

# Server-Fernverwaltung für Rechenzentrumsmitarbeiter

von Barry Nance, Network Testing Labs

Raritan Computer Europe B.V.  
Juli 2004

### **Copyright- und Warenzeichenvermerk**

Dieses White Paper enthält urheberrechtlich geschützte Informationen. Alle Rechte vorbehalten. Kein Teil des White Papers darf ohne die ausdrückliche vorherige Zustimmung durch Raritan Computer, Inc. fotokopiert, vervielfältigt oder in eine andere Sprache übersetzt werden.

© Copyright 2004 Raritan Computer, Inc., CommandCenter™, Dominion™ und das Raritan-Unternehmens-Logo sind Warenzeichen oder eingetragene Warenzeichen von Raritan Computer, Inc. Alle Rechte vorbehalten. Java® ist ein eingetragenes Warenzeichen von Sun Microsystems, Inc. Internet Explorer® ist ein eingetragenes Warenzeichen von Microsoft Corporation. Netscape® und Netscape Navigator® sind eingetragene Warenzeichen der Netscape Communication Corporation. RC4® ist ein eingetragenes Warenzeichen der RSA Corporation. Andere Warenzeichen oder eingetragene Warenzeichen sind Eigentum der jeweiligen Inhaber.

# Inhaltsverzeichnis

1.	Einführung .....	1
2.	Wer braucht KVM-Zugriff? .....	3
2.1.	Am Rack .....	3
2.2.	Auf dem Unternehmensgelände .....	3
2.3.	Fernzugriff auf Rechenzentren .....	4
2.4.	Zugriff auf Zweigstellengeräte .....	4
3.	KVM-over-IP-Technologien .....	6
3.1.	Einschränkungen durch die Bandbreite .....	6
3.2.	Sicherheit .....	7
4.	Probleme und Herausforderungen des Server-Zugriffs .....	8
4.1.	Leistung .....	8
4.2.	Sicherheit .....	9
4.3.	Flexibilität .....	9
4.4.	Einfache Handhabung und Installation .....	9
4.5.	Kosten .....	9
5.	Zusammenfassung .....	11
6.	Über den Autor .....	12
7.	Über die Network Testing Labs .....	13
8.	Raritan Computer – Profil .....	14
8.1.	Über Raritan Computer .....	14

# 1. Einführung

Die auf mehrere Standorte verteilten, komplexen IT-Infrastrukturen von heute, die aus heterogenen Servern, Routern, Switches und anderen Geräten bestehen, sind sehr schwer zu steuernde und zu verwaltende Umgebungen. IT-Abteilungen haben den Auftrag, die Betriebsleistung überall im Unternehmen - von den Rechenzentren des Hauptsitzes bis hin zu den Zweigstellen – zu erhalten, um damit die Geschäftstätigkeit zu unterstützen und gleichzeitig die Kosten so gering wie möglich zu halten.

Die finanziellen Folgen von Ausfallzeiten der IT-Infrastruktur können für Unternehmen sehr schwerwiegend sein: weniger Geschäftstätigkeit, Verlust von Benutzer- bzw. Kundenvertrauen, zusätzliche Lohnkosten, die durch die Beseitigung der Probleme entstehen, sowie Vertragsstrafen, aufgrund von vertraglichen Bindungen (Service Level Agreements) mit internen oder externen Kunden. Je nach Industriezweig variieren die Kosten von IT-Ausfallzeiten von hunderten bis zu mehreren Millionen Dollar pro Stunde.

In komplexen, verteilten IT-Umgebungen überwachen Software-Lösungen, wie z.B. Tivoli® von IBM, UnicenterTNG® von Computer Associates und HP Open View™ die Funktionalität der Geräte eines Netzwerks. Diese Lösungen wurden in erster Linie entwickelt, um auftretende Fehler zu entdecken und Netzwerk-Administratoren zu benachrichtigen. Die Funktionalität dieser Art von Geräte-Verwaltung beschränkt sich jedoch darauf, was man erreichen kann, wenn auf die Ziel-Geräte über eine Netzwerk-Schnittstellenkarte (siehe Abbildung 1) zugegriffen wird und das Betriebssystem des Geräts einwandfrei funktioniert. Wenn das Netzwerk nicht funktioniert oder sich das Geräte-Betriebssystem aufhängt oder abstürzt, müssen IT-Techniker für die Wiederherstellung der Funktionstüchtigkeit entsandt werden, um das Problem zu analysieren und die notwendigen Reparatur-Maßnahmen zu ergreifen.

