

Fremdzugriff auf Unternehmen

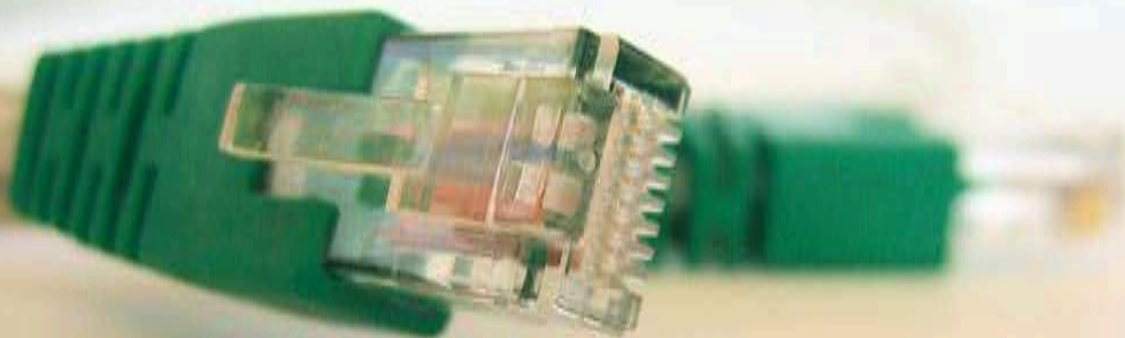
Den Zugriff auf Unternehmensdaten auch von außerhalb des Firmennetzes zu ermöglichen, ist zu einer gängigen Anforderung an die Unternehmens-IT geworden. Was auf den ersten Blick wie eine leicht durchschaubare Aufgabe wirkt, entwickelt sich bei konkreter Umsetzung zu einem Themenkomplex, der viele verschiedene Aspekte und Themenwelten berücksichtigen muss. Hier ein paar mögliche Betrachtungswinkel:

Identifikation des Anwenders und des Endgeräts

Aus Sicht des Anwenders ist die Grundforderung sehr einfach: Es muss nur funktionieren. Doch wer sind denn die Anwender? Das Spektrum reicht von eigenen MitarbeiterInnen, über Partner bis möglicherweise hin zu temporären Gastzugängen. Gefragt sind also Lösungen, die verschiedene Zugangsmöglichkeiten unter einem einheitlichen Konzept abbilden können. Möglicherweise reicht die Frage nach dem „wer?“ gar nicht aus, sondern auch das „Woher?“ kann eine entscheidende Rolle spielen. Während der Zugriff auf das Unternehmensnetzwerk von einem durch die IT gemanagten Gerät ein geplantes Szenario beschreibt, sollte sich der Funktionsumfang bei Anmeldung von einem Fremdrechner oder einem privaten PC deutlich restriktiver gestalten. Diesen Prozess nennt man Endpunkt-Analyse und kann auf diese Weise das Rechteprofil dynamisch erweitern oder einschränken, obwohl es sich immer um denselben Benutzer handelt.

Sicherheit aus logischer und technischer Sicht

Ein Zugriffsprofil ermöglicht den Zugang auf sensible Unternehmensressourcen – es muss also gewährleistet werden, dass niemand die Anmeldedaten ausspionieren oder den Datenverkehr mitschneiden kann. Als Universaltechnologie hat sich – gerade für den Zugriff über qualitativ schwankende Leitungstechnologien wie Funknetze oder UMTS – das SSL-Transportprotokoll (Secure Sockets Layer) etabliert. Es verhindert auf Basis von asymmetrischer Verschlüsselung, dass Datenpakete unbemerkt umgeleitet oder mitgeschnittene Informationen nachträglich entschlüsselt werden können (Man-in-the-Middle-Angriff). Jeder EDV-Benutzer ist damit schon in Berührung gekommen, wenn er aktiv im Internet Geschäfte getätigt hat – sei es die Online-Auktion, die Abfrage des Kontostands oder die Anmeldung am Webmail. So kann man relativ sicher sein, dass überall, wo das Browsen im Internet zur Verfügung steht, auch die Verbindung zu den Firmenressourcen möglich sein wird. Die technische Absicherung des Zugangs verhindert jedoch nicht den Missbrauch, wenn die logische Sicherheit vernachlässigt wird: Die Anmeldeformulare erlauben relativ freizügige Angriffe durch Ausprobieren verschiedener Passwörter (Wörterbuchattacken, Trivialkennworte, usw.). Als möglichem Ansatz bieten sich hier sog. Einmalpasswörter an, die von einem Schlüsselanhänger generiert werden, mit einer persönlichen PIN kombiniert sind und nicht vorausgeahnt werden können – so wird schwachen Anmeldekennungen das Missbrauchsrisiko genommen. Da diese Technik kontaktlos funktioniert, muss das Endgerät auch keine besonderen Voraussetzungen erfüllen.



