

Sieben Anforderungen für einen sicheren Remote-Zugang

Die Welt von heute ist dynamischer und unberechenbarer als jemals zuvor. Die Marktkräfte zwingen Unternehmen dazu, immer schneller Änderungen umzusetzen – im geschäftlichen wie auch im technischen Umfeld. Deshalb ist der schnelle Zugriff auf Geschäftsanwendungen und wichtige Informationen mittlerweile eine Grundanforderung für jedes moderne Unternehmen. Tatsache ist, dass Anwendungen heute das geschäftliche Rückgrat eines Unternehmens bilden – das reicht von ERP und E-Mail bis zu speziellen vertikalen Lösungen oder individuellen Web-Anwendungen. Praktisch jedes Unternehmen ist darauf angewiesen, entsprechende Anwendungen möglichst zügig, sicher und kosteneffizient für seine Mitarbeiter bereitzustellen.

Inhaltsverzeichnis

- 3 **Auswahl der richtigen Infrastruktur für die Anwendungsbereitstellung**
- 4 **Anforderung 1: Bereitstellung eines einfachen Zugriffs auf Daten und Anwendungen im Firmennetz für jedes Endgerät und jeden Ort**
- 5 **Anforderung 2: Finden Sie eine Lösung, die Ihr IT-Budget schont.**
- 5 **Anforderung 3: Finden Sie eine Lösung für eine umfassende und erweiterbare Endgeräteanalyse.**
- 6 **Anforderung 4: Finden Sie einen Anbieter, der eine komplette und integrierte Infrastruktur für die Anwendungsbereitstellung zur Verfügung stellen kann.**
- 8 **Anforderung 5: Identifizierung einer Lösung, die granulare Autorisierungsrichtlinien und effiziente Kontrollen auf Anwendungsebene unterstützt.**
- 9 **Anforderung 6: Identifizierung einer Lösung, mit der die Einschränkungen der Netzwerk-Zugangskontrolle beseitigt werden.**
- 10 **Anforderung 7: Identifizierung eines zuverlässigen Anbieters mit zukunftssicheren Angeboten, globaler Reichweite und einer starken Vision.**

Auswahl der richtigen Infrastruktur für die Anwendungsbereitstellung

Auf die Forderung nach einem sicheren Zugriff auf das Firmennetz über das Internet reagierten Unternehmen anfangs mit der Implementierung von IPSec-basierten VPNs (Virtual Private Networks). Damit sollte auf Netzwerkebene der Zugriff auf Server im Rechenzentrum bereitgestellt werden. Doch als die Anwender zunehmend auch von mehreren verschiedenen Standorten auf die Ressourcen zugreifen mussten, wurden die Grenzen dieser Technologie schnell deutlich. Das IPSec-Protokoll wird oft von Firewalls und ISPs (Internet Service Provider) blockiert. Zudem erwies sich die Installation und Verwaltung von IPSec-Client-Software als recht komplex. Das Konzept hielt einfach nicht, was es versprach. Anwender waren damit nicht in der Lage, überall und jederzeit auf die benötigten Informationen zuzugreifen.

Um diesen Mangel zu beseitigen und die Anwenderproduktivität zu erhöhen, wurde eine neue Klasse von VPNs entwickelt. Die Verschlüsselung des VPN-Traffic basierte dabei zunächst auf dem offenen SSL-Standard (Secure Sockets Layer) und später auch auf den TLS-Protokollen (Transport Layer Security). Dieses Konzept erlaubte es Remote-Anwendern, dieselben Protokolle zu verwenden, die auch für den Schutz des Zugriffs auf Websites genutzt wurden. Neben der einfachen Installation und Verwaltung und der besseren Connectivity wurden so auch die Anfragen beim Helpdesk auf ein Minimum reduziert. Diese Produkte sind unter dem Namen SSL VPN bekannt. Die VPN-Technologie machte schon bald den sicheren Zugriff über das Internet jederzeit von überall möglich. Das brachte aber viele neue Herausforderungen mit sich. Es gab für Unternehmen keine einfache Möglichkeit, den Zugriff auf die zahlreichen unterschiedlichen Geschäftsanwendungen bereitzustellen, die für die effiziente Nutzung von Informationen benötigt werden. Gleichzeitig konnte auch kaum verhindert werden, dass vertrauliche Daten in Geräten als Kopie oder im Cache verbleiben, wie zum Beispiel beim Zugriff über PCs in Internet-Cafés oder im Home Office.

Für eine befriedigende Lösung dieser Anforderungen benötigt man eine umfassende Architektur, die weit über die Fähigkeiten traditioneller Einzellösungen hinausgeht. Es kommt darauf an, nicht nur die Bereiche zu kontrollieren, auf die ein Anwender zugreifen darf. Es müssen auch Richtlinien umgesetzt werden, die genau festlegen, wie der Zugriff erfolgen darf. Innerhalb einer integrierten Infrastruktur für die Anwendungsbereitstellung arbeitet ein SSL VPN mit den Bereitstellungskomponenten für Client-Server-, Web- und Desktop-Anwendungen im Rechenzentrum zusammen. Auf diese Art wird sichergestellt, dass Anwendungen und Informationen mit der sichersten und effizientesten Methode bereitgestellt werden. Mit einer derartigen Lösung ist es nicht mehr nötig, kritische Informationen für den Zugriff durch die Anwender auf nicht vertrauenswürdigen Clients zu speichern. Der bisher übliche Kompromiss zwischen Zugänglichkeit und Sicherheit gehört damit der Vergangenheit an.

In diesem Dokument erhalten Sie ausführliche Informationen über diese Technologien und erfahren, wie damit selbst kritischste Fragen bei der Bereitstellung des Remote-Zugangs geklärt werden können. Damit sind Sie bestens gerüstet und können potenziellen Anbietern die richtigen Fragen stellen. Und Sie haben alle Informationen zur Hand, die Sie für die Planung einer modernen, leistungsfähigen Architektur benötigen.