Um die Zweigstellen-Infrastruktur zu verwalten, verwenden manche Unternehmen Software-Utilities wie Carbon Copy®, Windows® Terminal Services und PCAnywhere™. Ebenso wie die oben erwähnten komplexeren Software-Lösungen für Rechenzentren, verfügen diese Billig-Lösungen auch über begrenzte Zugriffsmöglichkeiten und Steuerungsfunktionen, und außerdem sind sie ebenfalls von einem funktionstüchtigen Betriebssystem der Ziel-Geräte abhängig. Darüber hinaus laufen einige Software-Lösungen nur mit bestimmten Servern und Geräten, sodass mehrere Produkte zur Fernverwaltung erworben werden müssen. Das Ergebnis ist eine Umgebung mit mehreren Logins, verschiedenen Benutzeroberflächen und anderen Faktoren, die eine Verwaltung eines ortsfernen Serverschranks erschweren. Während dies vielleicht für die Verwaltung der Zweigstelleninfrastruktur akzeptabel ist, reicht diese Lösung nicht aus, um ein Betriebssystem und die Server zu verwalten.

Die Steuerung auf BIOS- oder Konsolenebene ist entscheidend, wenn es darum geht, einen ausgefallenen Server wieder funktionstüchtig zu machen, da die User einen Computer noch über die KVM-Ports steuern können, selbst wenn das Betriebssystem nicht mehr funktioniert. Dies ist der Punkt, an dem hardwarebasierte KVM- (Keyboard/Video/Maus) und Steuerungs-Tools von seriellen Konsolen wirkungsvoll eingesetzt werden können. Sie tragen dazu bei, dass IT-Mitarbeiter die Funktionstüchtigkeit wieder herstellen und Geräte-Probleme beseitigen können, ohne jemals körperlich mit den eigentlichen Geräten in Berührung zu kommen.

Mit der richtigen KVM-Technologie und den geeigneten Tools können Rechenzentrumsmitarbeiter produktiver arbeiten, ob nun innerhalb oder außerhalb des Rechenzentrums. Sie können IT-Geräte nach Fehlern absuchen, konfigurieren, warten und sogar rebooten – als ob sie direkt am Rack stehen würden, auch wenn (und gerade wenn) der Server oder das Netzwerk ausgefallen ist.

Zusätzlich zu der Tatsache, dass Probleme viel professioneller angegangen werden können, ermöglichen KVM-Lösungen auch eine bessere vorbeugende Wartung. Darüber hinaus sparen sie kostbaren Platz im Rechenzentrum und in der Zweigstelle, da mehrfache Tastaturen, Monitoren, Mäuse und Kabel überflüssig werden.

Einige KVM-Lösungen arbeiten unabhängig vom Netzwerk – also „out-of-band“ — und leiten Tastatur-, Video und Maus-Signale in einem dedizierten Kabel von den Servern zum KVM-Umschalter. Diese analogen KVM-Lösungen sind ideal, um Server von einer Entfernung von bis zu 300 m vom Rechenzentrum aus zu steuern.

Für einen erweiterten Fernzugriff sind digitale KVM- bzw. KVM-over-IP-Lösungen ideal, da sie IP-basierte Netzwerke verwenden, um die Verwaltungsreichweite der Mitarbeiter des Rechenzentrums zu erweitern. Bevor sie über ein TCP/IP-Netzwerk weitergeleitet werden, werden analoge Tastatur-, Video- und Maus-Signale digitalisiert. System-Administratoren können sich über das Internet von jedem Ort aus einloggen und sofort mit der Beseitigung des Fehlers beginnen. Server-Administratoren müssen sich also nicht mehr während der Ausfallzeiten zu Zweigstellen oder zum Hauptsitz begeben, um einer Fehlermeldung nachzugehen oder Probleme zu beseitigen.

Der KVM-Fernzugriff ermöglicht den IT-Mitarbeitern nicht nur schneller zu reagieren und effizienter zu arbeiten, die Unternehmen können ihre IT-Ressourcen auch besser nutzen. Virtuelle IT-Teams können zum Beispiel für bestimmte Projekte oder für bestimmte Problemstellungen gebildet werden - ganz unabhängig vom geografischen Aufenthaltsort.

Aber nicht alle KVM-Fernlösungen sind gleich. Dieser Artikel identifiziert und analysiert die Parameter, die ein IT-Manager in Betracht ziehen sollte, um die richtige KVM-Lösung zu wählen. Der Artikel unterscheidet nach der Art des Zugriffs, den die Mitarbeiter des Rechenzentrums benötigen – je nach dem, ob sie am Rack, auf dem Unternehmensgelände oder weltweit arbeiten.

## 2. Wer braucht KVM-Zugriff?

Die KVM-Produkte, die in einem Unternehmen eingesetzt werden, beeinflussen zu einem großen Ausmaß die Effektivität, Produktivität und die Effizienz, mit der die Mitarbeiter eines Rechenzentrums arbeiten. Egal wie weit ein Rechenzentrumsmitarbeiter von den Servern entfernt ist, er benötigt einen reaktionsstarken, verlässlichen, sicheren und einfach zu handhabenden Server-Zugriff, um Einstellungen zu konfigurieren, zu verändern und jedes Serverproblem in möglichst kurzer Zeit zu lösen. Administratoren benötigen im Unternehmen drei verschiedene zuverlässige Zugriffsarten auf die Server: am Rack, auf dem Unternehmensgelände und als Fernzugriff.

