

## Server Based Computing (SBA) Terminalserver - Sicherheit

Terminalserver sind für viele Firmen eine kostengünstige Alternative, traditionelle Workstations zu konsolidieren, und eine unkomplizierte Möglichkeit, Mitarbeitern, Kunden und Filialen Anwendungen zur Verfügung zu stellen.

Oft wird aber übersehen wird, dass Server Based Computing (SBA) gravierende Sicherheitsprobleme beinhalten kann, wenn nicht wirksame Schutzmechanismen eingerichtet werden.

### Serversicherheit

Neben der Kommunikationssicherheit und einer starken Authentifizierung ist dem Thema Serversicherheit beim Server Based Computing eine erhöhte Priorität einzuräumen.

Unterschiedlichste Anwendungen und Daten werden auf Terminalservern zur Verfügung gestellt. Ob Bankensoftware, Office-Programme oder Mail-Clients, jede dieser Anwendungen hat seine Stärken aber auch Schwächen, welche auf Terminalservern ein erhöhtes Risiko darstellen können. Nicht selten bieten veröffentlichte Anwendungen Hintertüren für einen unautorisierten Zugriff auf den Server, so dass nicht freigegebene Programme ausgeführt oder bösartiger Code (Viren, Würmer, Trojaner) eingeschleust werden kann.

Die Härtung des Terminalservers durch Bordmittel, eine straffe Konfiguration oder der Einsatz von Virensoftware reichen in der Regel nicht aus, um unerlaubte Zugriffe auf den Rechner zu unterbinden.

Hier müssen Verfahren eingesetzt werden, die bereits auf Kernebene das Ausführen von Programmdateien steuern und kontrollieren. Das „Hashen“ von ausführbaren Dateien und die benutzerbezogene Authorisierung ist die zentrale Maßnahme, den Terminalserver effektiv abzusichern, ohne die erheblichen Vorteile des Server Based Computing preisgeben zu müssen.

### Kommunikationssicherheit

Beim Einsatz von Terminalservern ist eine ständige Verbindung zum Server nötig. Standardmäßig wird der Datenstrom im Klartext übertragen. Firmeninterne Daten und Prozesse zirkulieren so für jeden les- und manipulierbar zwischen den Clients und den Terminalservern. Das Sicherheitsrisiko ist unkalkulierbar höher, wenn über externe Netzwerke mittels Internet, ISDN, DSL oder gar Funknetze zugegriffen wird.

Verfahren, die die Kommunikationswege stark verschlüsseln, sind daher für sichere Terminalserverumgebungen obligatorisch. „Thick-client“ VPNs, die auf IPSec basieren, oder „Thin-client“ VPNs, die auf der Nutzung von SSL/TLS beruhen, sind hier empfehlenswerte Strategien. SSL-VPN Geräte oder das kosteneffiziente Produkt von Secure Gateway von Citrix sind Alternativen, mit denen sich ein hoher Sicherheitsstandard gewährleisten lässt.

## Authentifizierung

In Unternehmen, in denen Mitarbeiter oder Kunden von externen Standorten auf die Terminalserver zugreifen, stellt ein Login-Verfahren mit statischen Passwörtern ein erhebliches Risiko dar. Zu oft sind statische Kennwörter einfach zu erraten, zu stehlen oder durch Brute-Force-Angriffe verletzbar.

Anmeldeverfahren, die für jedes Benutzer-Login ein Einmalpasswort generieren, sind dagegen eine zuverlässige Alternative, diese Risiken auf ein Minimum zu reduzieren.

## Verfügbarkeit

Ein weiteres wichtiges Thema ist die ständige Verfügbarkeit der Terminalserver. Der Ausfall oder die Wartung eines Rechners darf die Nutzung der Terminalserver nicht verhindern.

Cluster-, Loadbalancing- oder andere HA-Lösungen müssen sicherstellen, dass die Terminalserver ihre Dienste ununterbrochen bereitstellen.

## Mit ITPro sind sie in allen Fragen der Sicherheit bestens beraten

Sichern Sie sich alle Vorteile des Server Based Computing. Nutzen Sie unsere Kompetenz und Erfahrung bei der Konzeption und Umsetzung Ihrer Terminalserverinfrastruktur.

ITPro Informationstechnologie Beratung GmbH  
Kaiserdamm 31  
14057 Berlin

Tel.: +49 30 428 45 17-0  
Fax.: +49 30 428 45 17-22  
Mail: [info@itpro.de](mailto:info@itpro.de)

**Ihr Ansprechpartner:**  
Server Based Computing  
Terminalserver - Sicherheit  
Georg Bauer

Tel.: +49 30 428 45 17-3  
Fax.: +49 30 428 45 17-22  
Mail: [gbauer@itpro.de](mailto:gbauer@itpro.de)