Raritan.
Know more. Manage smarter.™

Das dezentral organisierte Unternehmen:
Remote-Zugriff und Verwaltung von IT-Infrastrukturen

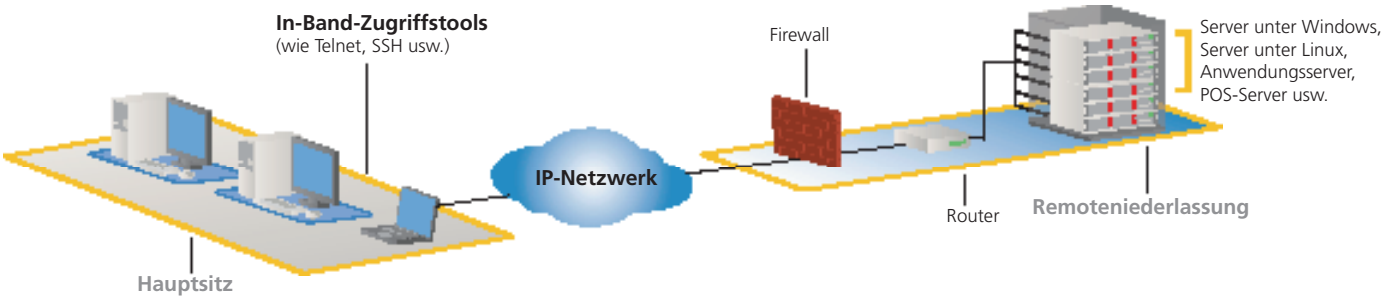
Überblick

Einerseits gilt die wachsende Zahl von Zweig- und Remoteniederlassungen eines Unternehmens als positives Zeichen für das Wachstum des Unternehmens, auf der anderen Seite kann diese Entwicklung für die Mitarbeiter der IT-Abteilung jedoch eine große Herausforderung darstellen. Neben der Verwaltung von Rechenzentren sehen sich IT-Teams mit zusätzlichen Aufgaben wie dem Verwalten und Reparieren der Ressourcen der Zweigniederlassungen (wie Router, Switche, Firewalls, WAN-Optimierungen und Server) konfrontiert. An diesen Remotestandorten beschäftigte Mitarbeiter verfügen in der Regel nicht über die zur Problembehebung erforderlichen IT-Kenntnisse. Aus diesem Grund greift eine Vielzahl von IT-Abteilungen bei der Diagnose und Behebung von Problemen an Remotestandorten auf Fernzugriffssoftware zurück. Diese Tools sind jedoch nur dann von Nutzen, wenn Betriebssystem und Netzwerk ordnungsgemäß funktionieren. Ist das Netzwerk oder das Betriebssystem nicht verfügbar, muss möglicherweise ein Mitarbeiter vor Ort gebeten werden, sich des Problems direkt am Serverschrank anzunehmen. Lässt sich das Problem auf diese Weise nicht beheben, entstehen durch Anreise, Arbeitszeiten und entgangene Gewinne möglicherweise zusätzliche Kosten.
Dieses Dokument erläutert die Vorteile von Out-of-Band-Zugriff und Steuerungstools für Zweigniederlassungen (in puncto Verfügbarkeit und Sicherheit).

Herausforderungen in Zweigniederlassungen

Die Internet Research Group schätzt, dass es alleine in den USA mehr als 1,5 Mio. Niederlassungen gibt, die direkt mit dem Hauptsitz kommunizieren. Und hierbei nicht berücksichtigt sind Terminals, Bankautomaten sowie andere SB-Transaktionsstandorte.
Die Einrichtung von Zweigniederlassungen führt zwar zu einer Vergrößerung der Reichweite des Unternehmens, sie bringen jedoch auch höhere Belastungen für die IT-Manager mit sich, die für das Installieren, Überwachen und Warten der technischen Ressourcen an den unterschiedlichen Standorten zuständig sind. Zu diesen Ressourcen zählen beispielsweise Netzwerkgeräte wie Router, Switche, WAN-Optimierungen und Firewalls. Aber auch verteilte Anwendungs- und Speicherserver für Transaktionen und E-Mails können zu diesen Ressourcen gerechnet werden.
Die Herausforderungen, die sich bei der Verwaltung von Remoteniederlassungen ergeben, lassen sich in den folgenden vier grundlegende Kategorien zusammenfassen:

