

Windows IT Pro

Das Magazin für den Windows-Administrator

Server-Konsolidierung

Anwendungen in der Sandbox

KVM-Switch:

Direkt oder auf Distanz

Virtualisierung:

Möglichkeiten & Grenzen

TOOLKIT

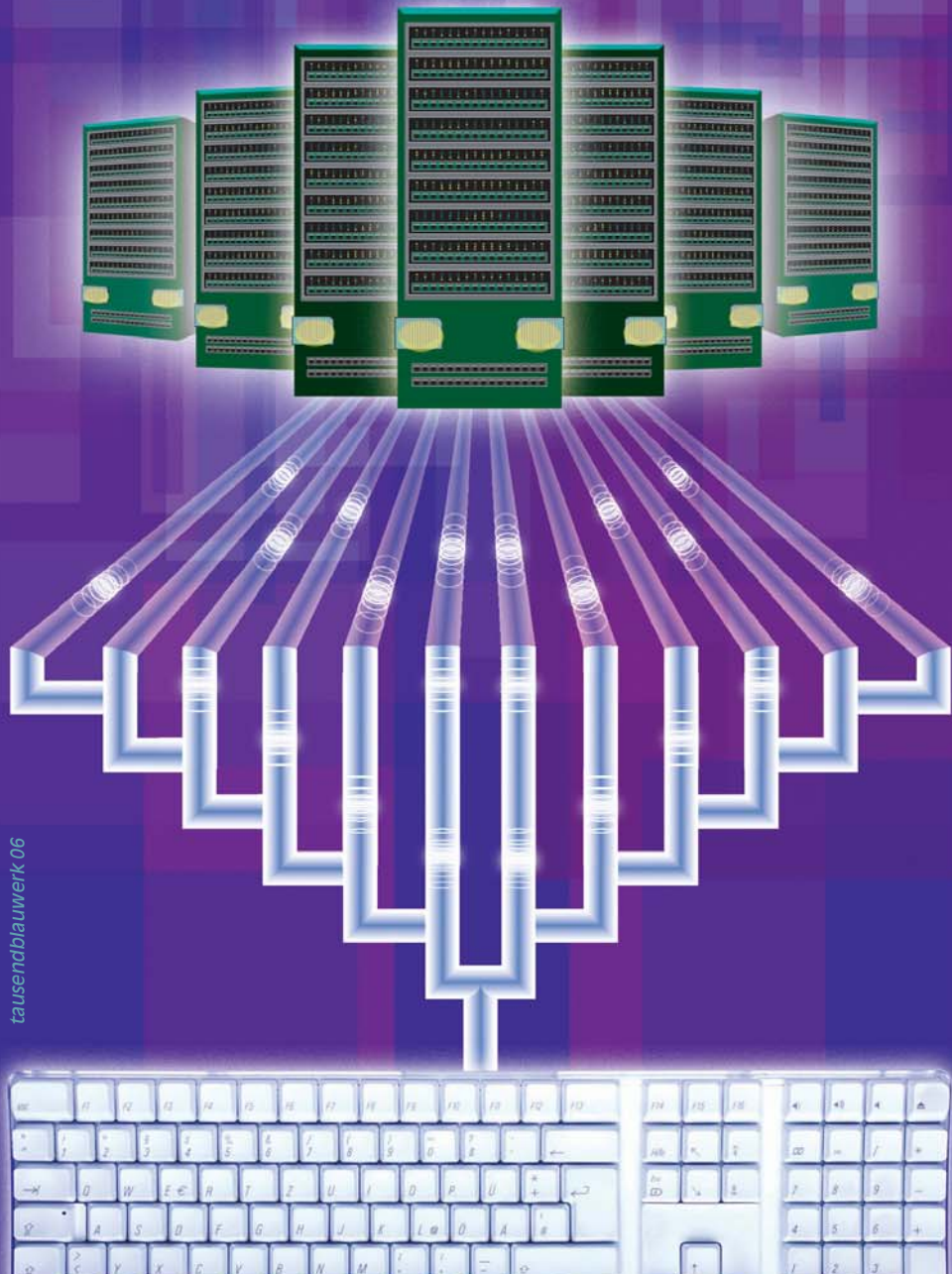
- Grundlagen für die Fehlersuche im DNS
- Die Ereignisanzeige im Griff: Alle Vorkommnisse schnell finden

SPECIAL

- Scan&Block hilft den Netzwerken
- Rights Management Services (RMS) in der Praxis

LAB-REPORT

- Festplattenmanagement: Teilen & Herrschen
- Sicherheitsanalyse: Schwachstellen im Blick
- Alternative für das Office



tausendblauwerk 06

**Sonderdruck für
Guntermann & Drunck GmbH**

Direkt oder mit Distanz

von Thomas Bär

Während sich viele Probleme im Tagesgeschäft eines Administrators mit Hilfe eines Skripts oder durch einen Batch-Job automatisieren lassen, existieren doch eine ganz Reihe von Aufgaben, die einen direkten Zugriff auf die Rechner im Serverraum erfordern: Hier können die KVM-Systeme eine deutliche Arbeitserleichterung darstellen.