### 2.1. Am Rack

Es gibt Mitarbeiter, die Zugriff auf mehrere Server direkt „am Rack“ benötigen, da sie zum Beispiel CD-ROMs einlegen, Kassettenbänder auswechseln, neue Server einrichten und hin und wieder ausgefallene Stromversorgungen, Netzwerkadapter oder Festplatten-Laufwerke austauschen müssen.

Rechenzentrumsmitarbeiter, die Geräte bedienen, konfigurieren und Reparaturen ausführen – die also direkt im Rechenzentrum arbeiten – kommunizieren typischerweise mit einzelnen Servern über einen einfachen, direkt angeschlossenen, analogen KVM-Umschalter. Alle KVM-Kabel der Server eines Pools oder einer Untergruppe sind direkt an einem KVM-Umschalter angeschlossen, an dem wiederum eine reelle Tastatur, ein Monitor und eine Maus hängen. Für den Fall eines mehrfachen User-Zugriffs zur gleichen Zeit verfügen einige Switches über Anschlüsse für bis zu 16 User; andere unterstützen sogar noch mehr User.

Die lokalen KVM-Geräte können mit Hilfe von Koaxial- oder Unshielded Twisted Pair (UTP) Cat5-Kabeln angeschlossen werden. Cat5-Kabel bieten eine höhere Bandbreite innerhalb der lokalen Zone bis zu ca. 300 m. Einige KVM-Umschalter können miteinander verkettet oder in Kaskadenschaltung angeordnet werden, um eine große Anzahl von Servern zu bedienen. Andere Lösungen, insbesondere digitale KVM-Lösungen können bis auf Tausende von Servern erweitert werden, indem einfach Umschalter dem Netzwerk zugefügt werden, wobei jeder Umschalter seine eigene IP-Adresse hat.

### 2.2. Auf dem Unternehmensgelände

Eine andere Gruppe von IT-Mitarbeitern – nämlich Kapazitätsplaner, Problemlöser und Netzwerktechniker, die sich irgendwo auf dem Unternehmensgelände oder auf einem Campus befinden – muss ebenfalls Server bedienen. Aber diese Mitarbeiter müssen nicht unmittelbar am Rack arbeiten.

Diese Gruppe benötigt KVM-Verbindungen, die Signale über größere Entfernungen hinweg als normale Koaxial-KVM-Kabel übertragen können. Die Mitarbeiter, die sich in einem anderen Raum bzw. in einem anderen Stockwerk befinden, benötigen eine KVM-Umschalter-Ausstattung, mit deren Hilfe sie sich direkt neben dem Server zu befinden scheinen. Während sich ein UTP-Cat5-Kabel für ein Campus-Gelände eignet, das sich in einem Umkreis von 300 m um die Server erstreckt, ist ein Glasfaserkabel eine gute Lösung für Entfernungen von fast bis zu 10 km. KVM-over-IP-Verbindungen sind ebenfalls gute Alternative.

### 2.3. Fernzugriff auf Rechenzentren

Eine weitere Gruppe, wie z.B. zentral arbeitende übergeordnete Betriebszentrumsleiter, benötigen den Fernzugriff auf die Server. Diese Mitarbeiter können sich im Hauptsitz des Unternehmens oder auch in einem anderen Land befinden.

Diese Betriebszentrumsleiter brauchen KVM-Verbindungen, die über ein Netzwerk laufen – WAN, VPN oder das Internet. Betriebszentrumsmitarbeiter verfügen aufgrund von KVM-over-IP über spezielle komfortable Möglichkeiten, aber mit KVM-over-IP geht man – je nach KVM-Hersteller – Kompromisse bei der Bandbreitenausnutzung und der Reaktionsschnelligkeit ein. Um diese Probleme anzugehen, muss darauf geachtet werden, dass die KVM-over-IP-Tools eines Herstellers einen Grad an Verschlüsselung, Komprimierung und Bandbreiten-Management aufweisen, der die aktuellen und zukünftigen Sicherheits- und Leistungsanforderungen erfüllt.

### 2.4. Zugriff auf Zweigstellengeräte

IT-Mitarbeiter benötigen nicht nur den Fernzugriff auf Server in Rechenzentren, sondern es fällt auch oft in ihren Verantwortungsbereich, Server und Netzwerk-Geräte in Zweigstellen zu verwalten. Die Ausstattung in einer Zweigstelle kann oft sehr vielfältige Geräte beinhalten, wie z.B.:

- KVM-gesteuerte Server wie z.B. Windows-, Linux- und Solaris-Server
- Über serielle Konsolen gesteuerte Geräte wie z.B. Router/Switches, Firewalls, Netzwerk-Anwendungen, HVAC-Steuerungen, Sicherheitssysteme, Telecom-Controller und kopflose (headless) Server (UNIX, Linux, Solaris)