Steuerung und Komplexität: Netzwerke von Remoteniederlassungen können sich aus einer Reihe verschiedenartiger Komponenten – also verschiedener Geräte von unterschiedlichen Herstellern – zusammensetzen. Die zunehmende Komplexität dieser Netzwerke führt dazu, dass vermehrt Befürchtungen vom Auftreten von Fehlern sowie zu deren Behebung angestellt werden. Und bei hunderten oder gar tausenden IT-Ressourcen auf der ganzen Welt kann immer weniger auf eine zentralisierte Verwaltungsschnittstelle für diese Geräte verzichtet werden.
Sicherheit: In vielen Zweigniederlassungen – insbesondere bei Einzelhandelsfilialen und Banken – sind sensible Kundendaten und/oder Kreditkartendaten gespeichert, die ohne geeignete Schutzmaßnahmen im Falle eines Eindringens gefährdet sein können. Der vermehrte Einsatz von Wi-Fi in Zweigniederlassungen verschärft dieses Sicherheitsproblem zusätzlich.
Begrenzte finanzielle Mittel und Ressourcen: Remoteniederlassungen verfügen in der Regel nicht über eine eigene IT-Abteilung. In diesem weit verbreiteten Szenario obliegt das Diagnostizieren und Beheben von Netzwerk und Serverproblemen den IT-Administratoren am Hauptsitz. Da die Behebung von Problemen von Zeit zu Zeit auch die Anwesenheit vor Ort erforderlich macht, können sich die mittlere Reparaturdauer (Mean Time To Repair, MTTR) sowie die Betriebskosten erhöhen, da Reisekosten entstehen. Eine weitere Option besteht im Beauftragen eines Dienstleisters, der die Behebung vor Ort vornimmt. Doch auch diese Möglichkeit ist zumeist mit hohen Kosten verbunden. Handelt es sich um ein schwer wiegendes Problem, das umgehend behoben werden muss, kommt eine Anreise möglicherweise gar nicht in Frage. Für Abhilfe sorgen hier Fernzugriffstools zum Zugriff auf und Beheben von IT-Problemen einer Zweigniederlassung. Die meisten Fernzugriffslösungen teilen sich in In-Band- und Out-of-Band-Kategorien auf.



In-Band-Zugriffsoptionen

Remoteverwaltungssoftware: Diese Art von Lösung ermöglicht IT-Administratoren den Zugriff auf den Desktop sowie auf Anwendungen des Zielservers. Ein deutlicher Nachteil von Remoteverwaltungssoftware besteht darin, dass sie nur verwendet werden kann, wenn das Zielbetriebssystem verfügbar ist. Reagiert das Betriebssystem nicht mehr, oder ist es abgestürzt, ist der Zugriff auf den Server nicht möglich. Darüber hinaus sind diese Softwarelösungen von einer Verbindung mit der Netzwerkkarte des Zielservers abhängig. Auch hier gilt: Ist das Netzwerk nicht verfügbar, lässt sich das Problem nicht beheben.

Tabelle 1 veranschaulicht die Lücke zwischen Remotezugriffssoftware und Out-of-Band-Optionen wie KVM-over-IP.

	In-Band	Out-of-Band
Aufgaben	**Remotezugriffssoftware**	**KVM-over-IP**
Remotezugriff auf Server	✓	✓
Zugriff auf BIOS-Ebene	✗	✓
Zugriff per DFÜ-Verbindung bei Nichtverfügbarkeit des Netzwerks	✗	✓
Benutzerprofile, Berechtigungen auf Portebene	✗	✓
Unterstützung mehrerer Benutzer, gleichzeitige Sitzungen	✗	✓
Warmstart	✓	✓
Kaltstart	✗	✓*
Protokollierung	✗	✓