Kaum ein Administrator würde jeden Server im Serverraum mit Tastatur, Maus und Monitor ausstatten: Häufig kommen dann die so genannten KVM-Switches (Keyboard, Video, Mouse) zum Einsatz, die Eingabe- und Bildsignale zwischen Arbeitsplatz und Servern übertragen. Es gibt aber auch eine große Anzahl von Software-Tools, die einem Administrator den Zugriff auf entfernte Server- oder Workstationssysteme ermöglichen. So waren VNC-Server und -Viewer noch zu Zeiten der Windows-NT-Server aus kaum einer Serverumgebung wegzudenken. Inzwischen wird dieser „Urvater der Fernübertragung von Bildschirmhalten“ aber immer häufiger von Softwarelösungen verdrängt, die das in Windows standardmäßig zur Verfügung stehende „Remote Desktop Protocol“ (RDP) einsetzen.

Fernwartung per Software – bewährte Lösungen vorhanden. Diese Art der Software-basierenden Fernwartung ist zwar grundsätzlich sehr flexibel und wird aus diesem Grund auch häufig in der Praxis eingesetzt, aber auch solche Lösungen haben ihre Grenzen: Beispielsweise muss das entsprechende Betriebssystem einwandfrei funktionieren, damit ein Serversystem überhaupt über RDP angesprochen werden kann. Das Aufsetzen eines neuen Betriebssystems ist nur durch den Zugriff auf die „echte Konsole“ möglich. Zudem ist in den verschiedensten Foren im Internet immer wieder zu lesen, dass eine Reihe von Softwareinstallationen nur dann wirklich erfolgreich verläuft, wenn der Anwender auch wirklich direkt mit dem Rechner verbunden ist.

Neben den typischen Windows-Servern existieren aber noch eine ganze Reihe von Szenarien, bei denen eine Softwarefernwartung komplett unmöglich ist: Dazu gehören unter anderem Rechnersysteme, die

nicht über das normale Firmennetzwerk angesprochen werden können, spezielle Maschinensteuerungen, aber auch viele Systeme in der Studioteknik. Hier ist der Einsatz von KVM-Technik dann die einzige Alternative, wenn sich der Systemverwalter nicht für jede Änderung selbst zum Rechner begeben will oder kann.

dabei für die meisten Systemverwalter sicher die interessantere Variante, da diese verschiedene Vorzüge gegenüber der direkten analogen Übertragung zu bieten hat: So ist beispielsweise keinerlei Zusatzhardware am Arbeitsplatz des Bedieners erforderlich. Da auf eine feste Verkabelung mit den speziellen Kabeln verzichtet wer-