Anforderung 1:

Bereitstellung eines einfachen Zugriffs auf Daten und Anwendungen im Firmennetz für jedes Endgerät und jeden Ort

Für Sie ist es oberste Priorität, Ihren Anwendern eine bedienerfreundliche Zugangslösung zur Verfügung zu stellen, durch die diese ihre Arbeit reibungslos erledigen können. Viele Produkte konzentrieren sich ausschließlich auf die Zugangsmechanismen und vernachlässigen dabei die Benutzerfreundlichkeit. Die Lösung Ihrer Wahl sollte die folgenden Kriterien erfüllen:

- **Alle Client-Verbindungen müssen mit einem Protokoll geschützt werden, das überall im Internet einsetzbar ist.** IPSec bietet ein hohes Maß an Sicherheit, wird aber oft von Firewalls und ISPs blockiert. SSL- und TLS-Protokolle werden im Internet häufig für den sicheren Zugang zu Websites eingesetzt. Sie werden von allen modernen Web-Browsern unterstützt. Diese Protokolle werden von den meisten Firewalls und ISPs standardmäßig akzeptiert. Es werden also weniger Verbindungen zurückgewiesen, wodurch die Zufriedenheit der Anwender steigt.
- **Anwender müssen für den Zugriff auch Geräte verwenden können, auf denen keine Client-Software installiert werden kann.** SSL VPNs bringen eine signifikante Verbesserung mit sich – sie erlauben praktisch jedem Client-Gerät mit einem Web-Browser den Basiszugriff auf Dateien, E-Mails und Web-Ressourcen im Unternehmensnetzwerk.
- **Es müssen alle bei Ihnen eingesetzten Anwendungen unterstützt werden.** Viele Anbieter geben an, dass alle Anwendungen unterstützt werden. Diese Aussage sollten Sie aber in jedem Fall kritisch hinterfragen. Benötigen Sie Unterstützung für VoIP-Softphones, die auf mobilen Notebooks ausgeführt werden? Zwar verwenden VoIP-Lösungen nach Aussage ihrer Anbieter Standardprotokolle, oft sind aber herstellerspezifische Implementierungen integriert. Achten Sie darauf, dass das Zusammenspiel zwischen Ihrem VPN und Ihrer Telefonielösung getestet wurde.
Sie sollten auch Anwendungen testen, die serverseitig initiierte Verbindungen benötigen, wie z.B. Active FTP, diverse Instant-Messaging-Lösungen und Systemmanagement-Software. Viele SSL VPNs unterstützen diese Protokolle nicht. Darauf sollten Sie unbedingt achten.
- **Die Anwender sollten nicht selbst die richtige Zugangsmethode auswählen müssen.** Viele SSL VPN-Produkte haben sich aus einer Kombination verschiedener Technologien heraus entwickelt und überlassen dem Anwender die schwierige Entscheidung der Auswahl der richtigen Zugangsmethode. Das setzt bei den Anwendern technisches Wissen über verschiedene Aspekte voraus: Ist der VPN-Client aktiv oder verwende ich einen ausschließlich browserbasierten Zugriff? Muss ich die Proxy-Einstellungen meiner Anwendungen ändern? Ein besserer Ansatz ist es, wenn die Lösung für den Remote-Zugriff selbstständig die Client-Eigenschaften ermitteln und automatisch die beste Zugangsmethode festlegen kann. Die Anwender sollten sich nicht darum kümmern müssen, wie der Zugang bereitgestellt wird. Stattdessen sollte die richtige Zugangsmethode automatisch festgelegt werden.
- **Benutzerfreundlichkeit sollte selbst bei einer schwankenden Internet-Verbindung gewährleistet sein.** Wie gut ist das Reaktionsvermögen Ihrer Lösung bei einer Netzwerkverbindung mit geringer Bandbreite und hoher Latenz? Müssen auch Anwender in dezentralen Außenstellen unterstützt werden? Falls dies der Fall ist, muss Ihre Lösung den Datenverkehr optimieren können, um dem Anwender ein möglichst benutzerfreundliches Arbeiten zu ermöglichen.

Anforderung 2:

Finden Sie eine Lösung, die Ihr IT-Budget schont.

Ihre Anfangsinvestitionen stellen nur einen Bruchteil der Gesamtkosten dar, die durch eine Lösung für den Remote-Zugang entstehen. Sie sollten auch die oft „vergessenen“ Folgekosten für Training, Support und Wartung berücksichtigen. Hier finden Sie einige Hinweise, mit denen Sie die Kosten niedrig halten können:

- **Eine benutzerfreundliche Arbeitsumgebung sorgt für eine geringere Cost-of-Ownership.** Eine intuitiv zu bedienende Lösung, die den Zugriff von jedem Standort aus ermöglicht, reduziert den Trainingsaufwand und die Anzahl der Supportanfragen von frustrierten Anwendern.
- **Administratoren sollten Software nicht auf jedem einzelnen Client-Gerät installieren und pflegen müssen.** Ein weiteres wichtiges Kriterium für den Remote-Zugang ist die erforderliche Wartungsintensität für jedes Client-System. Da bei SSL VPNs Clients über das Web bereitgestellt werden, entfällt der mitunter enorme Wartungsaufwand, der bei IPSec VPNs an der Tagesordnung ist. Bei einigen Lösungen werden diese Clients automatisch aktualisiert, sobald neue Versionen verfügbar sind. Dadurch werden die Administratoren spürbar entlastet, da sie nicht mehr jedes einzelne Client-Gerät direkt verwalten müssen.

Anforderung 3:

Finden Sie eine Lösung für eine umfassende und erweiterbare Endgeräteanalyse.

Bei der Bereitstellung des Zugriffs von einem Client-System über das Internet kann Ihr Unternehmen nicht mehr kontrollieren, wie diese Clients konfiguriert sind. Zur zuverlässigen Vermeidung von Malware-Risiken sollten Sie darauf achten, dass Ihre Lösung die folgenden Kriterien erfüllt:

- **Die Client-Konfiguration sollte geprüft werden, bevor der Zugriff erlaubt wird.** Bei der Überprüfung kann die Sicherheitskonfiguration verifiziert werden, indem sichergestellt wird, dass aktuelle Antivirenprogramme und persönliche Firewalls auf den Clients aktiv sind. Zudem sollten auf den Clients auch die jeweils aktuellsten Versionen von Betriebssystem und Browser installiert sein.
Wird vor Beginn einer Remote-Sitzung eine Endgeräteanalyse durchgeführt, können mangelhafte Konfigurationen erkannt werden, die eine ordnungsgemäße Authentifizierung verhindern oder die Rechte des Anwenders während der Sitzung einschränken.
- **Die Konfigurationsüberprüfungen sollten kontinuierlich vorgenommen werden, um Änderungen während der laufenden Sitzung erkennen zu können.** Es reicht nicht aus, die Konfiguration nur am Anfang einer Sitzung zu prüfen, da Sitzungen durchaus mehrere Stunden oder sogar Tage dauern können. Stattdessen sollten die Konfigurationsüberprüfungen kontinuierlich durchgeführt werden. So wird gewährleistet, dass der Anwender seine Sicherheitssoftware nicht im Laufe der Sitzung einfach deaktiviert.
- **Wählen Sie eine Lösung, die die einfache Überprüfung der Systemidentität ermöglicht.** Nicht nur die Konfiguration eines Client-Systems muss geprüft werden. Es sollte auch ermittelt werden, wer diese Konfiguration vorgenommen hat. Systeme, die eindeutig vom eigenen Unternehmen stammen und entsprechend vorkonfiguriert sind, sollten als vertrauenswürdiger eingestuft werden, als andere Geräte. In der Vergangenheit konnten Systeme nur anhand von Client-Zertifikaten identifiziert werden – was mit einem enormen Aufwand für die IT-Abteilung verbunden war. Ein SSL VPN bietet dagegen alternative Identifizierungsmethoden, die für eine spürbare Entlastung der Administratoren sorgen. Dazu zählen die Verifizierung der MAC-Adresse, die Domänenmitgliedschaft und das so genannte Device Watermarking.

