

## Zusammenfassung

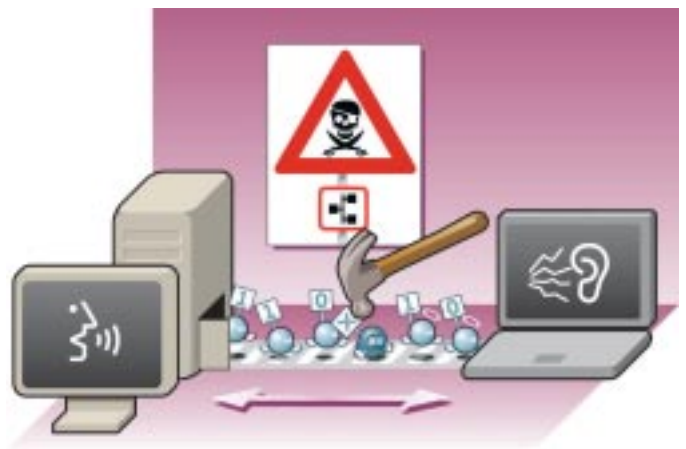
Aus zahlreichen Gründen, wozu unter anderem die Einführung leicht zu bedienender Softwareprogramme (Samba etc.) gehört, nimmt die Nutzung des Internets zur gemeinsamen Nutzung von Ressourcen zu.

Das gängigste und bekannteste Verfahren des unbefugten Zugriffs

auf einen Computer ist zweifellos die Nutzung von Funktionen zur gemeinsamen Nutzung von Ressourcen, die aus Unachtsamkeit und Unwissenheit nicht deaktiviert wurden. Diese Nachlässigkeit ermöglicht es einem Cracker, die Kontrolle über Ihren Rechner zu übernehmen und Daten und Ressourcen zu verändern.

## Inhalt

- 1 Das SMB/CIFS-Protokoll →
- 2 Potenzielle Risiken der gemeinsamen Nutzung von Ressourcen →
- 3 Wer ist betroffen? →
- 4 Bin ich den Gefahren der gemeinsamen Nutzung von Ressourcen ausgesetzt? →
- 5 Wie können Sie sich schützen? →
- 6 Anhang →



## 1 Das SMB/CIFS-Protokoll

Um Ressourcen in einem Netzwerk gemeinsam nutzen zu können, ist unabhängig davon, ob es sich um ein öffentliches oder privates Netzwerk handelt, die Verwendung eines Protokolls über die Bereitstellung oder Anforderung dieser Ressourcen erforderlich. Dieses höhere Protokoll wird von den gängigen Transport-/Kommunikationssteuerungsprotokollen wie etwa TCP/IP, Netbios, IPX etc. über das gesamte Netzwerk übertragen.

Das SMB-Protokoll (Server Message Block) wird für die gemeinsame Nutzung von Dateien, von am seriellen Port angeschlossenen Druckern und von Kommunikationsverbindungen des Typs "Named Pipe" verwendet. Dieses von IBM entwickelte Protokoll wurde Mitte der 80er Jahre eingeführt. Danach wurde es von Intel und Microsoft übernommen.

### ► SMB ist ein Client/Server-Protokoll

Dieses Protokoll basiert auf der "Request-Antwort"-Kommunikation zwischen einem SMB-Client und einem SMB-Server. Auf diese

Weise stellen die Server Ressourcen im Netzwerk zur Verfügung. Der Client baut eine Verbindung zum SMB-Server auf, dann ermittelt er über ein anderes Protokoll die verfügbaren Ressourcen, und anschließend kann er den Zugriff auf diese gemeinsam genutzten Ressourcen (Laufwerke, Peripheriegeräte etc.) anfordern.

### ► CIFS - common internet file system

CIFS ist die Weiterentwicklung des SMB-Protokolls. Dieses neue Protokoll wird ab MS Windows 2000 genutzt, um die gemeinsame Nutzung von Dateien und Peripheriegeräten in IP-Netzwerken zu ermöglichen. CIFS wird von den meisten EDV-Systemen wie etwa Linux, Unix, MS Windows NT, MS Windows 98, MS Windows 95, MS OS2 Lan Manager etc. unterstützt. Diese Weiterentwicklung wurde für die gemeinsame Nutzung von Ressourcen über das Internet optimiert.

## 2

## Potenzielle Risiken der gemeinsamen Nutzung von Ressourcen

Die gemeinsame Nutzung von Ressourcen kann die im Computer gespeicherten Daten aber auch Peripheriegeräte wie etwa Drucker oder jedes andere an die seriellen-, parallelen oder USB-Ports angeschlossene Gerät betreffen. Dieser Zugriff beschränkt sich nicht unbedingt nur auf die Betrachtung oder Nutzung dieser Ressourcen, sondern möglicherweise auch auf deren Änderungen oder Entfernung bzw. Abschaltung.