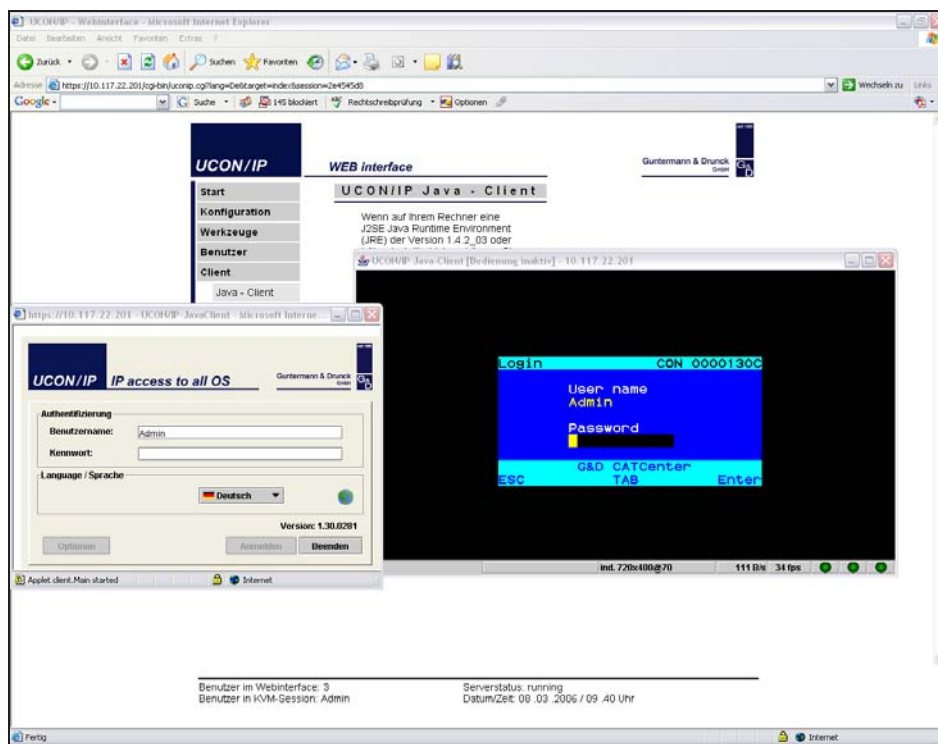


Bild 1. Management auf verschiedenen Wegen: KVM-Systeme von G&D lassen sich sowohl per „On Screen Display“ (OSD) oder per Software verwalten.

Zugriff per KVM: digital oder analog? Grundsätzlich wird beim Einsatz dieser Technik zwischen analoger und digitaler Übertragung der KVM-Signale unterschieden. Das Thema „KVM-over-IP“, also die digitale Übertragung von KVM-Informationen über das normale IP-Netz, ist

den kann, ist der Anwender zudem auch vom Einsatzort unabhängig. Die maximale Distanz zwischen dem Anwender und der zu steuernden Maschine ist quasi unbegrenzt, da viele Geräte entweder über VPN- oder direkt über ISDN-Zugänge angesteuert werden können.

Aber der große Vorteil der digitalen Übertragung – der Transport über das echte Netzkabel – hat auch negative Aspekte: So belasten die KVM-Signale die Bandbreite der regulären Verkabelung, und zudem besteht bei Einsatz dieser Technik generell ein gewisses Sicherheitsrisiko, da auch die Anmeldeinformationen wie Passwörter über diesen Weg transportiert werden müssen. Bei der analogen Übertragung hingegen handelt es sich um eine dedizierte 1:1-Verbindung zwischen Anwender und Rechner. Es kommt auf diese Weise zu keinerlei Latenzen beim Zugriff und die Performance entspricht der realen Darstellungsgeschwindigkeit auf dem Zielrechner. Da bei der analogen Übertragung eine eigene Verkabelung eingesetzt wird, ist diese Methode von Haus aus als sicherer einzustufen, wenn es um das Abhören der Signale durch unberechtigte Dritte geht.

KVM in der Praxis: Komplettsset für digitale und analoge Zugriffe. Die Firma Guntermann & Drunck aus dem Siegerland befasst sich schon seit 1985 mit der Entwicklung und Produktion von KVM-Systemen. Für diesen Praxistest stellte G&D der Windows IT Pro ein Komplettsset bestehend aus dem KVM Matrix-Switch „CATCenter X8“, einer analog/digitalen User Console mit der Bezeichnung „UCON/IP“ und einer analogen User Console, die den Namen „UCON/s“ trägt, zur Verfügung.

Während bei vielen einfachen KVM-Lösungen die PS/2- und VGA-Signale über lange Kabel direkt mit dem Switch verbunden werden, basieren die Geräte von G&D auf standardmäßigen CAT5/6/7-Kabel. Am Rechner selbst wird dabei ein so genannter Server-Anschluss-Dongle verwendet, wobei der Hersteller vier unterschiedliche Varianten für den Einsatz mit klassischer PS/2- oder Standard-USB-Peripherie sowie zwei USB-Typen für den Betrieb an Sun-Servern mit jeweils deutschem und US-amerikanischem Tastatur-Layout anbietet. Wenn es darum geht, einen Rechner direkt über zwei KVM-Switches anzusteuern, so lässt sich dies mit dem „CATPRO2/UC“ erreichen, der rückseitig über zwei RJ45-Buchsen für den Anschluss der CAT-Kabel verfügt. Sind die Serversysteme mittels Teleskopschienen im Rack eingebaut, so ist der „CATPRO2/extended“ mit einem 120 Zentimeter langen Anschlusskabel eine Alternative. Die Stromversorgung der Server-Anschluss-Dongles geschieht direkt über den PS/2- beziehungsweise den USB-Anschluss. In Abhängigkeit vom verwendeten CAT-Kabel lässt sich eine maximale Videoauflösung von 1920 x 1440 Pixel bei 75 Hz Bildschirmwiederholungs-frequenz erzielen.