Anforderung 4:

Finden Sie einen Anbieter, der eine komplette und integrierte Infrastruktur für die Anwendungsbereitstellung zur Verfügung stellen kann.

Zugriff von jedem Endgerät und jedem Standort aus – das ist eine zentrale Anforderung an Ihre Lösung für den Remote-Zugang. Das bedeutet, dass für Anwender der Zugriff nicht nur mit dem vom Unternehmen bereitgestellten Notebook möglich ist, sondern auch von jedem beliebigen anderen System aus – auch mit gemeinsam genutzten Geräten.

Überlegen Sie, auf welche Ressourcen Ihre Anwender zugreifen müssen: Dateien, E-Mails, Datenbanken usw. Glücklicherweise ist dieser Zugriff mit den meisten SSL VPN-Lösungen dank IP-Tunneling oder ausschließlich browsergestütztem Zugang möglich.

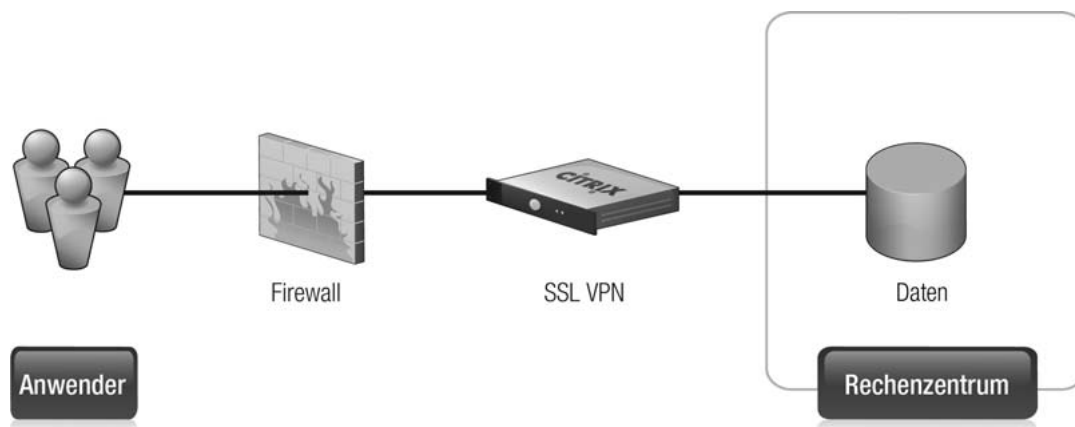


Abbildung 1 – Traditioneller Zugriff auf Daten

Leider werden bei traditionellen VPN-Lösungen andere Schlüsselanforderungen für die Gewährleistung des sicheren, komfortablen, kosteneffizienten Zugangs nicht berücksichtigt. Achten Sie darauf, dass Ihre Lösung die folgenden Kriterien erfüllt:

- **Anwender erhalten jederzeit Zugriff auf Anwendungen.** Dokumente und Informationen sind nutzlos, wenn die für die Anzeige der Daten benötigten Anwendungen nicht zur Verfügung stehen. Das klingt zwar einleuchtend – trotzdem sind die meisten VPN-Lösungen ausschließlich für den Zugriff auf Daten konzipiert. Die Notwendigkeit des Zugriffs auf die entsprechenden Anwendungen wird von diesen Lösungen völlig ignoriert. Ohne diese Fähigkeit kann kein geeigneter Zugriff ermöglicht werden. Die Anwender können dann nur die Informationen nutzen, auf die mit den auf dem Client-System vorinstallierten Anwendungen zugegriffen werden kann (sofern die korrekte Anwendungsversion vorhanden ist).

So ermöglichen SSL VPNs beispielsweise den Anwendern den Zugriff auf ihre Microsoft® Office-Dokumente, doch auf dem Client-Gerät ist unter Umständen die für die Anzeige dieser Dateien benötigte Office-Software gar nicht installiert. Mit einer integrierten Lösung für die Anwendungsbereitstellung kann ein Anwender über einen Browser in seinen Dateien navigieren und diese mit einer vom Rechenzentrum bereitgestellten Anwendung bearbeiten – eine Installation auf dem Client ist nicht erforderlich!

Achten Sie darauf, dass Ihr Anbieter ein integriertes Produktportfolio für die Bereitstellung von Anwendungen zu jedem Remote-Client – unabhängig von Hardwarekonfiguration und Betriebssystem – bietet.

- **Geistiges Eigentum muss zuverlässig geschützt werden.** Wie können Sie vermeiden, dass sensible Daten unabsichtlich auf einem Heim-PC oder einem geliehenen System gespeichert werden? Es sind mehrere Maßnahmen erforderlich um sicherzustellen, dass Daten nur vom bestimmungsgemäßen Anwendern angezeigt werden können.

An erster Stelle steht dabei der Web-Browser. Hier sollten entsprechende Richtlinien für den HTTP-Cache festgelegt werden, die eine Ablage der Daten im Cache verhindern.

Ein Säuberungsagent für den Browser-Cache entfernt zudem am Ende der Remote-Zugriffssitzung sensible Daten. Dieser Agent wird über das Web bereitgestellt. Er säubert den Cache, entfernt Cookies und löscht den Browser-Verlauf.

Manche SSL VPN-Lösungen bieten Sicherheitsfunktionen für den Desktop. Damit werden alle Daten, die während der Sitzung auf dem Client gespeichert wurden, isoliert, verschlüsselt und nach der Sitzung entfernt. Dafür muss aber auf dem Client spezielle Software installiert werden. Diese Vorgehensweise ist nicht für alle Geräte realisierbar und macht es außerdem erforderlich, sensible Daten auf den Client herunterzuladen. Aktuelle Einschätzungen der Sicherheitsrisiken, die kürzlich von verschiedenen Anbietern vorgenommen wurden, belegen aber die Einschränkungen dieses Konzepts. Daten verlassen oftmals den Kontrollbereich der sicheren Desktop-Umgebungen und werden in Bereichen des Client-Betriebssystems abgelegt, wie z.B. in virtuellen Auslagerungsdateien oder in Drucker-Spoolern. Nach dem Ende der Sitzung kann hier jeder, der Zugang zum Client-System hat, auf die Daten zugreifen.