*Bei Verwendung mit Remote-Stromzufuhrsteuerung

Tabelle 1

Terminal-Emulationsprotokolle: Für den Zugriff auf Geräte mit serieller Schnittstelle (wie Router, Switche, Firewalls, Power Distribution Units und Server) werden Telnet und das entsprechende verschlüsselte Gegenstück SSH verwendet. Ebenso wie bei der Remoteverwaltungssoftware ist diese Zugriffsmethode nur bei vorhandener Netzwerkverbindung effektiv. Sollte ein Problem mit dem WAN vorliegen, muss sich möglicherweise ein IT-Experte vor Ort damit auseinandersetzen. Darüber hinaus werden die Zweigniederlassungen aufgrund dieser Wartungsschnittstellen anfälliger für unbefugten Netzwerkzugriff, da diese Schnittstellen auch von Hackern zum Stehlen von Daten sowie zum Einschleusen von Viren verwendet werden können.

Die Sicherheitsvorteile einer Out-of-Band-Alternative wie einem sicheren Konsolenserver sind in Tabelle 2 dargestellt.

	In-Band		Out-of-Band
Aufgaben	**Telnet**	**SSH**	**Sicherer Konsolenserver**
Sichere Appliance	✗	✗	✓
Zugriff per DFÜ-Verbindung bei Nichtverfügbarkeit des Netzwerks	✗	✗	✓
Verschlüsselung	✗	✓	✓
Anpassung von TCP-Ports	✗	✗	✓
Sicheres Kennwort	✗	✗	✓
Sperrung bei wiederholter Kennworteingabe	✗	✗	✓
SYSLOG	✓	✓	✓
Erfassung von Tastatureingaben	✗	✗	✓
Sicherheitsbanner bei der Anmeldung	✗	✗	✓

Tabelle 2

Out-of-Band-Optionen

Sichere Konsolenserver: Der gemeinsame Nenner der meisten IT-Bereitstellungen für Zweigniederlassungen ist die Netzwerkverbindung, für die üblicherweise ein Router, ein Switch sowie eine Firewall benötigt werden. Fällt eine dieser Komponenten an einem Remotestandort aus, kann sich dies negativ auf das Unternehmen auswirken. Die Mehrzahl der Netzwerkgeräte verfügt über eine serielle Schnittstelle, und für den Zugriff und die Wartung wird – wie weiter oben bereits erwähnt – üblicherweise auf In-Band-Tools wie SSH und Telnet gesetzt. Bei Auftreten eines Problems mit dem Netzwerk lassen sich diese Zugriffstools jedoch möglicherweise gar nicht verwenden. Sichere Konsolenserver (Secure Console Servers, SCSs) bieten über SSH/Telnet und den Webbrowser Remotezugriff auf mithilfe der seriellen Schnittstelle verwaltete Server und andere serielle Geräte. Einer der Vorteile des SCSs: Hierbei handelt es sich um einen zentralen Zugriffs- und Steuerungspunkt für mithilfe der seriellen Schnittstelle verwaltete WAN- und Netzwerkgeräte sowie für Geräte zur Stromzufuhrsteuerung. Ein weiterer Vorteil besteht in der Möglichkeit zum Herstellen einer Modem-Verbindung, falls das WAN nicht verfügbar sein sollte. Dadurch muss sich der IT-Experte nicht extra an den Remotestandort begeben, was wiederum eine schnellere Reparatur ermöglicht.

Was bei der Auswahl eines Konsolenservers berücksichtigt werden sollte:

- Rechte und Authentifizierung
  - Lokale Konten
  - Zugriff auf Portebene
  - Sichere Kennwörter
  - Unterstützung von Active Directory, LDAP, RADIUS, TACACS+
- Konsolenfeatures
  - Protokollierung
  - SNMP-Traps
  - Solaris-Schlüsseltrapping
  - Shared access
- Management Features
  - E-mail Benachrichtigungen
  - SNMP Support
- Verwaltungsfeatures
  - SSH
  - Telnet
  - Webschnittstelle
  - DFÜ-Option
- Umgebungsverwaltung
  - Zwei Netzteile
  - Stromzufuhrverwaltung
  - CAT5-Verkabelung

"Ein Fehler in unserem Unternehmen führte vor einiger Zeit dazu, dass unsere Firewall nicht mehr funktionierte. Daraufhin konnte über das Netzwerk keine Verbindung mehr hergestellt werden. Das Ende vom Lied: Wir mussten jemanden an den Standort schicken, um den Server per Konsolenzugriff neu zu starten. Hätten wir damals schon den Dominion® SX verwendet, wäre das Problem in wenigen Minuten behoben gewesen. Ich glaube, das war das Ereignis, das uns deutlich vor Augen geführt hat, wie wertvoll die serielle sichere Konsolenserverlösung von Raritan für unsere IT-Infrastruktur ist."