Normalerweise sind die Mitarbeiter in diesen Zweigstellen keine IT-Experten und sind deshalb nicht in der Lage, diese Art von Problemen zu lösen und die Infrastruktur zu verwalten. In diesen Fällen verwenden Rechenzentrumsmitarbeiter Fernzugriff-Software-Lösungen, um das Problem der Fernwartung der Infrastruktur in den Griff zu bekommen. Die Software-Lösungen funktionieren jedoch nur, wenn auch das Netzwerk funktionstüchtig ist, und – im Falle eines Servers - wenn das Server-Betriebssystem in Ordnung ist. Wenn das Netzwerk ausgefallen oder das Server-Betriebssystem abgestürzt ist, werden die Mitarbeiter vor Ort oft gebeten, „zum Serverschrank zu gehen und die Reset-Taste zu drücken“, und wenn dann der Router oder Server nicht wieder funktioniert, müssen hohe Kosten und viel Zeit in eine Reise zur Zweigstelle investiert werden.

Für eine solche Situation ist die ideale Lösung ein Gerät, das alles in sich vereint, d.h. das sowohl über KVM-Ports als auch serielle Konsolen-Ports verfügt, und das mit einer Port-Dichte ausgestattet ist, die sich vom finanziellen Aufwand her für den Einsatz als Verwaltung von Zweigstellen-Geräten eignet, das heißt z.B. mit 4 KVM-Ports und 4 seriellen Ports. Hierbei ist es wichtig, dass Sie sich für eine Zweigstellen-Verwaltungslösung mit einem eingebauten Modem entscheiden, denn falls das Netzwerk-Edge-Gerät in der Zweigstelle ein Router ist, und dieser Router ausfällt, ist die einzige Möglichkeit, zum Router vorzustoßen und ihn wieder funktionstüchtig zu machen ohne dabei „ mit einem LKW anreisen müssen“, sich in das Gerät über ein Modem einzuwählen, und auf den Router über den seriellen Konsolen-Port zuzugreifen.

Die folgende Übersicht fasst die Optionen, die in Bezug auf die KVM-Konnektivität bestehen, nach diesen drei IT-Benutzergruppen zusammen. Es kommt darauf an, die beste Lösung für jede Situation zu wählen. KVM-Lösungen, die eine Cat 5-, Koaxial- und Glasfaser-Verkabelung aufweisen, sind sehr gut, was die Sicherheit und Bandbreite anbelangt, sie stoßen jedoch an ihre Grenzen, wenn es darum geht, größere Entfernungen zu überbrücken. KVM-over-IP überbrückt natürlich die größten Entfernungen, aber es kann zu einer geringfügigen Verzögerung bei Tastatur-, Maus und Video-Signalen kommen. Es gibt auch Hybrid-Lösungen, die analoge und digitale KVM-Umschaltungstechnologien kombinieren.

Die verschiedenen Hersteller haben KVM-Technologien auf den Weg gebracht, deren Erfolg in Bezug auf Reaktionsschnelligkeit, Bandbreitenausnutzung, Sicherheit, Erweiterbarkeit und andere Faktoren sehr stark variiert. Einige Hersteller von Server-Zugriffs-Geräten und -Technologien bieten Produkte an, die den Ansprüchen nur einer der drei Benutzer-Gruppen entgegenkommen, und dann irreführenderweise auch für die anderen Gruppen dieselbe „Lösung“ anbieten.

Achten Sie darauf, dass der KVM-Hersteller eine integrierte, plattformunabhängige Lösung bietet, die jeder autorisierte Benutzer aller drei Benutzer-Gruppen jederzeit von jedem Ort aus anwenden kann. Denken Sie daran, dass die Lösung von IT-Problemen oft mehr als nur einen Zugriff auf die Server erfordert; ein IT-Problemlöser kann auch den Zugriff auf serielle (RS-232) Geräte benötigen, wie z.B. Router, Switches und kopflose (*headless*) Server. Wenn es darüber hinaus einige Zweigstellen gibt, wird eine Lösung gebraucht, die es den Rechenzentrumsmitarbeitern ermöglicht, auf die Geräte an weit entfernten Orten zuzugreifen. Ein ideales KVM-System würde auch eine einfache, konsistente Übersicht über alle Geräte in den Rechenzentren und Zweigstellen möglich machen und darüber hinaus Produktmerkmale, wie z.B. eine intuitive Benutzeroberfläche und Single Sign-on auf sich vereinen.

Außerdem sollten KVM-Tools gut erweiterbar sein, mehrere Benutzer gleichzeitig unterstützen, mit mehreren Plattformen arbeiten, flexible Zugriffsoptionen haben und rückwärtskompatibel mit bereits vorhandener KVM-Ausstattung sein.