Besser ist es, die Daten gar nicht erst zu übertragen. Ein entscheidender Vorteil der integrierten Anwendungsbereitstellung ist die Tatsache, dass die Daten im Rechenzentrum verbleiben und die Anwender diese nur virtuell nutzen. Und es müssen keine Client-Komponenten installiert werden – die Lösung ist also auf jedem Gerät nutzbar.

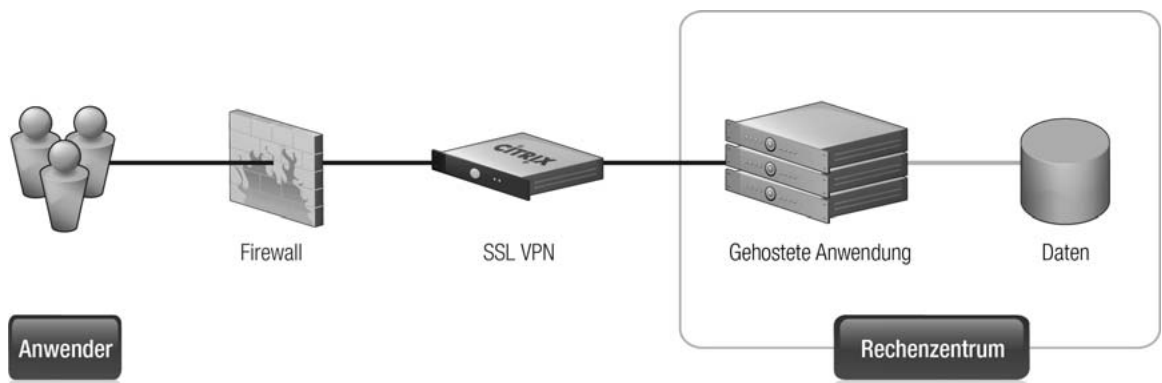


Abbildung 2 — Virtualisierter Zugriff auf Daten

Abbildung 2 zeigt eine integrierte Architektur für die Anwendungsbereitstellung mit einem SSL VPN, das gemeinsam mit einer oder mehreren Komponenten für die Kontrolle der Anwendungsbereitstellung implementiert wurde. Ergebnis:

- Anwendungen sind immer und für jedes Client-System verfügbar
- Anwendungen müssen nicht vorinstalliert werden
- Der Zugriff auf Anwendungen kann vollständig virtualisiert werden
- Daten müssen nicht das Rechenzentrum verlassen

Anforderung 5:

Identifizierung einer Lösung, die granulare Autorisierungsrichtlinien und effiziente Kontrollen auf Anwendungsebene unterstützt.

Viele Lösungen für den Remote-Zugang lassen den Unternehmen nur die Wahl zwischen Sicherheit oder Zugänglichkeit. Man muss sich also entweder für den Komfort der Anwender entscheiden, riskiert dabei aber unkontrollierte Zugriffe auf geistiges Eigentum. Oder man entscheidet sich für Informationssicherheit und nimmt dabei viele Einschränkungen in Kauf – was Anwender dazu bringt, nach alternativen Wegen für den Zugriff auf die benötigten Daten und Anwendungen zu suchen.

Dieses Dilemma können Sie mit einer Lösung vermeiden, die granulare Sicherheitskontrollen auf Anwendungsebene bietet. Im Folgenden werden die wichtigsten Anforderungen beschrieben:

- **Administratoren brauchen eine granulare Kontrolle über die Informationen, auf die zugegriffen werden darf.** Die ersten VPNs besaßen entweder gar keine Zugangskontrollen oder lediglich eine Kontrolle auf Netzwerkebene. Dadurch gewährten die Unternehmen den Anwendern zu große Zugriffsrechte, da die Kontrollroutinen auf Anwendungsebene nicht für bestimmte Websites und Dateiserver angewandt werden konnten. Einige SSL VPNs ermöglichen heute dank der Erkennung von Anwendungsprotokollen die Definition von Zugriffsrechten bis zur Ebene der konkreten Ressourcen.
- **Die Zugriffsrechte sollten sich nach dem jeweiligen Zugriffsszenario richten.** Würde Ihr Unternehmen den Anwendern erlauben, von einem Heim-PC oder einem gemeinsam genutzten Gerät aus auf sensible Finanzdaten oder Anwendungen zuzugreifen? Wahrscheinlich nicht. Doch ändert sich das sicher, wenn der Zugriff des Anwenders über einen Desktop oder über ein vom Unternehmen ausgegebenes Notebook erfolgt. Anhand der Antworten auf einige grundlegende Fragen zu den einzelnen Clients kann Ihre Lösung für den Remote-Zugang das Zugriffsszenario für jede Sitzung identifizieren und die Rechte entsprechend anpassen. Diese Fragen könnten z.B. folgendermaßen lauten:
 - Wo befindet sich der Client (im LAN, im Internet oder in einer dezentralen Niederlassung)?
 - Wurde das Gerät vom Unternehmen ausgegeben?
 - Handelt es sich um einen Desktop oder um ein Notebook?
 - Ist das Gerät ordnungsgemäß konfiguriert?
 - Wird das Gerät von mehreren Anwendern genutzt?

Nur wenige SSL VPNs geben Unternehmen die Möglichkeit, diese Fragen zu beantworten und Zugangsrichtlinien in Abhängigkeit vom Anwender UND vom Zugriffsszenario zu definieren. Für den vollständigen Schutz von Informationen ist das aber zwingend erforderlich.

- **Es sollte eine strikte Kontrolle der zulässigen Aktivitäten (Action Rights) vorhanden sein.** Bei der szenariobasierten Zugangskontrolle wird ermittelt, auf welche Dokumente und Anwendungen zugegriffen werden darf. Doch um zu kontrollieren, was der Nutzer mit den Dokumenten im jeweiligen Zugriffsszenario tun darf, ist eine weitere Kontrollinstanz erforderlich – die aber nur in einer integrierten Infrastruktur für die Anwendungsbereitstellung verfügbar ist.

Durch die Kontrolle der Aktivitäten, die ein Anwender in Verbindung mit den Ressourcen ausführen darf, können Unternehmen ein optimales Gleichgewicht zwischen den Sicherheitsanforderungen und dem Zugriffsbedarf ihrer Anwender herstellen. Der Administrator legt zum Beispiel richtlinienbasiert fest, dass Anwender beim Zugriff über einen Desktop-Rechner in einer dezentralen Niederlassung oder über ein vertrauenswürdiges Notebook im

Unternehmen volle Download-Rechte für Dokumente erhalten. Wenn der Anwender zu einem gemeinsam genutzten oder nicht vertrauenswürdigen Gerät wechselt, kann die Richtlinie automatisch angepasst werden. In dem Fall wird nur noch ein eingeschränkter Zugang mit einer virtualisierten Sitzung gewährt, die vom Rechenzentrum bereitgestellt wird. Während dieser virtuellen Sitzung kann die Funktionalität der jeweiligen Anwendung mit entsprechenden Richtlinien kontrolliert werden, so dass Dateien nicht auf dem Client-Gerät gespeichert und lokale Drucker nicht genutzt werden können.

