IP - Extendern liegt in der Synchronisation des entfernten innerhalb des Bildschirmvideos sichtbaren Maus-kursors mit dem vom lokalen Betriebssystem erzeugten Mauscursor. Um beide Mauskursoren synchron halten zu können, darf die Maussteuerung auf dem entfernten System keinerlei Nichtlinearitäten wie Mausbeschleunigung aufweisen, die in einigen Betriebssystemen wie OS/2 standardmäßig aktiviert sind. Die meisten Produkte im Markt fordern daher auf dem entfernten System einen speziellen Maustreiber in einer speziellen Konfiguration. Lediglich im Produkt LARA[1] der Peppercon AG ist ein sehr intelligenter Algorithmus implementiert, der auch nichtlineare Mauscharakteristik unterstützt.

Ein eleganter Weg, das Maussynchronisationsproblem zu lösen, wurde erstmals von der Firma Rose Electronic mit ihrem Produkt Ultralink[4] vorgestellt. Hier wird die lokale Maus unterdrückt und der Nutzer arbeitet nur mit der innerhalb des Videobildes übertragenen entfernten Maus. Dieser Ansatz erfordert jedoch eine sehr geringe Latenzzeit zwischen Mausbewegung und deren Darstellung auf dem entfernten Bildschirm und ist damit nur innerhalb lokaler Netze einsetzbar.

Wenige heute verfügbare KVM via IP Geräte tragen der Tatsache Rechnung, dass ein Rechner mehr Schnittstellen als nur Keyboard, VGA und Maus hat. Zum Beispiel erlaubt Peppercons LARA oder das Produkt Proxyview des israelischen Unternehmens Replicom[9] den Anschluss von Power und Reset Schaltern bzw. Spannungsschaltdosen für den kontrollierten Rechner.

Es ist zu erwarten, dass die KVM to IP Extender künftig mit weiteren Systemschnittstellen ausgerüstet werden, um einen über die reine Fernbedienung des Rechners hinausgehenden Funktionsumfang realisieren zu können. Peppercons LARA ist auch hier mit der Integration des IPMI Standards ein gewisser Vorreiter.

OS unabhängig	ja
Architektur-unabhängig	ja
Herstellerunabhängig	ja
Systemzustands-unabhängig	ja
Sicherheit	Authorisierung, Authentifizierung und Verschlüsselung
Clientsoftware	meist Webbrowser, auch Windowsclients
Verbreitung	neues Marktsegment, zur Zeit stark wachsend
Preis	3500 ... 7000 EUR

## 4 Vergleich und Fazit

Ein Vergleich der am Markt verfügbaren Remote Managementansätze unter den Gesichtspunkten Preis, Sicherheit, Unabhängigkeit von Architektur, Systemzustand, Betriebssystem sowie Hersteller und Funktionalität zeigt, dass es keine für alle Einsatzfälle gleichermaßen günstigste Lösung am Markt gibt. Wird der Remote Managementansatz auf die reine Anwendungsebene beschränkt, stellen sehr kostengünstige Softwarepakete sicherlich die günstigste Alternative dar. Bei Rechnern ohne graphische Benutzeroberfläche empfiehlt sich der Einsatz von Console Port Servern, wobei hierfür ein durchgängiger Managementansatz sowie entsprechende Reboot - und Powermanagementfunktionen fehlen. Den umfassendsten Managementansatz liefern dedizierte Remote Management Boards, die jedoch in den entsprechenden Rechner eingebaut werden müssen. Ist dies nicht mögch bzw. nicht erwünscht, bleibt als Alternative nur der Einsatz eines preisintensiven KVM to IP Extenders.

Eine Möglichkeit, den pro Port-Preis eines KVM to IP Extenders zu senken, besteht in der Kombination eines solchen Extenders mit einem analogen aber elektronisch steuerbaren Keyboard-Video-Maus- Umschalter. Derartige Kombinationen werden bereits heute fertig integriert angeboten. Die Produkte von Spezialanbietern von KVM to IP Extendern wie Replikom oder Peppercon ermöglichen ebenfalls eine integrierte Ansteuerung von KVM-Switchen, so dass auch bereits verfügbare installierte KVM-Switche für eine solche Lösung verwendet werden können.

## 5 Ausblick

Die erst in den vergangenen zwei Jahren in den Markt eingeführten KVM-to IP Extender haben dem Gesamtmarkt für Remote Management Lösungen neue Impulse verliehen. In den kommenden Jahren werden hier Kombinationen von KVM-to-IP mit anderen Managementansätzen wie Console Server zu beobachten sein. Diese Integration ist heute schon in Ansätzen bei Nutzeroberflächen zu beobachten. Insbesondere scheint das Powermanagement bzw. die Rebootmöglichkeit von Rechnern ein entscheidendes Leistungsmerkmal, das den KVM-to-IP Extendern erst noch erschlossen werden muss. Auch die Integration der vorgestellten Remote Management-Technologien in eingeführte Softwareumgebungen zum Management ist bisher über SNMP hinaus kaum gelungen. So wirken die meisten IPMI-basierten Produkte mehr oder weniger als Insellösungen. Es ist zu erwarten, dass auch hier in den kommenden Monaten integrative Ansätze am Markt erscheinen werden.

Trotz dieser Nachteile scheinen sich Remote Management Werkzeuge im Markt zu bewähren und sowohl tägliche Systemwartung als auch Fehlerbehandlung hinreichend gut zu unterstützen. Preislich machen Sie sich bei den hohen Ausfallkosten heutiger IT-Systeme allemal bezahlt.

## Literatur

- [1] Peppercon AG. Website. <http://www.peppercon.de>, 2002.
- [2] Thomas Breitfeld. Warum in die Ferne schweifen ? Kleine Taxonomie der Remote Management Systeme und deren Anwendung. *LANline special*, 2002.
- [3] Compaq Corp. Website. <http://www.compaq.com>.
- [4] Rose Electronics. Ultralink KVM Extender. <http://www.rosel.com>.
- [5] TU Braunschweig IBR. Snmp version 3. <http://www.ibr.cs.tu-bs.de/projects/snmpv3/>, 2002. Informationen und Linksammlung.
- [6] Intel, Hewlett-Packard, NEC, and Dell. Intelligent Platform Management Interface Specification. <http://www.intel.com/design/servers/ipmi/>, 2002.
- [7] University of Cambridge. Virtual network computing. <http://www.uk.research.att.com/vnc/>.
- [8] Dr. Christian Pätz. Remote Management Boards. *LANline special*, 10(5), 2001.
- [9] Replikom. Website. <http://www.replikom.com>, 2002.