Die Produktpalette von G&D umfasst verschiedenste Geräte vom zweifachen Umschalter bis hin zu mehrfach skalierbaren KVM-Switches. Das getestete CATCenter X8 ist ein zentraler KVM-Matrix-Switch für den Anschluss von bis zu 32 Servern und acht Konsolen bei einer Bauhöhe von einer Höheneinheit in einem stabilen Metallgehäuse. Durch eine mögliche Kaskadie-

nach diesem Wechsel problemlos über die KVM-Geräte ansprechen. Einer unserer Linux-Testrechner älteren Baudatums verfügt nur über einen fünfpoligen DIN-Anschluss für die Tastatur, sodass hier ein Adapter von DIN nach PS/2 zum Einsatz kam, während das Mausekabel des Dongles direkt mit dem PS/2-Mauseanschluss verbunden wurde. Auch diese uns zunächst et-

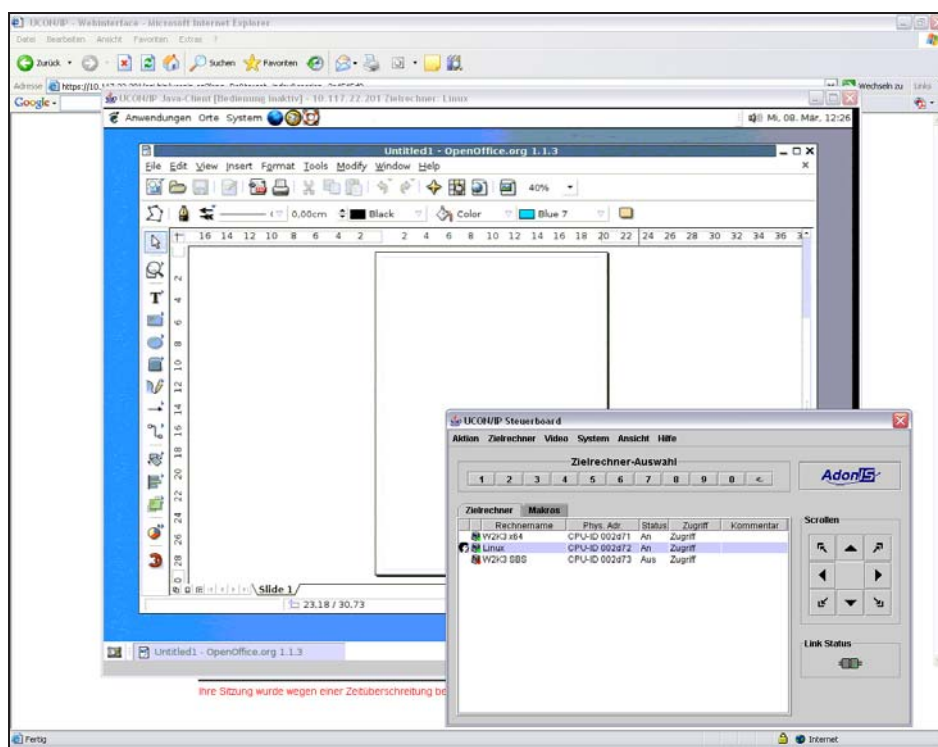


Bild 2. Als wäre man vor Ort: Der KVM-Zugriff, der digital über das IP-Netz erfolgt, gibt dem Anwender das Gefühl, auf lokalen Systemen zu arbeiten..

zung lässt sich die maximale Anzahl von zu steuernden Rechnern auf bis zu 512 Maschinen ausweiten. Für den Test wurden drei Testrechnersysteme über die CAT-PRO2-Dongles an das CATCenter angeschlossen.

Verkabelung und Zugriff: schneller Anschluss und einfache Bedienung.

Die Verkabelung selbst fällt erfreulich einfach aus. Die PS/2-Maus/Tastatur-Anschlüsse und der VGA-Ausgang werden mit dem Dongle verbunden, während dieser dann über das beiliegenden CAT-Patch-Kabel mit dem Switch verbunden wird. Bei einem Dell-Server mit Windows Server 2003 SBS-Installation wählten wir anstelle des PS/2- einen USB-Dongle, obwohl das System sonst stets über den klassischen Anschluss angesprochen wurde. Sowohl Windows, als auch die KVM-Geräte von G&D spielten bei dieser Konfigurationsänderung gut zusammen. Obwohl nie zuvor per USB angesteuert, ließ sich der Server

was ungewöhnlich erscheinende Konfiguration wirkte sich beim späteren Zugriff über das Netzwerk in keiner Weise negativ aus.