Anforderung 6: Identifizierung einer Lösung, mit der die Einschränkungen der Netzwerk-Zugangskontrolle beseitigt werden.

NAC-Lösungen (Network Access Control) wurden konzipiert, um die Sicherheit von Unternehmensnetzwerken zu gewährleisten. Diese Lösungen schränken den Zugriff ein, wenn ein Client nicht die in den Sicherheitsrichtlinien definierte Mindestkonfiguration vorweisen kann. Die NAC-Konzepte werden auch heute noch weiterentwickelt. Die Umsetzung ist aber nach wie vor problematisch oder kostspielig. Bei manchen Lösungen müssen zahlreiche Komponenten der vorhandenen Netzwerkinfrastruktur, z.B. Switches und Router, ausgetauscht werden. Andere Lösungen, die die Verteilung der IP-Adressen kontrollieren, können ganz einfach durch die Konfiguration von Clients mit statischen IP-Adressen ausgehebelt werden.

Ein SSL VPN mit Funktionen für die Endgeräteanalyse, das im Randbereich des Rechenzentrums implementiert wird, stellt eine gute Alternative zu den NAC-Lösungen dar. Und dieses Konzept beschränkt sich durchaus nicht nur auf den Remote-Zugang. Manche Hersteller bieten hochperformante SSL VPNs an, die flexibel für die Unterstützung aller Anwender im Unternehmen erweitert werden können. Die IT hat damit die Möglichkeit, den Zugriff aller Geräte im proprietären Netzwerk des Unternehmens zu kontrollieren.

Bei der Planung einer NAC-Lösung sind unbedingt die rigorosen Einschränkungen zu bedenken, die für die Anwender entstehen. Denn deren Clients müssen immer und überall ordnungsgemäß konfiguriert sein. Dieses Konzept gewährleistet zwar die strikte Einhaltung der Sicherheitsrichtlinien, ist aber mit Opportunitätskosten verbunden, die oft nicht beachtet werden. Beispiel: Ein Anwender muss sich einen Computer ausleihen, um eine zeitkritische Aufgabe durchführen zu können. Wie lange dauert es, diesen Rechner ordnungsgemäß zu konfigurieren? Kann der Rechner auch von einem Remote-Standort aus konfiguriert werden? Welche geschäftlichen Folgen entstehen, wenn der Mitarbeiter die Aufgabe nicht rechtzeitig erledigen kann? Was ist, wenn diese Aufgabe darin bestand, auf eine wichtige Verkaufspräsentation zuzugreifen und sie einem potenziellen Kunden zu zeigen? Waren die ganzen Schutzmaßnahmen für die Infrastruktur den Aufwand wert, der dem Anwender auferlegt wurde? Mit diesem Dilemma sollte kein Unternehmen zu kämpfen haben.

Wenn ein Anwender wie im oben beschriebenen Beispiel einen Zugang benötigt, kann mit der Endgeräteanalyse ermittelt werden, ob der Client ordnungsgemäß konfiguriert ist. Ist das der Fall, können die benötigten Informationen direkt auf den Client heruntergeladen werden. Der Anwender kann so seine Aufgabe ohne Verzögerungen durchführen. Wenn auf dem Client nicht das richtige Betriebssystem oder die falsche persönliche Firewall vorhanden ist, würden standardmäßige NAC-Lösungen den Zugriff einfach komplett verweigern. Eine integrierte Lösung für die Anwendungsbereitstellung mit einer Kontrolle der zulässigen Aktivitäten kann dieses Szenario erkennen und den Zugriff auf die angeforderten Daten virtuell bereitstellen. Der Anwender kann so seine Aufgaben auf einem nicht vertrauenswürdigen Gerät ausführen – und das ohne die Gefahr des Verlustes von geistigem Eigentum.

Anforderung 7:

Identifizierung eines zuverlässigen Anbieters mit zukunftssicheren Angeboten, globaler Reichweite und einer starken Vision.

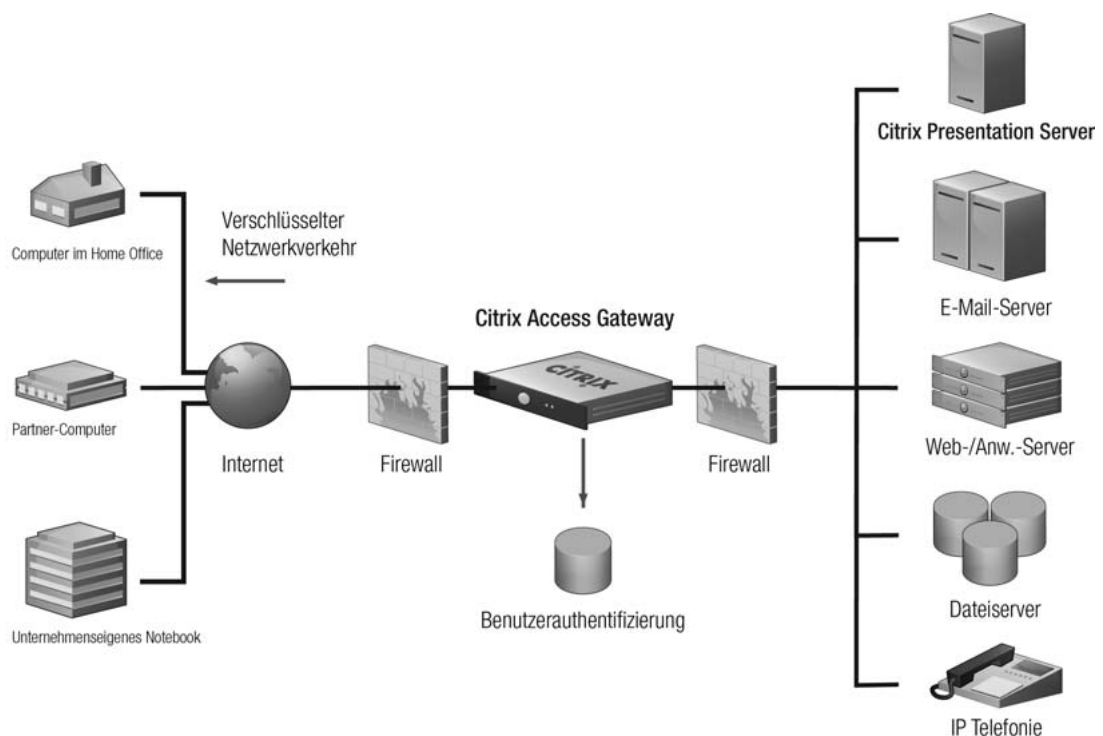
Ganz gleich, welche Lösung Sie für den Remote-Zugang implementieren – sie ist in jedem Fall ein strategischer und essentieller Bestandteil Ihrer Netzwerkinfrastruktur. Den bestmöglichen Schutz Ihrer Investitionen erreichen Sie durch die Zusammenarbeit mit einem Anbieter, der Ihre Implementierung über den gesamten Lebenszyklus wirkungsvoll unterstützen kann.