### 3. KVM-over-IP-Technologien

Die Technologie, die notwendig ist, um Video, Tastatur und Maus mit einer Vielzahl von Servern und Geräten zu verwenden, hat sich in den letzten Jahren enorm weiterentwickelt. Von rudimentären A/B-Switches über analoge KVM-Boxen mit begrenzter Funktionalität bis hin zu noch nie da gewesenen analogen und digitalen KVM-Systemen für den Zugriff und die Steuerung auf Unternehmensebene: KVM-Technologie spielt eine entscheidende Rolle in der IT-Gesamt-Management-Strategie eines Unternehmens.

Ein Rechenzentrumsmitarbeiter, der KVM-over-IP verwendet, ist vielleicht viele Kilometer vom Server entfernt, aber er kann eine Software starten oder stoppen, er kann die Software-Einstellungen neu konfigurieren und den Server rebooten – gerade so, als ob er direkt vor dem Server stehen würde. Der Mitarbeiter kann sogar auf BIOS-Ebene auf die Computer-Konfigurations-Daten zugreifen.

KVM-over-IP-Technologie verwandelt einen an ein Netzwerk angeschlossenen Client-Computer in eine Server-Konsole. Die Technologie verschlüsselt Tastatureingaben, Maus-Bewegungen und Maus-Klicks in TCP/IP-Pakete, die der Client an den Server schickt, und sie verschlüsselt auf ähnliche Weise die Video-Signale des Servers in TCP/IP-Pakete, damit der Server sie dann zum Client sendet. Jeder Hersteller hat dabei eine Obergrenze der Video-Auflösung, die die Technologie unterstützt. Es ist wichtig, darauf zu achten, dass die Produkte eines Herstellers mit den Server-Auflösungen arbeitet, die die Mitarbeiter im Augenblick oder in Zukunft benötigen. Die meisten KVM-Hersteller bieten eine maximale Video-Auflösung von 1280 x 1024, mit einer Bildwiederholrate von 60 Hz. In seltenen Fällen – was dafür aber umso bemerkenswerter ist – bieten Hersteller auch höhere Auflösungen.

#### 3.1. Einschränkungen durch die Bandbreite

Der KVM-over-IP-Client, z.B. die Benutzerstation, ob es sich dabei nun um einen PC, ein Notebook oder ein drahtloses Gerät handelt, verbindet sich normalerweise mit einem IP-Netzwerk über ein DSL mit mittlerer Geschwindigkeit oder eine Kabel-Modem-Verbindung oder vielleicht auch mit einer relativ langsamen 56k Einwahl-Verbindung. Leider ist es dann sehr leicht möglich, dass man aufgrund von Bandbreitenbeschränkungen zwischen Client und Server äußerst träge Reaktionen vom Server erhält. Darauf zu warten, dass eine Tastatur-Eingabe auf dem ortsfern angeschlossenen Server-Bildschirm erscheint oder dass ein Maus-Cursor mit den Mausbewegungen eines IT-Mitarbeiters Schritt hält, ist ärgerlich und unproduktiv. Wenn zudem das KVM-Tool nicht entsprechend konzipiert ist, können mehrere Mitarbeiter, die gleichzeitig auf die Server-Bank zugreifen, sich gegenseitig bremsen.

Ein sehr wichtiger Faktor ist das Datenvolumen, das der KVM-Client und der Server über das Netzwerk austauschen, insbesondere sind hier Server-Bildschirme mit hoher Auflösung zu nennen – KVM-over-IP-Video-Signale können sehr viel Netzwerk-Bandbreite verbrauchen. Wenn die KVM-over-IP-Software nicht gut entwickelt wurde, können mehrere Benutzer, die über dieselben Netzwerk-Verbindungen arbeiten, die verfügbare Bandbreite verbrauchen, und das Netzwerk im Schneckentempo arbeiten lassen.

KVM-Hersteller verwenden zwei Technologien, um die Netzwerk-Bandbreite zu reduzieren, die notwendig ist, um große Video-Datenmengen zu übertragen. Erstens, ein KVM-System hält fest, was bereits auf dem Bildschirm des IT-Mitarbeiters gezeigt wird, und schickt nur die Daten, die sich verändert haben, so genannte Deltas, über das Netzwerk. Indem anstelle des gesamten Bildschirms nur Deltas an den Client geschickt werden, reduziert sich der Bandbreitenverbrauch ganz erheblich.

Beachten Sie, dass manche KVM-Hersteller über bessere Algorithmen verfügen, um Deltas festzustellen, und so das Netzwerk weniger unnötig belasten. Zweitens, ein KVM-System komprimiert die Deltas, bevor sie übertragen werden. Da einiger Hersteller über effizientere Komprimierungs-Algorithmen verfügen, variiert die Größe der komprimierten Deltas von Hersteller zu Hersteller erheblich.

Beachten Sie auch, dass die selektive und intelligente Überwachung von Video-Parametern, wie z.B. die Menge an Farbdaten, die das KVM-System übermittelt, den Bandbreitenverbrauch beeinflusst. Bei einigen KVM-System-Lösungen ist es sogar möglich, dass die Benutzer eine Feineinstellung bei der Übertragung von Video-Daten des Systems vornehmen können. Zum Beispiel kann der Benutzer die Farbtiefe reduzieren und dann den Bildschirm mit weniger Farben sehen, um die Leistung des KVM-Systems zu verbessern und kurze Reaktionszeiten bei langsamen Verbindungen zu schaffen.