Die CATCenter-KVM-Switches selbst verfügen über keinerlei Anschlussmöglichkeit für Monitor, Tastatur und Maus, wie man es von „klassischen“ KVM-Switches her gewohnt ist. Für den Zugriff auf den Switch kommen bei diesen Geräten spezielle Konsolen zum Einsatz, die der Hersteller „UCON“ nennt. Je nachdem für welches Einsatzgebiet ein Gerät verwendet wird, können unterschiedliche Konsolen genutzt werden: So lässt sich beispielsweise der direkte Arbeitsplatz des Administrators mit einer UCON/s ausstatten. Diese analoge Konsole bietet den Zugriff auf ein CATCenter und zudem die Möglichkeit, bis zu zwei lokale Workstations mit Hilfe von CAT-PRO2-Dongles direkt anzuschließen. Bei einer solchen Konfiguration wäre es dann also möglich, den Arbeitsplatz des Administrators mit nur einem einzigen Monitor zu

betreiben. Die maximale Distanz zwischen einem Dongle und einer Konsole beträgt in Abhängigkeit von der Auflösung und dem verwendeten Kabel maximal 300 Meter.

Der Weg übers Netz durch die digitale Konsole. Eine andere „Konsolenvariante“ stellt die digitale Version UCON/IP dar. Sie bietet nicht nur den direkten analogen Zugriff auf den KVM-Switch, sondern hier kann der Administrator auch mit Hilfe eines Java-fähigen Browsers auf den Switch zugreifen. Laut Hersteller kommt dabei auf diesen Geräten eine bereits im Vorfeld entwickelte KVM-over-IP-Technik namens Acxos zum Einsatz.

Um auf Rechnersysteme zuzugreifen, die an den Switch angeschlossen sind, muss ein Java-Programm in einem Browserfenster geöffnet werden. Dieser Java-Client steht für Microsoft Windows ab der Version NT 4.0, Suns Solaris 8/9 und für die Linux-Distributionen FedoraCore, SuSE/Novell und Debian zur Verfügung. Die Konsole hat zudem einen ISDN-Anschluss, über den sich auch bei einem Totalausfall des Netzwerks ein Fernzugriff auf die Systeme realisieren lässt. Vergleicht man Bildqualität und subjektive Übertragungsgeschwindigkeit kann bei solch einer IP-basierenden Übertragung von Bildinformationen mit den entsprechenden Werten einer analogen 1:1-Verbindung, so wird man feststellen, dass die Qualität der IP-basierten Übertragung mit der einer 1:1-Verbindung nicht mithalten kann. Allerdings ist hier auch bei geringer Bandbreite der Netzwerkverbindung immer noch ein problemloses Arbeiten möglich.

Konfiguration: OSD oder Konfigurationssoftware. Drückt der Administrator am Arbeitsplatz die Standard-Hotkey-Kombination „STRG+NUM“, so erscheint auf dem Monitor das so genannte OSD-Menü (On Screen Display) des CATCenters. Der Hersteller nennt es auch „Advanced On Screen Information System“ (AdonIS), weil es mehr leisten kann, als man dies von einem Steuerungsfenster eines Monitors gewohnt ist. Bevor jedoch eine Änderung der Konfiguration oder ein Zugriff auf die angeschlossenen Server möglich wird, muss sich der Anwender auch hier zunächst identifizieren.

Angenehmer als über AdonIS lässt sich das CATCenter aber mit der speziellen Konfigurationssoftware administrieren. Dafür weist der Admin dem CATCenter zunächst über AdonIS eine IP-Adresse zu. Danach kann er dann mit der XView-Software weiterarbeiten. Diese bietet nicht nur eine übersichtlichere Darstellung als das OSD, sondern es ist hier auch möglich, Konfigurationen zu

speichern und wiederherzustellen. Zudem arbeitet die Software sehr praxisnah: Verändert der Admin auf diese Weise beispielsweise das Standard-Gateway, oder die IP-beziehungsweise DNS-Einträge, verlangt das Gerät eine Anmeldung des Administrators innerhalb der nächsten fünf Minuten. Erfolgt diese Anmeldung nicht, so geht das Gerät davon aus, dass eine unerreichbare Konstellation eingetreten ist und stellt selbstständig den vorherigen Zustand der Konfiguration wieder her.