INFORMATIONEN ÜBER CITRIX SYSTEMS, INC.

Citrix Systems, Inc. (NASDAQ: CTXS) ist der weltweit führende Anbieter von Infrastruktur zur Applikationsbereitstellung. Mehr als 200.000 Unternehmen weltweit verlassen sich auf Citrix, um den Anwendern jede Applikation orts- und zeitunabhängig zur Verfügung zu stellen - mit der höchsten Performance, der größten Sicherheit und den niedrigsten Kosten. Zu den Kunden zählen alle Fortune 100 Unternehmen und 98 Prozent der Fortune 500 Unternehmen ebenso wie tausende von kleinen und mittleren Unternehmen. Citrix Systems, Inc. hat seinen Hauptsitz in Fort Lauderdale, Florida (USA), und ist mit Niederlassungen in 29 Ländern vertreten. Citrix zählt 6.200 Handels- und Allianz-Partner in über 100 Ländern. Im Geschäftsjahr 2006 erwirtschaftete Citrix einen Umsatz von 1,1 Milliarden US-Dollar. Sie können also sicher sein, dass Citrix auch in Zukunft leistungsfähige Produkte und weltweiten Support anbietet. Damit erhalten Sie alles, was Sie für den Aufbau Ihrer integrierten Architektur für die Anwendungsbereitstellung benötigen.

CITRIX ACCESS GATEWAY

Citrix Access Gateway™ wird von den bedeutendsten Branchenanalysten wie Gartner und Forrester Research als ein führendes SSL VPN-Produkt bewertet. Bei einer Implementierung als ausgetestetes und bewährtes Gerät in der demilitarisierten Zone (DMZ) des Unternehmensnetzwerks stellt Citrix Access Gateway einen zentralen Punkt für den Zugriff auf Anwendungen und Ressourcen bereit, die im Rechenzentrum gehostet werden.



GEWÄHRLEISTUNG DES OPTIMALEN ZUGANGS

Mit Citrix Access Gateway™ können Anwender über beliebige Clients mit einem Web-Browser und Internet-Zugang eine sichere Verbindung zum Unternehmensnetzwerk aufbauen und so an jedem Ort produktiv arbeiten.

Dank der benutzerfreundlichen und intuitiven Oberfläche erhalten die Anwender den bestmöglichen Zugang – der Trainingsaufwand und die Anzahl der Supportanfragen werden dadurch spürbar reduziert. Verschiedene Funktionen, wie z.B. der Always-on-Zugang, sorgen dafür, dass Sitzungen nach Verbindungsabbrüchen oder beim Roaming zwischen Zugangspunkten automatisch wiederhergestellt werden.

Citrix Access Gateway vereinfacht den Zugriff über jedes System, indem die komplexen Abläufe für die Anwender einfach ausgeblendet werden. Der Zugang kann sich aus verschiedenen Gründen schwierig gestalten. Bei anderen SSL VPN-Produkten erhalten Anwender oftmals keinen vollständigen Netzwerkzugriff, da sie keine administrativen Rechte für ihr Client-System besitzen. Der Client-Installer von Citrix Access Gateway erkennt diese Situation und führt die Installation automatisch im Modus für Benutzer ohne Administrationsrechte durch. Die Anwender können alle TCP- und UDP-Protokolle verwenden, ohne Anwendungen neu konfigurieren zu müssen.

Wenn die Client-Software nicht installiert werden kann oder wenn Anwender auf einem geliehenen Rechner einen schnellen Zugang benötigen, ermöglicht Citrix Access Gateway den Zugriff auf geschützte Websites, freigegebene Dateien und E-Mails – und zwar auf jedem Gerät mit einem standardmäßigen Web-Browser. Dazu gehören auch einige Handhelds und andere kleinformatige mobile Endgeräte.

HÖCHSTE SICHERHEIT FÜR ANWENDUNGEN UND DATEN

Für Administratoren stellt Citrix Access Gateway einen zentralen Kontrollpunkt dar, über den die lebenswichtigen Ressourcen des Unternehmens anhand verschiedener Schlüsselfunktionen geschützt werden können:

- Die Endgeräteanalyse kann vor der Authentifizierung auf den Clients gestartet werden und anschließend kontinuierlich die Konfiguration und Identität des Systems überprüfen. Bei den Analyse-Scans werden folgende Aspekte geprüft:
 - Antivirensoftware (einschl. Prüfung auf aktuelle Virendefinition)
 - Persönliche Firewalls
 - Betriebssystem und Patch-Level
 - Browser-Typ und -Version
 - Bekannte MAC-Adressen
 - Client-Zertifikate
- Für Clients, die nicht die Mindestkonfiguration besitzen, kann der Zugriff eingeschränkt werden. Zudem können diese Clients auf eine spezielle Seite zur Installation der korrekten Software weitergeleitet werden.
- Die Anwenderauthentifizierung kann mittels verschiedener starker Authentifizierungsformen (einschl. Smartcards und Token-basierter Methoden) erfolgen oder über Authentifizierungsstellen vorgenommen werden, die das RADIUS- oder LDAP-Protokoll unterstützen.
- Die gesamte Kommunikation mit dem Client wird dank der starken Verschlüsselung des Datenverkehrs mit SSL und TLS sicher über das Internet übertragen.
- Administratoren können Autorisierungsrichtlinien für die gängigsten Ressourcentypen erstellen. In Citrix Access Gateway sind umfassende Informationen über Anwendungsprotokolle hinterlegt. Das ermöglicht den Administratoren die einfache und problemlose Kontrolle des Zugriffs auf Web-Anwendungen, freigegebene Dateien, E-Mails und Anwendungen, die auf Citrix Presentation Server™ gehostet sind, sowie andere Anwendungen, die auf TCP- oder UDP-Verbindungen zum Rechenzentrum angewiesen sind.

