

Remote Access sichert Business Continuity

Jederzeit und überall Datenfluss

Der Winter hat es wieder einmal bewiesen: Was nützen optimale Rechner- und Netzabsicherung in Ausweichrechenzentren, wenn Mitarbeiter nicht einmal zu ihren Arbeitsplätzen gelangen können, weil Straßen unpassierbar sind, Flughäfen geschlossen werden und mancherorts sogar der Busverkehr eingestellt wird? Die Lösung für derlei – und manche andere – Krisenfälle ist ein Remote-Access-Konzept, das von jedem Ort aus den Zugriff auf Daten und Anwendungen ermöglicht.

Energieversorger – vom klassischen Großunternehmen bis hin zu ihren kleineren Zulieferbetrieben – sind seit vielen Jahren stark von ihrer Informationstechnik abhängig. Mittlerweile betrifft dies aber nicht nur den Gau des Rechenzentrumsausfalls. Ebenso fatal kann es sich auswirken, wenn zum Beispiel Geschäftsführer oder auch Servicemitarbeiter in Krisensituationen keinen Zugang mehr zu ihrem Arbeitsplatz und damit ihrem System haben: Störungsmeldungen gelangen nicht zeitgerecht an ihren Empfänger, Entscheidungen müssen eventuell aufgeschoben werden, Termine werden nicht eingehalten. Wenn es sich dabei um geschäftskritische Vorfälle handelt, kann es das Unternehmen teuer zu stehen kommen.

Remote Access – heute unverzichtbar für Business Continuity

Gleichzeitig steigen die gesetzlichen Anforderungen an die Business Continuity – und damit an die Verfügbarkeit und Zuverlässigkeit der gesamten Informationstechnik. Ebenso wichtig ist aber, dass die Anwender in den Unternehmen sie auch jederzeit nutzen können. So sind die Business-Continuity-Maßnahmen zusätzlich zum bisherigen Notfall- und Wiederanlaufkonzept nun noch um einen weiteren Aspekt zu ergänzen: die Erreichbarkeit der Systeme und Arbeitsplatzrechner von außerhalb, idealerweise von jedem Rechner überall in der Welt.

Notfallmitarbeiter benötigen grundsätzlich im Krisenfall diesen Zugriff auf die wichtigsten Datenbanken und Applikationsserver ihrer Organisation. Außerdem müssen alle oder – je nach Unternehmensstrategie – ein zu definieren-

der Prozentsatz der Mitarbeiter, eventuell Kunden und Geschäftspartner ebenfalls jederzeit und auch von außerhalb Zugang zu ihren Daten und Anwendungen bekommen. Diese Aufgabenstellung ist heute durch ein intelligent geplantes Remote-Access-Konzept zu realisieren.

Remote Access: Worauf ist zu achten?

Im Extremfall kann es passieren, dass zusätzlich zu einem IT-Notfall, in dem alle Systeme in einem Ausweichrechenzentrum aktiviert werden müssen, einige Anwender auch von außen den vollen Datenzugriff benötigen. Daher sind die Remote-Access-Anbindungen auch zu dem Ausweichrechenzentrum oder den Notfallserversn einzurichten.

Die Anwendungen müssen entweder immer verfügbar oder im Notfall sofort aktivierbar sein und auch bei Spitzenbelastungen mit der gewohnten Performance funktionieren. Der Zugriff sollte auch für Ungeübte einfach bedienbar sein. Da Totalausfälle eher selten vorkommen, ist aus Kostengründen zu überlegen, nicht für jeden potenziellen Benutzer eine Einzellizenz zu erwerben, sondern eine Lösung zu wählen, die einen fallweisen Zugang ermöglicht.

Um den Zugriff im Extremfall auch von einem Internetcafé aus zu ermöglichen, müssen die Zugänge Hardwareunabhängig sein. Dennoch – und das gilt für Home Offices gleichermaßen – gilt das Diktat der absoluten End-to-End-Sicherheit. Die Sicherheitsregeln, z. B. der Login, dürfen sich nicht oder nur wenig von dem gewohnten Prozedere unterscheiden.

