Datenzugriffsrechte in Windows

In Windows kann direkt auf Daten eines anderen Computers zugegriffen werden. Das nennt man peer-to-peer Zugriff. Hierzu muß einfach eine Freigabe erzeugt werden und eine Zugriffskennung bekannt sein. Das dafür verwendete Protokoll ist das SMB (server message blocks) – Protokoll (1983, IBM).

Im Serverbetrieb spielt der peer-to-peer Zugriff wegen mangelnder Übersichtlichkeit und Datensicherheit keine Rolle.

Wichtige Daten sollten auf einer technisch dafür ausgerüsteten Maschine gespeichert sein. Schnelle Netzanbindung, robuste Hardware (z.b. redundante Netzteile), und ein schnelles, sicheres Festplattensystem (Raid) sind empfehlenswert.

In kleinen Netzen kann das der Domänencontroller sein, in größeren Netzen wird man einen separaten Fileserver (vielleicht ein geeignetes NAS) hierfür einsetzen.

Zum Verständnis des Daten-Sicherheitskonzepts von Windows muß man sich das grundliegende Bedienkonzept anschauen.

Es gibt hier die Unterscheidung in dedicated und non-dedicated Serversysteme. Ein dedicated Server kann nur einen speziellen Dienst, für den er optimiert ist, anbieten. Ein non-dedicated System kann mehrere Services anbieten.

Ein Zigarettenautomat ist ein klarer „dedicated"-Server. Da gibt's halt bloß Zigaretten.

Ein Kiosk mit Ausschank ist non-dedicated. Da können sie eine Zeitung kaufen, sich auch hinsetzen und ein Bier trinken, oder auch eine Bratwurst bestellen. Und Zigaretten hat er auch.

Windows hat(te) als Zielmarkt hautpsächlich den small-Office Bereich. Also kleine Netze, vielleicht bloß 10 Rechner.
In solchen kleinen Strukturen ist Anschaffung und der Betrieb von Servermaschinen für dedicated – Betrieb schlicht zu teuer.
Also ein Betriebssystem, das auch als Workstation genutzt werden kann. Quasi ein „normales" Windows, auf dem man auch mal irgendein Anwenderprogramm installieren kann.

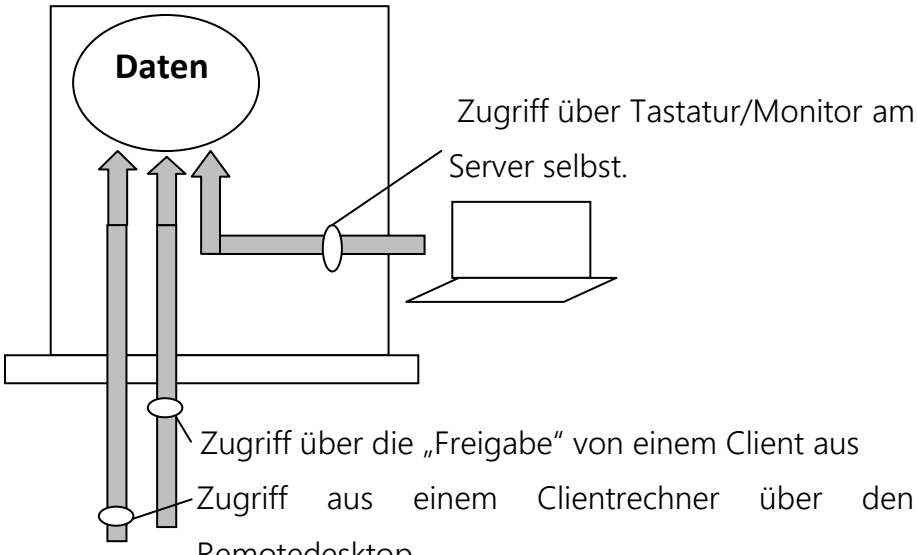
In anderen Systemen, Novell zum Beispiel, ist das nicht möglich. Auf einem Novell-Server kann keine Applikationssoftware – z.b. Textverarbeitung – installiert werden : ein dedicated Server !

Ein Nas ist auch ein dedicated Server.

Der dedicated Betrieb unterscheidet sich in Bezug auf die Datensicherheit wesentlich vom non-dedicated Betrieb.

Bei einem Server, dessen Daten ausschließlich über das Netz mit einem einzigen Protokoll zugegriffen werden können, genügt ein einziges Rechtesystem, das festlegt, wer wie auf die Daten zugreifen darf.

