

Mobiles Computing

für Systemadmins

Überblick

- Zugriffsoptionen
- Sicherheit
- Server-Setup / Information
- Client-Typen
- Client-Setup

Verbindungsoptionen

Verbindung

- Direkte Einwahl
- Transparente Verbindung

Zugriffsarten

- Direktzugriff auf (privilegierte) Systemconsole oder Console/Terminalserver mit Terminal-Emulation
transparenter Zugriff auf das System über einen Netzwerkdienst, z.B. per Terminal-Emulation (vt100, Citrix), RAS, WeBEM, Remote-Admin, etc)

Sicherheit (1)

- Client-System
 - Um sicher zu gehen, dass man überhaupt ein Client-System hat, muss man es stets mit sich herumschleppen. Auch wegen der fast unbegrenzten Möglichkeit, dass die Session überwacht, protokolliert oder manipuliert wird, wenn man auf Fremd-Hardware arbeitet (z.B. im Internet-Cafe), muss man den Client mit sich herumschleppen. Direktverbindunglesen von Passwörtern durch Direktverbindung praktisch nicht möglich. Back sichert vor Missbrauch durch Phreaker ab

Sicherheit(2)

- Transparente Verbindung
 - Verbindung kann von (fast) überall aufgebaut werden, ist nicht unbedingt auf ein Mobiltelefon angewiesen, eine Telefon-/ISDN-Leitung oder direkte Verbindung zum Internet reicht. Damit können schnellere Verbindungen zu geringeren Kosten aufgebaut werden. Passwörter können im Internet mitgelesen werden => verschlüsselte Verbindung ist zwingend erforderlich (z.B. vpn, ssh,)

Server-Setup

- Überwachung
 - Server müssen sich selber überwachen und bei Erreichen von Schwellwerten Alarm geben, bevor der Anwender etwas merkt (z.B. per SMS via email-SMS-Gateway)ichtige Server müssen von anderen Systemen überwacht werden, damit ein Totalausfall bemerkt wird die Überwachung muss Intelligenz investiert werden , ping reicht selten aus Überwachung muss protokolliert werden. riffote-Admin muss geübt werden Environment des Admin muss entsprechend eingerichtet werden.

Firewalls

- Für Systeme, die mit dem Internet verbunden sind und auf die transparent zugegriffen werden soll, ist die Absicherung mit einer Firewall unverzichtbar. Alles andere kann zivil- und arbeitsrechtliche Konsequenzen nach sich ziehen. Die alte Firewall-Weisheit: „so viel, wie nötig aber so wenig wie möglich“ frei zu geben, gilt auch hier.