Das CATCenter stellt sehr umfangreiche Einstellungsmöglichkeiten zur Verfügung. Neben dem Benutzermanagement mit unterschiedlichen Konstellationen von Zugriffsberechtigungen, einer Integration in Netzwerkverzeichnisdienste wie Active Directory oder LDAP, lassen sich auch „Log Out“-Zeiten oder Hotkeys nach eigenen Vorstellungen anpassen. Weitere Netzwerkfunktionen runden das positive Gesamtbild ab. So lassen sich beispielsweise Statusinformationen an einen Syslog-Server übersenden oder Maschinen per Wake-On-LAN aufwecken. Aber auch andere Konfigurationen lassen sich neben den Netzwerkeinstellungen sehr detailliert festlegen: So ist es unter anderem möglich, den im CATCenter angezeigten Rechnernamen eines angeschlossenen Servers oder auch die Positionierung des Infotextes bei der Umstellung per Hotkey, OSD-

Menü oder Autoscan frei einzustellen. Es gehört zu den unbedingten Voraussetzungen für professionelle KVM-Geräte, dass sich in das Sicherheitskonzept eines Unternehmens einbinden lassen müssen, da es hier immer auch um den Zugriff auf sicherheitskritische Systeme geht. Um eine redundante Stromversorgung zu gewährleisten, hat das Gerät ein externes zweites Netzteil, das mit einem vierpoligen Mini-DIN-Stecker als sekundäre Stromversorgung angeschlossen wird. Beim Betrieb dieser KVM-Systeme fällt zudem angenehm auf, dass sie im Betrieb sehr leise sind. Dies liegt unter anderem daran, dass im Gerät-eineren Notebook-Technik in Form von Intel Pentium-M-Prozessoren zum Einsatz kommt, was eine aktive Kühlung unnötig macht.

Das Sicherheitskonzept: Betriebs-sicherheit und Zugriffsschutz. Diese Bauweise stellt einen weiteren Pluspunkt bei der Betriebssicherheit dar: Wo kein Lüfter ist, kann auch keiner ausfallen. Ein weiteres „klassisches“ bewegtes Bauteil mit der Tendenz zum Ausfallen ist eine Festplatte. Auch hier wurde vorgesorgt, da in diesen KVM-Systemen nur Compact-Flash-Module zur Speicherung von Informationen eingesetzt werden. Der konsequente Einbau von doppelt vorhandenen Netzwerkkarten stellt einen weiteren Schritt in Richtung erhöhter Betriebssicherheit dar, weil sich die Geräte auf diese Weise in zwei unterschiedliche Netzwerkstrukturen einbinden lassen. Abgerundet wird das Sicherheitskonzept durch die Unterstützung aktueller Techniken einer 128-Bit SSL-Verschlüsselung der IP-Verbindung, dem automatischen Log-Out bei fehlender Aktivität seitens des Anwenders und frei definierbare Benutzer mit unterschiedlichen Zugriffsrechten. Die von uns getesteten Geräte hinterließen im praktischen Einsatz einen durchwegs positiven Eindruck, wobei besonders der gute Aufbau und die einfache Bedienung der Systeme hervorzuheben sind. Die mitgelieferten gedruckten Handbücher sind von außerordentlich guter Qualität und beschreiben alle Funktionen sehr genau. Die Verfasser haben dabei auch auf entscheidende Details aus dem Tagesgeschäft geachtet: So werden beispielsweise die Anmeldeinformationen mit dem Standardpasswort nicht irgendwo mitten im Text genannt, sondern finden sich im Anhang auf einer separaten Seite. Diese Seite kann nach Inbetriebnahme entfernt und sicher verwahrt werden. So stellen dann auch die im Schrank verstauten Handbücher kein Risiko mehr dar, falls das vorkonfigurierte Passwort nicht geändert wurde. (fms)

KVM-System



Hersteller:
Guntermann & Drunck GmbH
Telefon 02739 / 8901100
<http://www.GDsys.de>

Preise:
CATPRO2 Dongle 162,40 Euro
CATCenter X8 5742,00 Euro
UCON/s 1276,00 Euro
UCON/IP 3654,00 Euro

Pro:

- ausgereiftes KVM-Konzept
- einfache Inbetriebnahme
- Sicherheit durch Redundanzen

Kontra:

- IP-Übertragung spürbar langsamer als 1:1 Verbindung