-
- Administratoren können in Abhängigkeit von der Anwenderidentität und der Gruppenmitgliedschaft (abgeleitet von den LDAP- oder RADIUS-Authentifizierungsstellen) den Zugriff auf Ressourcen entweder gewähren oder verweigern. Darüber hinaus ist es möglich, die Richtlinien auf das jeweilige Zugangsszenario des Clients (ermittelt anhand der Client-Konfiguration, der Systemidentität oder der Position im Netzwerk) abzustimmen. Auf diese Weise können die Rechte von Anwendern geändert werden, wenn sie zwischen verschiedenen Systemen wechseln.
 - Mit der zum Patent angemeldeten Citrix SmartAccess-Technologie mit Action Rights wird nicht nur kontrolliert, auf welche Ressourcen ein Anwender zugreifen kann. Es wird auch die sicherste und optimalste Zugriffsmethode ermittelt.
 - Die Aktivitäten von Anwendern und Administratoren können mit den Überwachungsfunktionen von Citrix Access Gateway umfassend nachverfolgt werden. Auf Wunsch können Protokolleinträge an einen externen Syslog-Server übermittelt werden, um die Einträge mit anderen Produkten im Netzwerk zusammenzuführen.
 - Mit verschiedenen Redundanzoptionen stellt Citrix Access Gateway sicher, dass Sitzungen selbst dann aufrecht erhalten werden, wenn ein einzelnes Gerät oder ein ganzer Rechenzentrumsstandort nicht mehr verfügbar ist.

EINFACHE ADMINISTRATION UND GERINGE TOTAL COST OF OWNERSHIP

Citrix Access Gateway bietet zahlreiche Funktionen für die Reduzierung des administrativen Aufwands. Dank Auto-Download und Auto-Update des Clients ist es nicht mehr erforderlich, jedes einzelne Client-System manuell zu aktualisieren. Die Anwender von Windows®-Desktops sowie von Linux- und Mac OS X-Clients können einfach über einen Web-Browser auf die entsprechenden Daten im LAN zugreifen.

Durch die zentrale Administration lassen sich alle Geräte über eine einzige Konsole verwalten. Die rollenbasierte Administration ermöglicht die Delegation der Verantwortlichkeiten an mehrere Personen.

Dank der SNMP-Unterstützung wird die Notwendigkeit der kontinuierlichen Überwachung des Diagnose- und Performancestatus des Geräts auf ein Minimum reduziert. Damit können Citrix Access Gateway-Geräte beim Auftreten relevanter Ereignisse direkt die gängigen Systeme für das Netzwerk-Monitoring und -Management benachrichtigen.

Darüber hinaus ist es möglich, mehrere Authentifizierungspunkte und virtuelle Server zu nutzen. So lässt sich ein einzelnes Gerät so konfigurieren, dass mehrere verschiedene Anwendersegmente unterstützt werden. Die Mitarbeiter des Unternehmens können zu einer dedizierten Anmeldeseite geleitet werden, wo sie die Authentifizierungsdaten für das Standard-Unternehmensverzeichnis eingeben müssen. Partner können über eine andere URL zu einer separaten Anmeldeseite geleitet werden und sich dort an dem Verzeichnis anmelden, das die Partnerkonten enthält. Dieselbe Methode kann auch bei der Übernahme neuer Unternehmen angewandt werden. Das ermöglicht den zügigen Zugang zu Informationen, ohne dass dazu Benutzerkonten mit dem primären Unternehmensverzeichnis zusammengeführt werden müssen. Auch auf neue Anforderungen können Sie mit Ihrer vorhandenen Infrastruktur schnell, flexibel und effizient reagieren – und somit Ihre Investitionen umfassender nutzen.

UMFASSENDE ANWENDUNGSBEREITSTELLUNG MIT CITRIX PRESENTATION SERVER

Gemeinsam stellen Citrix Access Gateway und Citrix Presentation Server™ eine schlagkräftige, vollständig integrierte Infrastruktur für die Anwendungsbereitstellung dar. Keine andere Lösung bietet einen so hohen Integrationsgrad. Mit dieser Kombination erhalten die Anwender den Zugang mit dem besten Benutzerkomfort. Gleichzeitig ist die effiziente Kontrolle der geschäftskritischen Ressourcen gewährleistet.

Citrix Presentation Server hostet Anwendungen auf Servern im Rechenzentrum und stellt einen virtualisierten Zugriff auf diese Anwendungen für die meisten Client-Plattformen bereit. Die Anwendung und ihre Dokumente verbleiben sicher im Rechenzentrum, werden den Clients aber über eine Netzwerkverbindung zur Verfügung gestellt.

Citrix Access Gateway behandelt die Anwendungen wie jede andere geschützte Ressource und fungiert als zentraler Kontrollpunkt für die Gewährleistung der sicheren Bereitstellung. Administratoren können anhand von Richtlinien die Anwendungen festlegen, die den Anwendern bereitgestellt werden sollen. Ändert sich das Zugangsszenario, können diese Richtlinien entsprechend angepasst werden. Wenn ein Anwender zwischen verschiedenen Clients wechselt, sorgen Access Gateway und Presentation Server gemeinsam für die automatische Wiederverbindung des Anwenders mit den Anwendungen, mit denen er auf dem vorherigen Client gearbeitet hat. Diese Technologie nennt Citrix SmoothRoaming™.

SmoothRoaming unterstützt auch szenariobasierte Richtlinien. Beispiel: Ein Anwender nutzt im Büro eine sensible Finanzanwendung und möchte anschließend auf seinem Heim-PC weiterarbeiten. Für diesen Fall können Richtlinien definiert werden, mit denen verhindert wird, dass SmoothRoaming im Heimbereich des Anwenders eine Wiederverbindung zu dieser Anwendung vornimmt.

Mit Citrix Presentation Server können auch die so genannten Action Rights umgesetzt werden. Administratoren können anhand von Richtlinien festlegen, dass Dokumente nur in einer virtualisierten Umgebung angezeigt werden dürfen. Auf diese Weise wird der optimale Schutz von wichtigen Daten gewährleistet. Wichtige Anwendungsfunktionen, wie z.B. das Drucken auf dem lokalen Drucker oder das Speichern auf dem lokalen Laufwerk des Clients, können per Richtlinie deaktiviert werden. Durch die Möglichkeit, das Speichern von Daten auf nicht vertrauenswürdigen Client-Systemen zu unterbinden, haben Administratoren die volle Kontrolle über den gesamten Fluss von sensiblen Informationen.

Mit der integrierten Infrastruktur für die Anwendungsbereitstellung bringen Citrix Access Gateway und Citrix Presentation Server auch den Anwendern entscheidende Vorteile, da sie von jedem Ort aus auf die benötigten Anwendungen zugreifen können.