Darüber hinaus können einige Lösungen so programmiert werden, dass die Bandbreite, die für die Benutzer verfügbar ist, beschränkt wird, damit wichtigere Anwendungen nicht behindert werden. Eine wirklich ideale KVM-Lösung, die das Problem Bandbreite angeht, lässt eine Einstellung des Bandbreitenverbrauch je nach Benutzer zu. Für sehr netzwerkintensive Organisationen kann der Einsatz eines zweiten, separaten Netzwerks nur für den KVM-Zugriff die Lösung des Bandbreiten-Problems darstellen.

### 3.2. Sicherheit

Die beste KVM-Lösung sollte Datensicherheit und Authentifizierung durch ein Daten-Verschlüsselungs-Schema bieten, wie z.B. Secure Sockets Layer (SSL), und keine größeren Veränderungen bei der Konfiguration der Firewall erfordern. In der besten aller möglichen Welten würde das KVM-over-IP-Tool nur die Öffnung eines einzigen Ports in der Firewall notwendig machen. Wenn eine KVM-over-IP-Lösung über ein Virtual Private Network (VPN) arbeiten kann, ist das ebenfalls ein dickes Plus.

Was die Sicherheit anbelangt, wenden einige Hersteller einen 128-Bit-Verschlüsselungsstandard an, der auch den Bandbreitenverbrauch und die Gesamtleistung beeinflussen kann. Sowohl die SSL-Kommunikationen als auch der Datenstrom, der zwischen den Remote Clients und den Servern übermittelt wird, sollten verschlüsselt werden. Einige Hersteller verschlüsseln nur die Tastatur- und die Maussignale und lassen Video-Signale unverschlüsselt. Dies ist nicht so sicher wie Systeme, in denen Tastatur-, Maus- und Video-Signale verschlüsselt werden.

Um den Zugriff auf wichtige Active-Directory-Strukturen und andere entscheidende Verwaltungsdaten zu steuern, sollte das KVM-over-IP-Produkt mit allen Sicherheits-Protokollen arbeiten, die Industrie-Standard sind, wie z.B. die Windows NT-Authentifizierung (NTLM), Lightweight Directory Access Protocol (LDAP), Radius, Active Directory und TACACS+. Die Sicherheitsmerkmale sollten im KVM-over-IP-Produkt integriert sein. Es sollte nicht notwendig sein, einen separaten Server nur für die KVM-over-IP-Authentifizierung zu kaufen und zu konfigurieren. Weil die KVM-Lösung immer verfügbar sein muss, um Probleme zu lösen, die in einem Rechenzentrum auftreten können, muss sie eine eigenständige Lösung sein — absolut unabhängig von externen Servern. Wenn z.B. die Windows-Server in einem Rechenzentrum von einem böartigen Wurm oder Virus angegriffen werden, sollte die KVM-Lösung sich bei der Authentifizierung nicht auf dieselben Windows-Server stützen. Die Authentifizierung der KVM-Lösung selbst sollte aktiviert werden, wenn ein Active Directory Server nicht mehr verfügbar ist.

## 4. Probleme und Herausforderungen des Server-Zugriffs

Wenn ein Mitarbeiter des Rechenzentrums ein Problem zeitnah beseitigen möchte, benötigt er ein KVM-System, das reaktionsschnell aber nicht belastend ist. Im Folgenden finden Sie eine umfassende Liste von Problemen und Herausforderungen, die bei der Bewertung und Auswahl von KVM-Produkten in Betracht gezogen werden sollten. Um die Arbeit zu erleichtern, sind diese Überlegungen in verschiedene Kategorien unterteilt – Leistung, Sicherheit, Flexibilität, einfache Handhabung und Kosten.

### 4.1. Leistung

**Leistung/Maus-Synchronisierung** – Wie lange dauert es, bis die Handlung des Mitarbeiters, der den Server bedient, auf dem Monitor sichtbar wird?

**Bandbreitenausnutzung** – Nimmt die Leistung je nach Netzwerk-Umgebung, Einwahl, DSL, WAN, IP ab? Kann ein Administrator oder Benutzer die Bandbreite drosseln? Wird Bandbreite vom Rechenzentrums-Netzwerk abgezapft? Gibt es eine konfigurierbare Video-Komprimierungstechnologie?

**Reaktionsfähigkeit der Client-Software** – Ist die Client-Komponente für den Server-Zugriff gut konzipiert? Braucht Sie für die Übermittlung viel Zeit, wenn sie ein Java-Applet in den Web-Browser herunterlädt? Wenn das Applet heruntergeladen wurde, hält das Applet mit dem Mitarbeiter Schritt oder ist es träge? Ist die Software bei Clients, die nicht browserbasiert sind, urheberrechtlich geschützt? Hat sie ungewöhnliche oder einschränkende PC- oder Betriebssystem-Anforderungen?