Zwei Wege führen zum Ziel

PC- und DSL-Anschlüsse als technische Voraussetzungen für den Remote-Zugriff sind heute nahezu in allen Home Offices vorhanden. Soll oder muss der Mitarbeiter auch von (Dienst-)Reisen zugreifen, so können Notebooks oder PDA genutzt werden, in Notfällen auch PC in Hotellobbys. Hier ist allerdings zu bedenken, dass sich die beiden Zugangswege – eigene oder fremde Rechner – durchaus unterscheiden: Client-Software kann nur auf der eigenen Hardware installiert werden. Insofern muss das Unternehmen



Klaus Brandstätter,
Geschäftsführer HOB GmbH &
Co. KG, Cadolzburg.

bei der Technikauswahl strategisch vorgehen und die Vor- und Nachteile abwägen. Als Lösungen haben sich zwei sichere Wege bewährt, die sich im Wesentlichen durch den Verschlüsselungsstandard unterscheiden: SSL- und IPsec-basierte Zugänge.

SSL: Überall auf jedem Rechner online

Das SSL-Protokoll ist sehr sicher und zunehmend verbreitet, weil es End-to-End-Verbindungen auf Applikationsebene ermöglicht, die in jeder Umgebung funktionieren und nur in wenigen Fällen geblockt werden. Der große Vorteil ist, dass auf dem externen Rechner lediglich ein Browser nötig ist – ohne weitere Installationen, Treiber oder Administratorrechte. Zudem wird bei vielen Anbietern ein Client (nativ oder Java) passend zur Anwendung benötigt – etwa ein RDP-Client für den Zugriff auf Office-Produkte. Sind diese Voraussetzungen gegeben, lädt der Browser beim ersten Zugriff ein Java-Applet und startet die Applikation. Das Applet bleibt im Cache und bei jedem Start wird die neue Version abgeprüft.

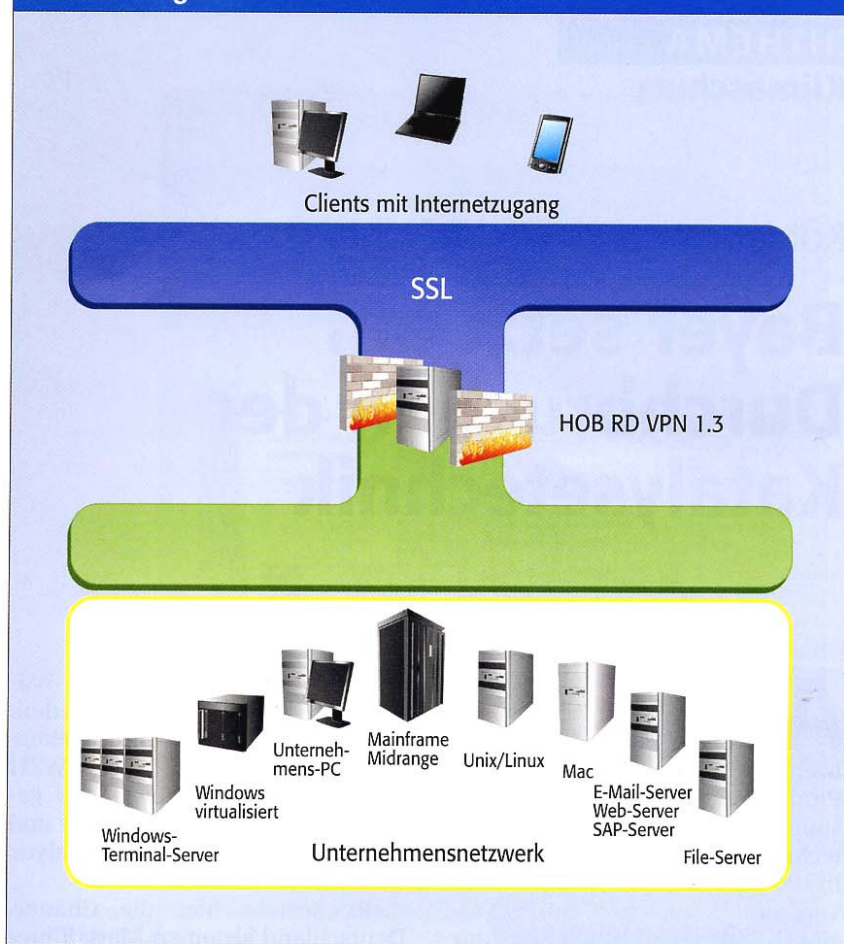
Für Administratoren, die in Krisenfällen für ihren Support den vollen Netzwerkzugriff benötigen, eignet sich das Point-to-Point-Protocol (PPP), um auch von fremden Rechnern aus unkompliziert auf die Netzwerkinfrastruktur, ja sogar ihre Desktops zuzugreifen. Alle Protokolle wie TCP, UDP oder ICMP werden automatisch durch den sicheren Tunnel geroutet.

Für den höchstmöglichen Schutz unternehmenskritischer Daten sollte eine zusätzliche Sicherheitssoftware installiert werden, die den Client vor dem Zugriff nach bestimmten Kriterien wie Virens Scanner überprüft.

SSL-VPN in der Westentasche

Eine weitere Variante auf SSL-VPN Basis sind USB-Sticks für die Authentifizierung und in manchen Fällen auch den Zugriff zum Firmen-Intranet beziehungsweise in die Unternehmens-Cloud. Dabei handelt es sich um installationslose Smartcard-Leser mit verschlüsseltem Speicher, die eine hochsichere und einfache Kommunikation garantieren, während sie den Zugriff durch Dritte verhindern.

Einsatzmöglichkeiten



Einsatzmöglichkeiten von HOB RD VPN 1.3

Voller Netzzugriff via IPsec VPN

Für Firmen, die auf dem externen Endgerät Client-Software installieren können oder wollen, kommt auch die standardisierte VPN-Technologie mit den Protokollfamilien IPsec und IKE/ISAKMP in Frage. Dafür erstellt die zentrale Administration im Rahmen eines unternehmensweiten Rollouts eine Client-CD für alle Remote-Rechner, die nach dem Start alle festgelegten Features automatisch installiert. Allerdings werden mit IPsec Daten versandt, die nicht in jeder Infrastruktur ihr Ziel erreichen, weil preisgünstige Komponenten das IPsec-Protokoll oft nicht unterstützen.

Besser ohne Datendownload

Auch für den Zugriff mit modernen Mobiltelefonen gibt es mittlerweile Client-Lösungen, die für die Darstellung auf kleinen Handy-Monitoren optimiert sind. Aus Sicherheitsgründen werden keinerlei Daten geladen, sondern während des Zugriffs nur Bildschirminhalte übertragen. Diese Lösung basiert auf zwei Softwarekomponenten: Der Mobil-Client wird auf dem Endgerät selbst installiert, im Unternehmen bzw. Ausweichrechenzentrum steht als Gegenpart ein spezieller Server im Lan oder Intranet.

Wichtig ist allerdings, hier auf eine optimale Bandbreitenausnutzung und kurze Verbindungszeiten zu achten, dass sie über gängige Schnittstellen mit Webservice-fähigen Applikationen wie SAP, Exchange, IMAP und SMTP-Mailanwendungen funktionieren und die wichtigsten Betriebssysteme – Windows, Linux, mobile Geräte von Apple (iPhone, iPad) und Android – unterstützen.

Fazit

Krisensituationen kommen immer überraschend. In Stresssituationen wird so manche Fehlentscheidung getroffen – seien es unpassende Techniken oder falsche Realisierungspartner. Um den Geschäftsbetrieb aufrecht erhalten zu können, wenn die Mehrzahl der Mitarbeiter nicht an den Arbeitsplatz kommen kann, sollten die Entscheider zeitgerecht einen Remote-Access-Zugang sorgfältig planen. Welche Lösung letztlich für die Anforderung die Beste ist – SSL, IPsec VPN oder USB-Stick – kann jedes Unternehmen nur nach umfassenden Analysen selbst entscheiden.

(40323)

kb@hob.de

www.hob.de