Bei dem non-dedicated Server „Windows“ gibt es aber viele verschiedene Zugriffswege auf Daten :



Die im dedicated-System existierende Zugriffsparametrierung entspricht hier den „Freigaberechten“, die den Zugriff über das SMB-Protokoll regeln. Aber sowohl der direkte Zugriff an der Maschine als auch der RDP-Zugriff umgehen diese Rechte ! Es braucht ein weiteres Rechtesystem, das die Daten schützt. Dazu werden Parameter direkt an die Daten auf der Speicher-platte drangeschrieben.

Freigaberechte :

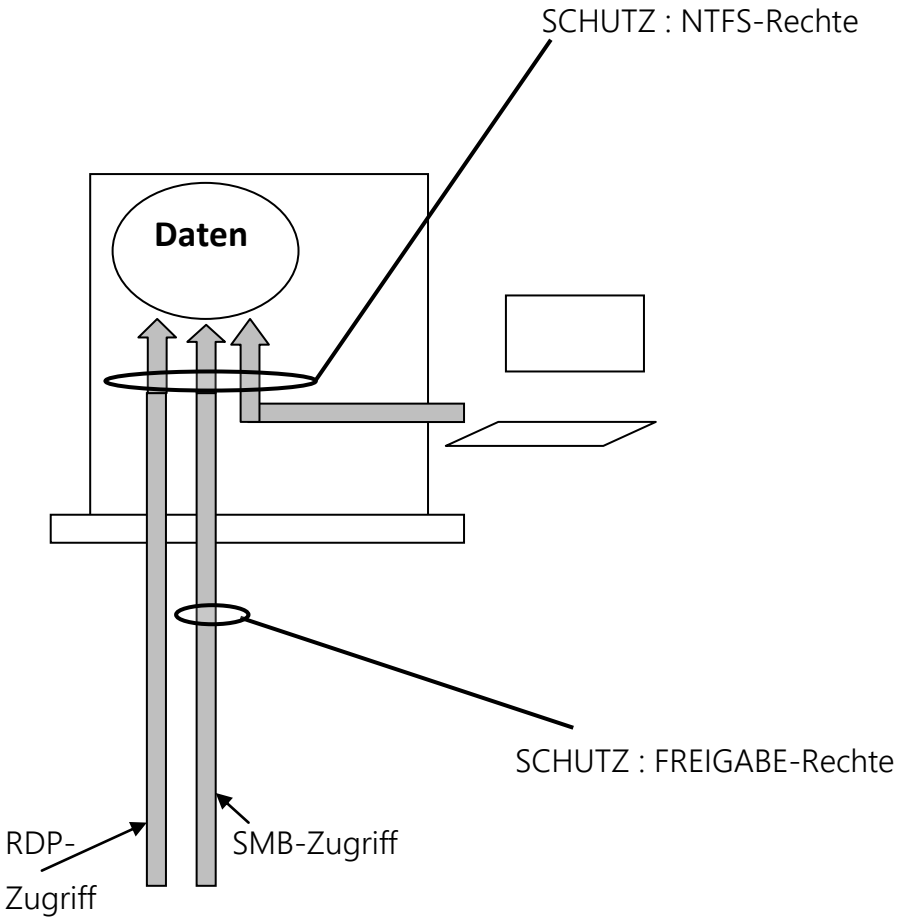
Wirken ausschließlich auf den Netzzugriff über das Freigabeprotokoll (SMB : server message blocks). Werden im System gespeichert, nicht als Attribute auf der Festplatte. Zugriffe über direkt angeschlossene Hardware (Terminal) oder die netzgestützten Terminal-Services (Remote Desktop : RDP-Protokoll) werden nicht beeinflußt !

NTFS-Attribute :

Sitzen als Filesystem-Attribute an den Daten der Festplatte. Administrierbar unter SICHERHEIT bei den Eigenschaften der Daten in Windows. Wirken auf alle Zugriffe.

Ein dedicated Server benötigt keine Attribut-Rechte, das macht ihn deutlich übersichtlicher !

Bei überlagerter Parametrierung (Freigaberechte und NTFS-Rechte auf das selbe Objekt) überwiegt immer die Einschränkung !


SCHUTZ : NTFS-Rechte
Daten
SCHUTZ : FREIGABE-Rechte
RDP-
Zugriff
SMB-Zugriff