Artikel wurde in folgenden Themenkategorien gefunden:
Fachthemen » IT-Sicherheit » Ausfall- und Prozesssicherheit
Zeitschriften » IT-SICHERHEIT » News und Artikel » Ausfall- und Prozesssicherheit

09.02.2011
Klaus Brandstätter, HOB GmbH & CO. KG

Jederzeit und überall sicher in Verbindung

Business Continuity durch Remote Access

Die beste Rechner- und Netzabsicherung nützt nichts, wenn Mitarbeiter in Krisenfällen nicht zu ihren Arbeitsplätzen gelangen.

Die Lösung dafür ist ein sicheres Remote Access Konzept, das von jedem Ort aus den Zugriff auf Daten und Anwendungen ermöglicht. Klaus Brandstätter, Geschäftsführer des Connectivity-Spezialisten HOB GmbH & Co. KG erklärt, was bei der Planung zu beachten ist.

Waren bisher nur Großunternehmen oder der Mittelstand nahezu vollkommen von ihrer Informationstechnik abhängig, so sind dies heute auch alle Freiberufler, Selbstständigen und Kleinst-Handwerksbetriebe.

Das gilt nicht nur für Notsituationen ausgefallener Rechenzentren, sondern auch dann, wenn Mitarbeiter keinen Zugang mehr zu ihrem Arbeitsplatz und damit ihrem System haben. Gerade dafür sind die Risiken angesichts des Klimawandels und der Globalisierung deutlich gestiegen: Flutkatastrophen nehmen zu, im Winter kommt es zu wochenlangem Glatteis-Chaos. Durch die Reisemobilität können Grippewellen zu bedrohlichen Pandemien werden. Und dass ein Vulkanausbruch den Luftverkehr stilllegt, war im Sommer 2010 auch eine neue Erkenntnis. Auch Streikwellen wie im Oktober in Frankreich durch Kraftstoffmangel und den Zusammenbruch des öffentlichen Verkehrs können Menschen und ganze Branchen lahmlegen.

Gleichzeitig steigen die gesetzlichen Anforderungen an die Business Continuity - und damit an die Verfügbarkeit und Zuverlässigkeit der IT-Systeme. Ebenso wichtig ist aber, dass die Anwender sie auch jederzeit nutzen können.

Remote Access - heute unverzichtbar für Business Continuity

Bis vor kurzem kam dem Desaster Recovery in Form einer Wiederanlaufstrategie in Ausweichrechenzentren die tragende Rolle zu. Daran wird sicherlich auch zukünftig keiner zweifeln: Je nach Abhängigkeit von der IT müssen die Systeme mit einer minimalen Downtime wieder funktionieren.

Allerdings sind die Business Continuity Maßnahmen noch um einen weiteren Aspekt zu ergänzen: Alle oder ein zu definierender Prozentsatz der Mitarbeiter, eventuell Kunden und Geschäftspartner brauchen jederzeit und auch von außerhalb Zugang zu ihren Daten und Anwendungen. In jedem Fall benötigen Notfallmitarbeiter im Notfall einen Zugriff auf die wichtigsten Datenbanken und Applikationsserver einer Organisation. Die Lösung dafür ist ein intelligent geplantes Remote Access Konzept.

Worauf ist bei modernen Remote Access Konzepten zu achten?

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

Die Anwendungen müssen entweder immer verfügbar oder im Notfall sofort aktivierbar sein und auch bei Spitzenbelastungen mit der gewohnten Performance funktionieren. Ganz wichtig ist hier, dass der Zugriff für Ungeübte einfach bedienbar ist, weil die IT-Administration in Krisensituation mit anderen Aufgaben alle Hände voll zu tun hat. Eine weitere Anforderung betrifft die Kosten: Da Totalausfälle eher selten vorkommen, ist zu überlegen, nicht für jeden potenziellen Benutzer mit eine Einzellizenz zu erweben, sondern eine Lösung zu wählen, die einen fallweisen Zugang ermöglicht.

Um den Zugriff von überall - im Extremfall auch von einem Internet-Café - aus zu ermöglichen, müssen die Zugänge Hardware-unabhängig sein. Dennoch - und das gilt für Home Offices gleichermaßen - gilt das Diktat der absoluten End-to-End-Sicherheit. Diese ist gerade in Notfällen wichtig, weil Unternehmen dann besonders leicht angreifbar sind. Die Sicherheitsregeln, z.B. der Login zur Authentifizierung, dürfen sich nicht oder nur wenig von dem gewohnten Prozedere unterscheiden, um in Stresssituationen Fehler zu vermeiden.

Werden unternehmenseigene oder private Rechner genutzt, sollten diese keine oder nur verschlüsselte Daten enthalten, damit im Verlustfall keine kritischen Informationen in falsche Hände gelangen.

Bedarf analysieren: Welches Remote Access Konzept?

Die Grundsatzfrage ist, ob die externen Zugänge und damit Arbeit z.B. im Home Office oder Hotel nur für den Krisenfall eingerichtet oder grundsätzlich in die Unternehmensphilosophie aufgenommen werden sollen. Dem entsprechend sind die Mitarbeiter bzw. Arbeitsplätze festzulegen, die den Fernzugriff nutzen.

Die technischen Voraussetzungen für den Remote Zugriff in Home Offices sind heute praktisch überall vorhanden: Nahezu jeder nutzt PCs und DSL-Anschlüsse, so dass die Tele-Arbeit jederzeit möglich ist. Soll oder muss der Mitarbeiter auch von (Dienst-) Reisen zugreifen, so können Notebooks oder PDAs genutzt werden. Für Notfälle gibt es PCs in Hotellobbys.

Hier allerdings ist zu bedenken, dass sich die beiden Zugangswege eigene oder fremder Rechner nicht völlig gleichen: Auf der eigenen Hardware kann auch Client-Software installiert werden, auf fremdem Systemen nicht. Insofern muss das Unternehmen 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.

Via SSL ohne Client-Software überall verbunden

Eine sehr sichere und zunehmend verbreitete Variante ist das SSL-Protokoll. SSL-Lösungen ermöglichen End-to-End-Verbindungen auf Applikationsebene, die in jeder Umgebung funktionieren und nur in wenigen Fällen geblockt werden.

Der große Vorteil einer SSL-Lösung ist, dass auf dem externen Rechner keine Installationen, Treiber oder Administratorrechte nötig sind. Erforderlich ist lediglich ein Browser. 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.

Administratoren benötigen in Krisenfällen für ihren Support den vollen Netzwerkzugriff, der durch das Point-to-Point-Protocol (PPP) möglich ist. Damit

können sie auch von fremden Rechnern aus unkompliziert auf die Netzwerkinfrastruktur, ja sogar ihre Desktops zugreifen. Alle Protokolle wie TCP, UDP oder ICMP werden automatisch durch den sicheren Tunnel geroutet.

Für den höchst möglichen Schutz unternehmenskritischer Daten sollte eine zusätzliche Sicherheitssoftware installiert werden, die den Client vor dem Zugriff nach bestimmten Kriterien wie z.B. Virenscanner überprüft.

Mobile USB-Sticks mit SSL-VPN

Eine weitere Remote Access Variante auf SSL-VPN Basis sind USB-Sticks, welche die Authentifizierung und in manchen Fällen auch den sofortigen Zugriff zum Firmen-Intranet bzw. in die Unternehmens-Cloud ohne vorherige Installation von Software oder Treiber ermöglichen. Dabei handelt es sich um installationslose Smartcard-Leser mit verschlüsseltem Speicher im USB-Produktformat, die eine hochsichere und einfache Kommunikation garantieren, während sie den Zugriff durch Dritte verhindern.

Voller Netzzugriff via IPsec VPN

Ist es seitens der IT-Strategie möglich, auf dem externen Endgerät eine Client-Software zu installieren, so kommt auch die standardisierte VPN-Technologie mit den Protokollfamilien IPsec und IKE/ISAKMP in Frage.

Für die relativ einfache Software-Installation kann die zentrale Administration im Rahmen eines unternehmensweiten Rollouts eine Client-CD für alle Remote-Rechner erstellen, die nach dem Start alle festgelegten Features automatisch installiert. Allerdings muss dies auf den Remote-Computern erlaubt sein. Auch werden mit IPsec Daten versandt, die nicht in jeder Infrastruktur ihr Ziel erreichen, weil preisgünstige Komponenten das IPsec-Protokoll oft nicht unterstützen.

Mobile Client Lösungen ohne Datendownload

Sollen für den Zugriff keine Rechner, sondern Mobiltelefone genutzt werden, gibt es auch dafür angepasste Client-Lösungen, die für die Darstellung auf kleinen Handy-Monitoren optimiert sind. Aus Sicherheitsgründen - so ein Smartphone geht schnell verloren - werden keinerlei Daten geladen, sondern während des Zugriffs nur die Bildschirminhalte übertragen.

Diese Remote Access Lösung basiert auf zwei Software-Komponenten: Der Mobil-Client wird auf dem Endgerät selbst installiert, im Unternehmen bzw. Ausweichrechenzentrum steht als „Gegenpart" ein spezieller Server im LAN oder Intranet. Diese Konfiguration erlaubt nach der Authentifizierung des Users den Zugriff auf alle Daten und Anwendungen.

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

Fazit

Krisensituationen kommen meist überraschend. In der Hektik wird so manche Fehlentscheidung getroffen - sei es für die unpassende Technik oder den falschen Realisierungspartner. Oft bedeutet dies anschließend zusätzlichen Arbeitsaufwand und/oder finanzielle Verluste.

Um den Geschäftsbetrieb auch aufrecht erhalten zu können, wenn die Mehrzahl der Mitarbeiter nicht an den Arbeitsplatz kommen kann, sollten Unternehmen zeitgerecht für einen Remote Access Zugang sorgen. Welche Lösung letztlich gewählt wird - SSL, IPsec VPN oder USB-Stick-Lösungen - muss jedes Unternehmen nach seinen Gegebenheiten entscheiden.

zurück