**Blockierter vs. nicht blockierter Zugriff** – Gibt es genügend Client-Pfade zu jedem Rack, sodass mehrere Benutzer immer auf den bzw. die Server zugreifen können, den/die sie verwalten müssen?

**Wiederherstellung nach Katastrophen** – Kann das Tool den Mitarbeitern des Rechenzentrums helfen, das System nach größeren Katastrophen, wie zum Beispiel einem verheerenden Netzwerk-Ausfall, wiederherzustellen? Unterstützt die Lösung einen „Single Sign-on“ oder müssen die Mitarbeiter sich durch mehrere Logons kämpfen, bevor sie zu dem Gerät gelangen, auf das sie zugreifen müssen?

**Maximale Video-Auflösung** – Unterstützt das KVM-Tool eine Video-Auflösung in der Höhe, die benötigt wird?

**Netzwerk-Backup** – Welche alternativen Server-Zugriffsmöglichkeiten gibt es, wie zum Beispiel Back-up-Modem-Zugriff, wenn das Netzwerk ausfällt?

**Eigenständig** – Ist die KVM-Lösung eigenständig, sodass sie immer verfügbar ist, auch wenn die Daten-Server ausfallen?

## 4.2. Sicherheit

**Server- und Netzwerksicherheit** – Genügt das Tool den Ansprüchen des Unternehmens, wenn es darum geht, die Authentizität und Vertraulichkeit der Interaktionen zwischen Server und Mitarbeitern zu wahren?

**Protokoll-Unterstützung** – Arbeitet das KVM-System mit Industriestandard-Sicherheitsprotokollen?

**Authentifizierung** – Ist Sicherheit und Authentifizierung in der Box integriert oder braucht das KVM-Produkt einen zentral platzierten Authentifizierungs-Server? Wenn es einen externen Server für die Authentifizierung benötigt, stellt sich die Frage, was passiert, wenn die WAN ausfällt. Wie wird die Authentifizierung der ortsfernen Mitarbeiter durchgeführt?

**Verschlüsselung** – Bietet das System eine 128-Bit-Verschlüsselung? Verschlüsselt es Tastatur-, Maus- und Videosignale, oder nur Tastatur- und Maussignale?

## 4.3. Flexibilität

**Erweiterbarkeit** – Kann eine Fern-Zugriffs-KVM-Lösung erweitert werden, wenn das Unternehmen wächst? Lässt sie mehrere Benutzer gleichzeitig auf einen Server-Pool zugreifen? Oder ist der gleichzeitige Zugriff auf zwei oder vier Personen beschränkt?

**Kompatibilität mit neuen Technologien** – Ist es wahrscheinlich, dass die Lösung, mit Neuentwicklungen im KVM-Bereich arbeiten kann?

**Plattformunabhängig** – Lässt sie die Verwaltung einer heterogenen Computer-Umgebung zu?

## 4.4. Einfache Handhabung und Installation

**Breite der Produktpalette** – Verfügt das Produkt über eine Vielfalt von Benutzer- und Port-Konfigurationen für den maximalen nicht blockierten Zugriff?

**Einfache Verwaltung** – In welchem Ausmaß interferiert das KVM-Tool mit den täglichen Aufgaben des Mitarbeiters, der den Server bedient?

**Steuerungsmöglichkeiten** – Kann das Tool mit seriellen Konsolen und Leistungsregelungs-Geräten integriert werden? Gibt es einen „Single Sign-on“ für kaskadierte Switches?

**Setup und Konfigurierung** – Sind Setup und Wartung einfach? Benötigt man zusätzliche Software oder andere Hilfsmittel? Bleiben die Server-Namen erhalten, wenn ein Switch ausfällt? Erkennt das KVM-Produkt den Server an seinem neuen Ort, wenn das Bedienungspersonal den Server bewegt und ihn im Netzwerk an einer anderen Stelle neu angeschlossen hat?

## 4.5. Kosten

**Versteckte Kosten** – Benötigt das Produkt einen dedizierten Authentifizierungs- oder System-Verwaltungs-Server, oder ist alles bereits im Switch enthalten?

**Budget und Ressourcen** – Wie hoch sind die positiven bzw. negativen finanziellen Folgen der Einführung des KVM-Tools auf die Ausgaben, die Produktivität und die Auslastung der Computer-Umgebung?

**Investitionsschutz** – Inwiefern macht ein neues KVM-Tool die Veränderung von Elementen der Computer-Umgebung — einschließlich bereits existierender KVM Geräte — notwendig, damit das neue Tool integriert werden kann? Kann es mit älteren KVM-Systemen arbeiten oder erfordert es den Austausch von gut funktionierender Hardware, nur um die KVM-Erweiterung integrieren zu können?