nsdaten – aber sicher!

Flexible Anwendungszwecke

Der Zugriff auf Unternehmensressourcen kann verschiedene Informationsquellen umfassen: vom Zugriff auf beinahe jede denkbare Anwendung über Citrix-Terminaldienste, Browser-basierte Informationen wie Intranetportale, Dateitransfer oder allgemeine Webdienste, bis hin zu proprietären Protokollen wie E-Mail-Synchronisation für Laptops. Hier schließt sich auch wieder der Kreis zur Endpunktanalyse, d. h. die Funktionsmatrix verhält sich situationspezifisch granular. Die Lösung muss dann auch noch einsetzbar sein, ohne den Anwender mit Spezialkenntnissen über VPN-Technologien zu belasten.

Das Citrix Access Gateway bei BITMARCK

BITMARCK muss eine Vielzahl von Zugangsbedürfnissen umsetzen: Vom Vertrieb, über die Administration bis hin zum Partnerzugang für Test- und Pilotbenutzer im iskv_21c-System umfasst das Spektrum verschiedene Anwendungen und Szenarien. Mit dem Technologiekonzept des Citrix Access Gateway konnten die Anforderungen unter den dargestellten Kriterien ideal umgesetzt werden. Infolge der Erweiterung des mobilen Zugangs stieg zwangsläufig

auch die Erwartungshaltung an möglichst hohe Verfügbarkeit rund um die Uhr und minimale Wartungsfenster. Zum Einsatz kommt deshalb ein Doppelcluster des Citrix Access Gateway, der durchgängig umfassend redundant ausgelegt ist und seit der Inbetriebnahme unauffällig stabil läuft.

Über die Net.workers AG

Das Beratungshaus mit Stammsitz in Hagen agiert seit 1996 erfolgreich im IT-Markt und ist spezialisiert auf die Themen Datenkommunikation, IT-Sicherheit (ISO27001, BSI-Standard), Anwendungsbereitstellung und Infrastrukturtechnologien. Die übergreifende Betrachtung von IT-Lösungen vom Netz bis zum Anwendungsservice erlaubt die Durchführung komplexer IT-Projekte unter einer durchgängigen Leitung und Technologiekompetenz. Als Teil der Controlware-Gruppe mit über 350 MitarbeiterInnen in Deutschland agiert Net.workers als Competence-Center für das Geschäftsfeld Application Delivery und deckt damit Szenarien von Mittelstand bis hin zum Großkundenumfeld ab. Im Projektgeschäft verfügt Net.workers über höchste Hersteller- und Mitarbeiterzertifizierungen, beispielsweise bei Microsoft und Citrix.

<http://www.networkers.de>



Über den Autor

Thorsten Rood ist seit über 15 Jahren im IT-Beratungs- und Projektgeschäft tätig und arbeitet als Principal Architect für die Net.workers AG mit Fokus auf dem „dynamischen Rechenzentrum“. Er verfügt über Installationsreferenzen für mehrere tausend Anwender und Systeme weltweit agierender Unternehmen aller Branchen. Er ist außerdem regelmäßiger Sprecher auf IT-Fachkonferenzen für Application Delivery und Referent für Architekturfragen.

**Networkers AG
Gesellschaft für
Internet Technologie**

Firmensitz
Bandstahlstrasse 1
58093 Hagen

Registergericht
Amtsgericht Hagen, HRB 3350

Vorstand
Dr. Thomas Kretzberg,
Dipl.-Ökonom Bernd Schwefing

Aufsichtsratsvorsitzender
Dipl.-Ing. Helmut Woerner

<http://www.networkers.de>