Kevin Byrne
Network Operations Engineer,
Charter Communications

KVM-over-IP: KVM-Switche bieten Zugriff auf Server sowie die Möglichkeit zum Steuern von Servern, die über eine Schnittstelle für Tastatur/Video/Maus verfügen. Durch ihren Einsatz wird dem Anwender der Eindruck vermittelt, sich direkt im Rechenzentrum zu befinden und dort auf den Server zuzugreifen.

KVM-über-IP-Switche bieten die gleichen Funktionen, verwenden jedoch eine sichere IP-Verbindung. Ein deutlicher Vorteil ist hierbei die Möglichkeit des ortsunabhängigen Serverzugriffs, die diese Methode zur idealen Zugriffs- und Steuerungslösung für die Server einer Zweigniederlassung macht. Ganz gleich, ob sich der zuständige IT-Administrator in der Hauptniederlassung befindet oder um zwei Uhr morgens zu Hause sitzt, während draußen ein Schneesturm tobt: Er hat immer Zugriff auf die Ressourcen der Zweigniederlassung.

Darüber hinaus verfügen KVM-über-IP-Switche sowohl über In-Band- als auch über Out-of-Band-Zugriff. Mit anderen Worten: Die Mitarbeiter der IT-Abteilung haben die Möglichkeit, den Zugriff auf die Server sowie deren Steuerung auf Betriebssystem-/Anwendungsebene vorzunehmen. Sollte das Betriebssystem nicht reagieren, steht immer noch die BIOS-Ebene zur Verfügung. Darüber hinaus sind KVM-über-IP-Switche mit einem integrierten Modem ausgestattet, das im Falle eines Netzwerkausfalls eine alternative Zugriffsmethode per DFÜ-Verbindung bietet.

Weitere praktische Features wie Virtual Media ermöglichen den Mitarbeitern der IT-Abteilung das Übertragen von auf dem Desktop, auf CD-ROMs oder auf USB-Sticks gespeicherten Dateien an Server auf der ganzen Welt. Dieses Tool eignet sich perfekt für Upgrades und Patches, die an einer Vielzahl von Remotestandorten installiert werden müssen.

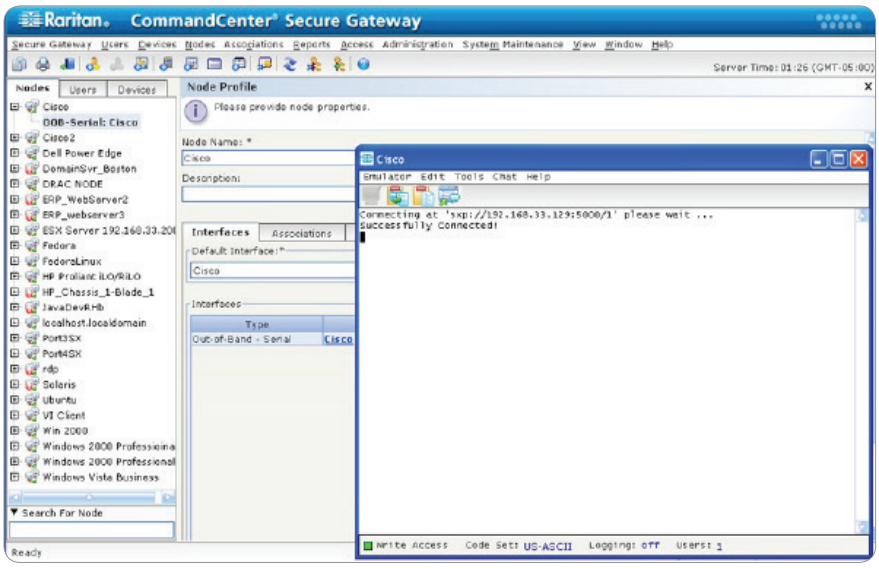
Im KVM-über-IP-Verbraucherratgeber werden die folgenden Aspekte aufgeführt, die bei der Auswahl eines Switches berücksichtigt werden sollten:

- Echter zeit- und ortsunabhängiger Zugriff auf Ressourcen
  - Unterstützung mehrerer Plattformen
  - Browser-/Desktopkompatibilität
  - IP- und DFÜ-Zugriff
  - Kostenloser, herunterladbarer Client
  - Unblockierter Zugriff über lokale Ports
  - Vollständige Stromzufuhrsteuerung per Remote Power Control
  - Virtual Media-Zugriff
- Hohe Sicherheit und Leistung
  - Auf ein Minimum reduzierte Anfälligkeit
  - Steuerung des externen und internen Zugriffs
  - Syslog-Unterstützung
  - Datenverschlüsselung
  - Unterstützung sicherer Kennwörter
- Anwendungs-basierte Lösungen
  - Implementierung
  - Größe und Portdichte
  - Zuverlässigkeit und Verfügbarkeit

Intelligente Power Distribution Units: In manchen Fällen lässt sich ein Problem nur noch durch einen Kaltstart beheben. Während schaltbare Power Distribution Units (PDUs) üblicherweise mit dem Neustart per Fernzugriff in Verbindung gebracht werden, sind einige PDUs mit Features ausgestattet, die die Verwendung zusätzlicher Überwachungsfunktionen ermöglicht. In einer Zweigniederlassung, in der sich die IT-Geräte üblicherweise in einem Schrank oder in einem kleinen Raum befinden, ist es besonders wichtig, dass bei Überschreiten der für Umgebungsfaktoren oder für den Stromverbrauch festgelegten Schwellenwerte eine entsprechende Benachrichtigung ausgegeben wird. So lassen beispielsweise Luftzirkulation und Kühlung in kleinen Büros häufig zu wünschen übrig, und meist ist auch nur eine Sicherung vorhanden, durch die auch andere Geräte gesichert sind. Durch die Überwachung der Temperatur innerhalb des Schranks sowie durch die Überwachung des Stromverbrauchs lässt sich möglicherweise einem Ausfall oder einer Beschädigung der Geräte vorbeugen.

Bei der Auswahl einer Lösung für die Stromzufuhrverwaltung per Remotezugriff sollten folgende Faktoren berücksichtigt werden:

- Serieller Remote- und TCP/IP-Zugriff zur Schaltung auf Portebene
- Benutzerkonfigurierbare Verzögerungen auf Portebene für kontrolliertes Hoch- und Herunterfahren der Stromversorgung (Power Sequencing)
- Informationen zum Stromverbrauch auf Geräte- und Portebene
- Benutzerdefinierte Schwellenwerte
- Warnhinweise per SNMP, E-Mail und Syslog bei Überschreitung von Schwellenwerten
- AES-Verschlüsselung mit bis zu 256 Bit und Unterstützung sicherer Kennwörter
- Erweiterte Autorisierungsoptionen einschließlich der Berechtigungen für die Portebene sowie LDAP/S, RADIUS und Active Directory®
- Unterstützung von HTTP, HTTPS, IPMI, SMASH-CLP, SSH, Telnet und SNMP