Da die gemeinsame Nutzung von Ressourcen natürlich das Hauptziel der Errichtung eines lokalen Netzwerks darstellt, ist die Bereitstellung eben dieser Ressourcen auf dem Präsentierteller nicht ratsam. Zu den möglichen Konsequenzen eines derartigen Vorgehens gehören:



## Mögliche Konsequenzen

- **Betrachtung, Diebstahl oder Vernichtung von Daten**
- **Beschädigung von Systemdateien**
- **Diebstahl von UIDs/Passwörtern (UID = User-ID = Benutzername)**
- **Denial of Service-Angriffe**
- **Virusinfektionen**
- ...

## 3

## Wer ist betroffen?

Alle Bürger, KMUs und Behörden die über ein öffentliches oder ein privates Netzwerk Ressourcen oder Daten, durch die Funktion der gemeinsamen Nutzung, zur Verfügung stellen, wissend oder unwissend.

## 4

## Bin ich den Gefahren der gemeinsamen Nutzung von Ressourcen ausgesetzt?

Es muss zwischen Einzelplatz-Anwendern, die normalerweise keinen Grund haben, die gemeinsame Nutzung von Ressourcen zuzulassen, und den an ein lokales Netzwerk angeschlossenen Anwendern unterschieden werden. Sie sollten jedoch wissen, dass bestimmte EDV-Systeme (Betriebssysteme) standardmäßig Funktionen zur gemeinsamen Nutzung von Ressourcen aktivieren.

Um zu ermitteln, ob Ihr Rechner derartigen Gefahren ausgesetzt ist, sollten Sie das Konfigurationsmenü Ihres Netzwerks aufrufen

und überprüfen, ob die Funktion "Gemeinsame Nutzung von Dateien und Druckern" aktiviert ist. Ist dies der Fall, so sind Sie ein potenzielles Ziel für Cracker.

Um Ihre Konfiguration zu überprüfen, können Sie auch einen Test ausführen, den Sie unter folgender Adresse finden:

<http://security.symantec.com/sscv6/>

## 5

## Wie können Sie sich schützen?

► Wenn Sie über einen Einzelplatzrechner verfügen:

Wenn Ihr Computer nicht an ein lokales Netzwerk angeschlossen ist, ist es am besten,

→ **die Funktion der gemeinsamen Nutzung von Dateien und Druckern zu deaktivieren.**

Im Anhang sind die abhängig vom Betriebssystem Ihres Computers auszuführenden Schritte beschrieben.

### ▶ Wenn Ihr Computer an ein lokales Netzwerk angeschlossen ist

Falls Sie diese Funktionalität wirklich benötigen, empfehlen wir Ihnen die Befolgung der nachfolgend aufgeführten Empfehlungen:

- ▶ **Nutzung einer Firewall** oder Parametrierung der Firewall-Funktion von MS Windows XP, um das Protokoll zur gemeinsamen Nutzung von Dateien auf Ihr lokales Netzwerk zu beschränken und um jegliche Ausbreitung über öffentliche Netzwerke zu verhindern (Ports 445, 135, 137, 138, 139).
- ▶ **Erstellen Sie ein einziges gemeinsam genutztes** Laufwerk im Stammverzeichnis Ihrer Festplatte und schützen Sie den Zugriff durch ein sicheres Passwort.
- ▶ **Löschen Sie das Benutzerkonto** "Gast" Ihres Systems und schützen Sie alle anderen Benutzerkonten durch sichere Passwörter und eine Sperre des Benutzerkontos nach einer gewissen Anzahl an falschen oder unbefugten Zugriffsversuchen.
- ▶ **Achten Sie darauf, dass die Virenschutz-Plattform immer aktiv** und auf dem neuesten Stand ist, um die Ausbreitung von Viren zu verhindern.
- ▶ **Verwenden Sie, um ein Minimum an Anonymität zu wahren**, soweit dies möglich ist eine dynamische IP-Adressenvergabe und vermeiden Sie die Nutzung von unveränderlichen IP-Adressen.

## 6

## Anhang

### 6.1 Deaktivierung unter MS Windows XP

- ▶ **Deaktivieren Sie das Netbios-Protokoll** in den Eigenschaften der verwendeten Fernverbindung. Lesen Sie auch Praktisches - Lösungen Firewall unter Windows XP
- ▶ **Nutzen Sie die Firewall-Funktion** von MS Windows XP. Lesen Sie auch Praktisches - Lösungen Deaktivieren unter Windows XP

**Tip:** Wenn Ihr Computer ein Einzelplatzrechner ist, können Sie außerdem die gemeinsame Nutzung von Dateien auf der Ebene Ihres lokalen Netzwerks deaktivieren:



### 6.2 Deaktivierung unter MS Windows 2000

- ▶ **Deaktivieren Sie das Netbios-Protokoll** in den Eigenschaften der verwendeten Fernverbindung. Lesen Sie auch Praktisches - Lösungen Deaktivieren unter Windows 2000

**Tip:** Wenn Ihr Computer ein Einzelplatzrechner ist, können Sie außerdem die gemeinsame Nutzung von Dateien auf der Ebene Ihres lokalen Netzwerks deaktivieren:

