

Agil durch Fernzugang

Business-Continuity durch Zugriff von außen sichern

Nahezu drei Viertel der Deutschen möchten gerne von zu Hause aus arbeiten – dass dieser Wunsch eher unfreiwillig zum Zwang werden kann, beweisen derzeit diskutierte Maßnahmenpläne für den Fall einer ersten Influenza-Welle. Um die Business-Continuity für den erfolgreichen Betrieb auch von externen Standorten aufrechterhalten zu können, sollten Unternehmen rechtzeitig den Einsatz von Remote-Access-Lösungen erwägen.

Von Klaus Brandstätter, Cadolzburg

Die Diskussion, wie Unternehmen im Ernstfall einer Influenza-Pandemie ihre Business-Continuity aufrechterhalten und damit auch den in Gesetzen und Vorschriften beschriebenen Compliance-Anforderungen an eine gesicherte Geschäftsführung nachkommen, ist schon länger ein Thema: Bereits im August 2007 gab das Schweizer Pharmaunternehmen Roche bekannt, dass ein Notfallplan den Schutz der Mitarbeiter durch Arbeit von zu Hause aus vorsehe. „Der wichtigste Service, den wir definiert haben, ist der Remote-Zugriff unserer Mitarbeiter auf die Computer-Systeme“, erläuterte damals Roche-CIO Jennifer Allerton: „Im Falle des Ausbruchs einer Pandemie, wenn die WHO die höchste Alarmstufe – also Phase 6 – ausgerufen hat, soll lediglich eine Gruppe von 10 % der wichtigsten Mitarbeiter ihren Arbeitsplatz aufsuchen. Für den Rest müssen wir den Remote-Zugriff sicherstellen.“

Ebenfalls schon 2007 ergab allerdings eine Studie der Unternehmensberatung Mercer, dass nur 47 % der großen Unternehmen einen Notfallplan erstellt und nur

17 % ein Budget für die Pandemievorsorge eingeplant haben. Wo dies weiterhin nicht erfolgt ist, sollte man die aktuelle Diskussion rund um die H1N1-Grippe zum Anlass nehmen. Gartner-Analystin Roberta Witty warnte unlängst Unternehmen, sich auf das eigentliche Problem einer Pandemie vorzubereiten: Als größte Schwierigkeit sieht sie das massive Fernbleiben der Mitarbeiter von ihren Arbeitsplätzen.

Doch nicht nur Probleme im eigenen Land können Unternehmen beeinträchtigen, wie ein Fall Anfang Mai in Hongkong zeigte: Dort saßen Gäste in einem Hotel fest, weil die chinesischen Gesundheitsbehörden dieses aufgrund eines mexikanischen Gastes unter Quarantäne gestellt hatten. Gerät ein Manager mit wichtigen Entscheidungsbefugnissen in eine solche Situation, kann er mit Handy-Kommunikation alleine oft nicht viel ausrichten: Es fehlen schlicht die gewohnten Zugriffe auf die Systeme, die er bei seinen Geschäftspartnern oder an eigenen Firmenstandorten hätte. Ein beizeiten geplanter und eingerichteter Remote-Access auf Unter-

nehmenssysteme liefert sowohl im „Normalbetrieb“ auf Geschäftsreisen als auch bei außergewöhnlichen Umständen klare Vorteile.

BC mal anders

Im Zusammenhang mit Business-Continuity denkt man überwiegend zunächst an zutritts-sichere Rechenzentren, geschützte Datenbanken, Backup, Recovery, Ausweichräumlichkeiten und Wiederanlaufzeiten. Der Gedanke an nicht-verfügbare Mitarbeiter liefert dem Thema jedoch eine weitere Dimension – dabei sind zwei Ziele zu verfolgen: Erstens müssen alle wesentlichen Systeme auch von außen sicher zu betreiben und zu administrieren sein. Zweitens benötigt eine (große) Anzahl der Mitarbeiter die Möglichkeit, von zu Hause oder anderen räumlich entfernten Standorten zu arbeiten – und das so uneingeschränkt, als säßen sie an ihrem Firmenarbeitsplatz.

Organisationen, welche die Fortführung ihres gesamten Geschäftsbetriebs auch dann garantieren wollen, wenn im ungünstigsten Fall nur noch eine Rumpfmannschaft im Unternehmen vor Ort arbeiten kann, benötigen eine hochverfügbare, leistungsstarke und leicht bedienbare Remote-Access-Lösung. Dass sich damit nicht nur in kritischen Zeiten die Business-Continuity aufrechterhalten, sondern auch sonst die Attraktivität des Arbeitsplatzes und damit des gesamten Unternehmens erhöhen lässt, ist eine willkommene Begleiterscheinung. In vielen Fällen können die Nutzung von Home-Offices oder der Einsatz freier Mitarbeiter, die technisch voll ins Unternehmensgeschehen eingebunden sind, zudem auch Kosten sparen helfen.

Bedarf analysieren

Ob in einem Remote-Access-Projekt externe Zugänge nur für den Krisenfall eingerichtet werden oder

diese Möglichkeit grundsätzlich genutzt werden soll, ist eine der ersten Fragen, die es zu beantworten gilt. Dem entsprechend sind die Mitarbeiter beziehungsweise Arbeitsplätze festzulegen, für die ein Fernzugriff zur Verfügung stehen soll. Je nach Anforderungsprofil ist zudem zu überlegen, wie umfassend dieser Zugriff sein soll: nur auf den eigenen Arbeitsplatz oder auf alle Firmensysteme.

Schlussendlich stellt sich die Frage nach der Technik: Hier spielen die Themen Sicherheit, Verfügbarkeit, Performance und auch Kosten entscheidende Rollen. Denn das Internet bringt zwar Arbeitsplatz-Desktops und Systeme „virtuell“ in alle Welt, birgt aber auch Sicherheitsprobleme beziehungsweise Anforderungen hinsichtlich der Authentifizierung von Kommunikationspartnern sowie der Integrität und Vertraulichkeit übermittelter Daten.

Hilfe für diese ersten Analyseschritte bieten Systemhäuser oder Hersteller von Remote-Access-Lösungen üblicherweise in Form von Workshops an, in denen Spezialisten gemeinsam mit dem Kunden den genauen Bedarf ergründen. An derartigen Workshops sollten gegebenenfalls sowohl IT-Fachpersonal als auch Vertreter der einzelnen Fachabteilungen teilnehmen.

Die technischen Voraussetzungen für den Remote-Zugriff von daheim sind heute praktisch überall vorhanden: Nahezu jeder (zumindest mit IT vertraute) Mitarbeiter besitzt einen oder sogar mehrere PCs und nutzt DSL-Anschlüsse mit Flatrates, sodass auch in Krisenzeiten Tele-Arbeit jederzeit möglich sein sollte. Soll oder muss der Zugriff auch während (Dienst-) Reisen erfolgen, so kommen dafür Notebooks oder PDAs infrage – notfalls stehen oft auch einfache PCs in Hotellobbys oder Internetcafés zur Verfügung. Dabei allerdings ist zu bedenken,

dass die Zugangswege über eigene Systeme und fremde Rechner nicht gleichwertig sind: Während man auf eigener Hardware auch Client-Software installieren kann, ist dies auf fremden Systemen in der Regel nicht möglich. Hier sind bereits bei der Technikauswahl die einzelnen Vor- und Nachteile verschiedener Zugangsverfahren genau abzuwägen.

SSL ohne Client-Software

Eine zunehmend verbreitete Variante ist der Remote-Access via SSL-Protokoll: Deartige Lösungen ermöglichen End-to-End-Verbindungen auf Applikationsebene, die in (nahezu) jeder Umgebung funktionieren und nur in ganz wenigen Fällen geblockt werden. Der große Vorteil ist, dass man auf dem externen Rechner keinerlei besondere Installationen, Treiber oder Administratorrechte benötigt – als Plattform genügt der 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 übli-

cherweise ein Java-Applet und startet die gewünschte (Remote-)Applikation. Serverseitig sind meist spezielle Appliances oder Software-Lösungen im Einsatz, die für die Verbindung zu den gewünschten Applikationen sorgen.

Speziell Administratoren werden in Krisenfällen einen umfassenden Netzwerkzugriff benötigen. Hier ist bei der Auswahl der verwendeten SSL-Lösung darauf zu achten, ob dies – beispielsweise über PPP-Tunnel – zu realisieren ist. Für den höchstmöglichen Schutz unternehmenskritischer Daten ist überdies ein zusätzlicher Integrity-Check empfehlenswert, der den genutzten Client vor dem Remote-Zugriff nach bestimmten Kriterien (z. B. Aktualität/Vorhandensein eines Virens scanners) überprüft.

IPSec für vollen Netzzugriff

Der zweite anerkannte Fernzugang erfolgt per Virtual Private Network (VPN) mit den Protokollfamilien IPsec und IKE/ISAKMP: Ist ein solches VPN errichtet, ist der Anwender auch via Internet sicher

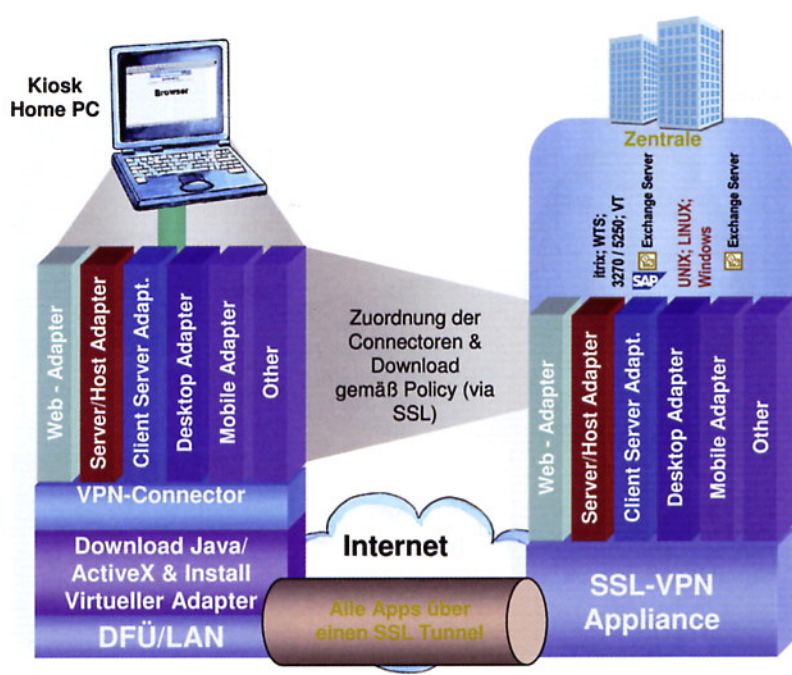


Abbildung 1: Der Fernzugang per SSL erfordert serverseitig eine Adaption an die jeweiligen Applikationen, auf dem Client jedoch üblicherweise weder Administratorrechte noch spezielle Software.

an die interne Netzwerkstruktur angebunden. IPSec arbeitet auf der Netzwerkebene (ISO/OSI-Layer 3) und stellt somit eine transparente Infrastruktur für alle IP-Protokolle zur Verfügung, die keine Adaption an konkrete Anwendungen erfordert.

IPSec, VPNs und ihre Administration müssen dabei nicht übermäßig kompliziert sein: Es gibt heute durchaus Lösungen, die einfach zentral zu implementieren und auch zu verwalten sind. Doch egal, ob das Roll-out manuell, aus der Lösung heraus oder per allgemeiner Software-distribution erfolgt: Zumindest einmalig sind auf den Remote-Computern Administrationsrechte erforderlich, um die VPN-Komponenten zu installieren. Zudem versendet IPSec Datenpakete, die nicht in jeder beliebigen Infrastruktur ihr Ziel erreichen: Preisgünstige Komponenten unterstützen das IPSec-Protokoll oft nicht.

Verschlüsselung mit Zertifikat

Gerade Krisensituationen sind leider ein idealer Nährboden

für Menschen, die mögliche IT-Sicherheitslücken suchen und für unberechtigte Zugriffe ausnutzen. Zudem mag ein Unternehmen in solchen Zeiten solche Übergriffe nicht sofort bemerken, weil schlicht andere Probleme im Vordergrund stehen. Zugriffe über öffentliche Netze sollten ohnehin grundsätzlich nur verschlüsselt erfolgen – hinsichtlich der genutzten Algorithmen und damit der Sicherheit des Fernzugangs bestehen keine prinzipiellen Unterschiede zwischen guten IPsec- und SSL-Lösungen. Bei entsprechendem Schutzbedarf kann es zudem sinnvoll sein, auf eine Evaluierung der eingesetzten Verschlüsselung nach den international anerkannten Common Criteria zu achten.

Berechtigungskonzept

Um hohe Sicherheitsanforderungen zu erfüllen, ist darüber hinaus sowohl für IPSec-VPNs als auch für SSL-Lösungen ein Berechtigungskonzept mit entsprechenden Authentifizierungslösungen erforderlich: entweder über User-ID/Passwort, Smartcards oder andere Hardware-Token oder auch Einmal-

passwort und Client-SSL-Zertifikate. Die eingesetzte Lösung sollte hier eine den Unternehmensanforderungen entsprechende Flexibilität aufweisen und eine zentrale Benutzerverwaltung mit Schnittstellen zu Verzeichnisdiensten (z. B. Active Directory, LDAP) ermöglichen.

Fazit

Krisensituationen kommen meist plötzlich und überraschend – in der dann vorherrschenden Hektik werden leicht Fehlentscheidungen getroffen, sei es für eine unpassende Technik oder den falschen Realisierungspartner. Oft bedeutet dies anschließend zusätzlichen Arbeitsaufwand oder finanzielle Verluste.

Um den Geschäftsbetrieb auch dann aufrechterhalten zu können, wenn die Mehrzahl der Mitarbeiter nicht mehr an den Arbeitsplatz kommen kann, sollten Unternehmen daher vorausschauend für eine passende Remote-Access-Lösung sorgen.

In vielen Fällen wird eine hochqualitative SSL-Lösung der optimale Weg sein, um einer Vielzahl von Nutzern unkomplizierten Zugang von beinahe beliebigen Systemen aus zu ermöglichen.

Wo Administratoren oder Anwender weiter gehende Rechte oder den Vollzugriff auf die gesamte Netzinfrastruktur benötigen, kann dies durch die Nutzung von Tunnel-Optionen oder die Einrichtung von IPsec-VPNs erfolgen – insofern können durchaus auch Mischlösungen sinnvoll sein.

Klaus Brandstätter ist Geschäftsführer der HOB GmbH & Co. KG in Cadolzburg bei Nürnberg.

Abbildung 2: IPsec-VPNs machen den Remote-Client zum Teil des internen Netzes, weswegen LANseitig ein entsprechendes Gateway genügt – auf den Clients ist jedoch üblicherweise eine Softwareinstallation erforderlich.