**Software** – Erfordert es zusätzliche Software auf der Client- und/oder Server-Seite?

**Gesamtkosten des Erwerbs** – Was sind die Gesamtkosten des KVM-Tools für das Unternehmen, wenn jeder Aspekt des Rechenzentrums-Betriebs in Betracht gezogen wird?

## 5. Zusammenfassung

KVM-Fernzugriff ist ein einfaches und zugleich leistungsstarkes Konzept. Es ermöglicht die Verwaltung eines ganzen Rechenzentrums mit Zweigstellen von dem Ort aus, wo sich die IT-Ressourcen befinden; dies vereinfacht die IT-Verwaltung, spart Kosten und verbessert die Betriebsleistung. Die richtige KVM-Entscheidung ermöglicht den IT-Mitarbeitern einen reaktionsschnellen, sicheren, flexiblen, einfachen und preisgünstigen Zugriff auf die IT-Geräte Ihres Unternehmens, um diese verwalten zu können.

Raritan Computer bietet sowohl analoge als auch digitale KVM-Lösungen an, sodass IT-Organisationen die leistungsstärksten Lösungen abgestimmt auf ihre spezifische IT-Infrastruktur erwerben können. Faktoren wie Nähe zum Rack, Anzahl der Server und Geräte, sowie der Benutzer sollten in die Überlegungen mit einbezogen werden, um die beste Raritan-Lösung auszuwählen.

## 6. Über den Autor

Barry Nance ist ein Netzwerkexperte, Kolumnist für Zeitschriften, Buchautor und Anwendungsarchitekt. Er kann auf 29 Jahre Erfahrung im IT- Bereich (Technologie, Methoden und Produkte) zurückblicken. In den letzten zwölf Jahren bewertete er im Auftrag der Network Testing Labs Tausende von Hardware- und Software-Produkte für Computerworld, BYTE Magazine, Government Computer News, PC Magazine, Network Computing, Network World und viele andere Veröffentlichungen. Er ist Autor von vielen Tausend Artikeln und drei erfolgreichen Büchern: Introduction to Networking (4. Auflage), Network Programming in C und Client/Server LAN Programming.

Er konzipierte erfolgreiche Web-basierte E-commerce-Anwendungen, schuf Datenbank- und Netzwerk-Benchmark-Tools, schrieb mehrere Netzwerk-Diagnostik-Software-Utilities und entwickelte eine Anzahl von Netzwerk-Protokollen für spezifische Zwecke.

Seine E-mail-Adresse ist [barryn@erols.com](mailto:barryn@erols.com).

## 7. Über die Network Testing Labs

Network Testing Labs widmet sich der unabhängigen Technologieforschung und führt Produktbewertungen durch. In ihrem Netzwerklabor sind eine Vielzahl von Computertypen und praktisch jede Art von Netzwerkgeräten in immer neuen Variationen miteinander verbunden. Ihre Autoren sind Netzwerkexperten, die klar und verständlich über komplexe Technologien und Produkte schreiben.

Die Experten von Network Testing Labs schreiben Bewertungen von Hardware- und Softwareprodukten, Analysen von Neuentwicklungen, Fachartikel, Skripts für Technologie-Workshops, Titelgeschichten, Leitfaden zur Käuferorientierung und kompetente Technologie-Ausblicke. Unsere Experten hielten über eine Reihe von Themen auf der PC Expo und anderen Veranstaltungen Vorträge. Darüber hinaus schufen Sie Industriestandard-Netzwerk-Benchmark-Software, Datenbank-Benchmark-Software und Netzwerk-Diagnostik-Utilities.

## 8. Raritan Computer – Profil

### 8.1. Über Raritan Computer

Raritan Computer Inc. ist ein führender Hersteller von Lösungen zur Verwaltung von IT-Infrastrukturen für den sicheren Zugriff sowie die Überwachung und Verwaltung von Servern und anderen IT-Geräten in Rechenzentren und Zweigstellen. Produkte von Raritan werden eingesetzt, um Millionen von Servern in mehr als 50.000 Rechenzentren, Computer-Testlabors und anderen Umfeldern überall auf der Welt zu steuern und zu verwalten. Vom Kleinunternehmen bis zum Konzern, die komplette Produktpalette von Raritan umfasst kompatible und erweiterbare, digitale and analoge KVM-, serielle Konsolen- und Fern-Konnektivitäts-Produkte, die IT-Experten extrem verlässliche, flexible und sichere Lösungen bieten, um IT-Geräte zu verwalten und gleichzeitig die Betriebsleistung zu verbessern. Raritan wurde 1985 gegründet und blickt auf 19 Jahre ertragreiches Wachstum und technologische Innovation zurück. Raritan verfügt über 25 Niederlassungen und wird in 76 Ländern vertrieben. Weitere Informationen über das Unternehmen erhalten Sie bei [www.raritan.com](http://www.raritan.com) oder rufen Sie uns an: Tel. +31(0)10 284 40 40.