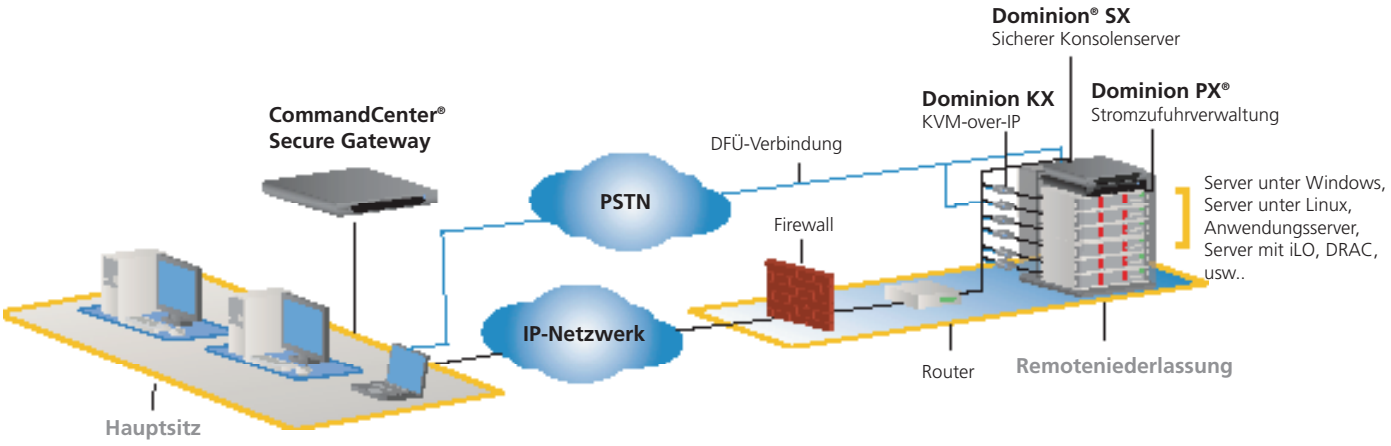


Beispielbildschirm aus CommandCenter® Secure Gateway. Diese Lösung bietet zentralisierten Zugriff auf IT-Geräte sowie entsprechende Verwaltungsfunktionen.

Zentralisierte Verwaltung: Die Verwaltung dutzender, hunderter oder gar tausender Standorte kann eine respekteinflößende Aufgabe darstellen. Selbst bei Verwendung von KVM-über-IP, sicheren Konsolenservern, Embedded Service Processors (iLO, DRAC, RSA) und intelligenten PDUs für die Problembehebung per Remotezugriff müssen sämtliche verschiedenartigen Ressourcen in einer kombinierten Anzeige überwacht werden können. Denken Sie an eine zentralisierte Verwaltungslösung mit Unterstützung einer breiten Palette von Geräten sowie mit fortschrittlichen Sicherheits- und Autorisierungsfunktionen.

Fazit

Zwar gibt es keinen adäquaten Ersatz für einen vor Ort befindlichen IT-Experten, der die Dinge am Laufen hält, dies ist jedoch ein Luxus, den sich nur die wenigsten Unternehmen leisten können. Die zweitbeste Lösung besteht in der Verwendung geeigneter Tools zur Ausdehnung der Reichweite der am Hauptsitz tätigen IT-Mitarbeiter auf die Remotestandorte des Unternehmens. Während einige dieser Tools derzeit scheinbar sehr günstig oder gar kostenlos zu haben sind, ergeben sich die Kosten bei diesen Produkten durch Abstriche bei Verfügbarkeit und Sicherheit. Das Ergebnis sind möglicherweise unerwartete Reisekosten und Ausfallzeiten, also eben jene Aspekte, die durch den Einsatz von Fernzugriffslösungen vermieden werden sollen. Die Lücken, die sich durch die Verwendung von In-Band-Zugriffstools ergeben, lassen sich am besten mit Out-of-Band-Lösungen schließen. Weitere Informationen zur hilfreichen Rolle von Raritan beim Verwalten und Warten der Netzwerke von Remoteniederlassungen finden Sie auf **Raritan.de/branch-office-management.**



Raritans Engagement

Raritan ist ein langjähriger Branchenführer für fortschrittliche RZ-Management-Produkte. Raritans Marken beinhalten Paragon und Dominion- sicherer Out-of-band-Zugriff und Kontrolle von Servern, die PX-Familie intelligenter PDUs, Power IQ RZ-Strom- und Energiemanagementsoftware und dcTrack- eine fortschrittliche DCIM-Lösung für RZ-Änderungs- und Kapazitätsmanagement mit Best Practices. Raritan-Produkte haben sich immer durch einfache Nutzung und beste Leistung ihrer Klasse hervorgetan. Wenn Ihr Unternehmen damit anfängt, DCIM-Tools zu testen, empfehlen wir Ihnen, dcTrack zu berücksichtigen. Mit Hauptsitz in Somerset, NJ, hat Raritan 38 Niederlassungen weltweit und bedient 76 Länder. Für weitere Informationen gehen Sie auf **Raritan.de**

C1016 R1