ENTWICKELT FÜR DIE ANFORDERUNGEN ALLER UNTERNEHMEN

Citrix Access Gateway ist in drei Editionen erhältlich. Damit können Sie ganz flexibel das Produkt auswählen, das Ihren geschäftlichen Anforderungen und Ihrem Budget entspricht.

- Die **Citrix Access Gateway™** Standard Edition ist einfach zu installieren und zu verwalten. Sie ist die kosteneffizienteste Lösung, die derzeit auf dem Markt erhältlich ist. Mit einem Access Gateway-Gerät in Ihrer DMZ sorgen Sie für den sicheren Zugriff auf Ihre geschützten Ressourcen. Dazu gehören auch die Anwendungen, die über Citrix Presentation Server bereitgestellt werden.
- Die **Citrix Access Gateway™** Advanced Edition unterstützt eine größere Anzahl von Geräten und Anwendern und bietet dafür zusätzliche Funktionen, wie z.B. ausschließlich browserbasierter Zugriff auf Ressourcen, Support für mobile Geräte und eine ausgeklügelte Policy Engine mit umfassenden SmartAccess-Funktionen und Action Rights-Kontrollen.
- Die **Citrix Access Gateway™** Enterprise Edition ist die ideale Lösung für anspruchsvolle Unternehmensumgebungen – nicht zuletzt dank der enormen Skalierbarkeit, Performance sowie dem flexiblen Management. Die integrierten Hochverfügbarkeitsoptionen unterstützen die Business-Continuity-Planung mit redundanten Anwendungspaaren und mit standortübergreifenden Failover-Funktionen. Die integrierten Funktionen für die Anwendungsbeschleunigung und -optimierung sorgen für den schnellen, effizienten Remote-Zugang – und damit für einzigartigen Benutzerkomfort.

Weitere Informationen

Weitere Informationen über die Citrix Access Gateway-Produkte erhalten Sie unter <http://www.citrix.de>.

NOTICE

Die Informationen in diesem Dokument können ohne vorherige Ankündigung geändert werden. DIESES DOKUMENT WIRD „WIE GESEHEN“ OHNE JEDLICHE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNGEN ZUR VERFÜGBARKEIT GESTELLT, EINSCHLIESSLICH DER GEWÄHRLEISTUNG IM HINBLICK AUF HANDELSTAUGLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHTVERLETZUNG VON RECHTEN. CITRIX SYSTEMS, INC. („CITRIX“) IST WEDER FÜR HIERIN ENTHALTENE TECHNISCHE ODER INHALTLICHE FEHLER ODER AUSLASSUNGEN HAFTBAR NOCH FÜR DIREKTE SCHÄDEN, ZUFÄLLIGE SCHÄDEN, FOLGESCHÄDEN ODER ANDERE SCHÄDEN, DIE SICH AUS DEN INHALTEN ODER DER NUTZUNG DIESES DOKUMENTS ERGEBEN. DIES GILT AUCH DANN, WENN CITRIX IM VORAUS VON DER MÖGLICHKEIT SOLCHER SCHÄDEN IN KENNNTNIS GESETZT WURDE. DIE IN DIESEM DOKUMENT ANGEFÜHRTE FALLENBEISPIELE DIENEN LEDIGLICH DEMONSTRATIONSZWECKEN. DIE FÜR SIE ZU ERWARTENDEN KOSTEN UND ERGEBNISSE KÖNNEN UNTER UMSTÄNDEN ABWEICHEN.



Über Citrix: Citrix Systems, Inc. (NASDAQ: CTXS) ist der weltweit führende Anbieter von Infrastruktur zur Applikationsbereitstellung. Mehr als 200.000 Unternehmen weltweit verlassen sich auf Citrix, um den Anwendern jede Applikation orts- und zeitunabhängig zur Verfügung zu stellen – mit der höchsten Performance, der größten Sicherheit und den niedrigsten Kosten. Zu den Kunden zählen alle *Fortune* 100 Unternehmen und 98 Prozent der *Fortune* 500 Unternehmen ebenso wie tausende von kleinen und mittleren Unternehmen. Citrix Systems, Inc. hat seinen Hauptsitz in Fort Lauderdale, Florida (USA), und ist mit Niederlassungen in 29 Ländern vertreten. Citrix zählt 6.200 Handels- und Allianz-Partner in über 100 Ländern. Im Geschäftsjahr 2006 erwirtschaftete Citrix einen Umsatz von 1,1 Milliarden US-Dollar. Die Niederlassung für die Vertriebsregion Central Europe (Deutschland, Österreich, Schweiz und Osteuropa) befindet sich in Hallbergmoos bei München. Weitere Informationen finden Sie unter www.citrix.de.

© 2007 Citrix Systems, Inc. Alle Rechte vorbehalten. Citrix®, Citrix Presentation Server™, Citrix Access Gateway™ und SmoothRoaming™ sind Warenzeichen von Citrix Systems, Inc. und/oder seinen Niederlassungen und können im Patent and Trademark Office der USA oder in anderen Ländern eingetragen sein. Microsoft® und Windows® sind in den USA und/oder anderen Ländern eingetragene Warenzeichen der Microsoft Corporation. Alle anderen Warenzeichen oder eingetragenen Warenzeichen sind das Eigentum der jeweiligen Besitzer.

Citrix Worldwide

HAUPTSITZ EUROPA

Citrix Systems International GmbH

Rheinweg 9
8200 Schaffhausen
Schweiz
Tel: +41 (0)52 6 35 77-00
www.citrix.com

EUROPÄISCHE NIEDERLASSUNGEN

Citrix Systems GmbH

Am Söldnermoos 17
85399 Hallbergmoos / München
Deutschland
Tel: +49 (0)811 83-0000
www.citrix.de

Citrix Systèmes SARL

7, place de la Défense
92974 Paris la Défense 4 Cedex
Frankreich
Tel: +33 (0)1 49 00 33 00
www.citrix.fr

Citrix Systems UK Limited

Chalfont Park House, Chalfont Park
Chalfont St. Peter
Gerrards Cross
Buckinghamshire, SL9 0DZ
United Kingdom
Tel: +44 (0)1753 276 200
www.citrix.co.uk

HAUPTSITZ

Citrix Systems, Inc.

851 West Cypress Creek Road
Fort Lauderdale, FL 33309
USA
Tel: +1 (800) 393 1888
Tel: +1 (954) 267 3000
www.citrix.com

HAUPTSITZ ASIEN/PAZIFIK

Citrix Systems Asia Pacific Pty Ltd.

Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central
Hong Kong
Tel: +852 2100 5000
www.citrix.com

Citrix Online Division

5385 Hollister Avenue
Santa Barbara, CA 93111
Tel: +1 (805) 690 6400
www.citrixonline.com