# Schriftliche Ausarbeitung im Fach Internet Security: SMB / CIFS Sicherheit

von Mario Bacic

am 27.06.04

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# 1 Einführung

Das **Server Message Block** (= SMB) Protokoll wurde zu Beginn der 80'er Jahre von IBM, Microsoft und Intel entwickelt. Seit dieser Zeit wurde es von Microsoft stetig erweitert und dient heute als Grundlage für die Datei- und Drucker-Freigabe in allen Windows-Versionen. Im Jahre 1997 wurde das Protokoll durch Microsoft in **Common Internet File System** (= CIFS) umbenannt und teilweise durch einen Internet Draft dokumentiert (vgl. [1]). Schon zuvor wurden grobe Funktionsabläufe des Protokolls durch ein offizielles Dokument offen gelegt (vgl. [2]).

Das SMB Protokoll verfolgt einen Client – Server Ansatz. Dabei ist der Client der Initiator der Kommunikation und sendet eine spezifische Anfrage an den Server, worauf dieser eine Antwort zurücksendet. Im folgenden wird kurz auf die grundlegenden Eigenschaften und Erweiterungen des SMB Protokolls eingegangen. Danach werden mögliche Sicherheitsrisiken im Detail erläutert.

## 1.1 Die NetBIOS Schnittstelle

Ältere SMB Implementierungen setzen auf der **Network Basic Input Output System** (= NetBIOS) Schnittstelle auf. Diese wurde im Jahre 1985 von IBM entwickelt, um Anwendungen eine plattformunabhängig Kommunikation innerhalb eines Netzes zu ermöglichen. Die Schnittstelle bietet grundlegende Methoden für den Sitzungsaufbau und den Dateitransfer zwischen zwei Rechnern. Zwei **Requests for Comments** (= RFC) beschreiben die NetBIOS Schnittstelle und den Einsatz von TCP/IP als Transportprotokoll detailliert (vgl. [3, 4]).

NetBIOS besitzt drei Bestandteile. Der **NetBIOS Name Service** (= NBNS) enthält ein Namensverzeichnis aller NetBIOS Netzteilnehmer mit ihrer jeweiligen IP Adresse. Zum Austauschen von Kontrollinformationen wird der **NetBIOS Datagram Service** (= NBDS) benutzt. Schließlich bietet der **NetBIOS Session Service** (= NBSS) einen zuverlässigen Sitzungsdienst an, durch welchen Nutzdaten zwischen verschiedenen Rechnern transportiert werden können.

Jeder Teilnehmer wird in einem NetBIOS Netz durch einen eindeutigen Namen identifiziert, der insgesamt 16 Zeichen lang sein darf. Davon können 15 Zeichen vom Benutzer gewählt werden. Das letzte Zeichen wird durch den lokalen NBNS vergeben und beschreibt eine

Eigenschaft des Netzteilnehmers.

## 1.2 Authentisierungsverfahren

Das SMB Protokoll unterstützt insgesamt zwei Sicherheitsmodelle. Zum einen ist es möglich, den Zugriff auf eine Freigabe über ein freigabespezifisches Passwort sicherzustellen. Außerdem können auch auf Benutzerebene Zugriffsrechte gewährt und entzogen werden. In allen aktuellen Microsoft-Implementierungen wird ausschließlich das zweite Sicherheitsmodell unterstützt. Unabhängig vom Sicherheitsmodell kann die Übertragung des Passwortes unverschlüsselt oder mit Hilfe des **Challenge-And-Response**-Verfahrens verschlüsselt erfolgen. Beim **Challenge-And-Response**-Verfahren sendet der Freigabeserver eine zufällig gewählte Zeichenkette, den so genannten Challenge Code, an den Client. Dieser berechnet mit Hilfe eines Verschlüsselungsverfahrens und des Passwortes eine Zeichenkette, den so genannten Response Code, und sendet diesen an den Server zurück. Der Server erzeugt ebenfalls einen Response Code und vergleicht ihn mit dem vom Client empfangenen. Falls beide Response Codes übereinstimmen, weiß der Server, dass in beiden Fällen das gleiche Passwort als Grundlage diente und kann somit den Benutzer erfolgreich authentisieren.

Das SMB Protokoll unterstützt verschiedene **Challenge-And-Response**-Verfahren, die alle zwei Phasen enthalten. In der ersten Phase wird nach einem bestimmten Verfahren aus einem Passwort ein so genannter Hash Wert erzeugt. Anschließend wird in der zweiten Phase mit Hilfe des Hash Wertes der Challenge Code verschlüsselt. Häufig wird das Ergebnis der ersten Phase zwischengespeichert um den Gesamtprozess zu beschleunigen. Beide Phasen werden, wie erwähnt, jeweils auf dem Client und dem Server durchlaufen. Die vom ursprünglichen SMB Protokoll unterstützten Verfahren werden nun näher erläutert.

### 1.2.1 LAN Manager

Der älteste Algorithmus, welcher zum Generieren einer Response eingesetzt wird, ist der sog. **LAN Manager** (= LM) Algorithmus. Dieser basiert auf einem Passwort, welches maximal 14 Zeichen lang sein darf. Dabei entspricht ein Zeichen genau einem Byte.

In der ersten Phase wird das Passwort, wenn es nicht 14 Zeichen lang ist, entweder mit '0'-Bytes aufgefüllt oder entsprechend verkürzt. Danach wird es in zwei, je sieben Zeichen lange, Hälften geteilt. Außerdem werden alle Kleinbuchstaben der Passworthälften in Großbuchstaben konvertiert. Zuletzt wird jede Passworthälfte als Schlüssel benutzt um eine Zeichenkette, die als Magic Word bezeichnet wird, mit Hilfe der **Data-Encryption-Standard**-Funktion

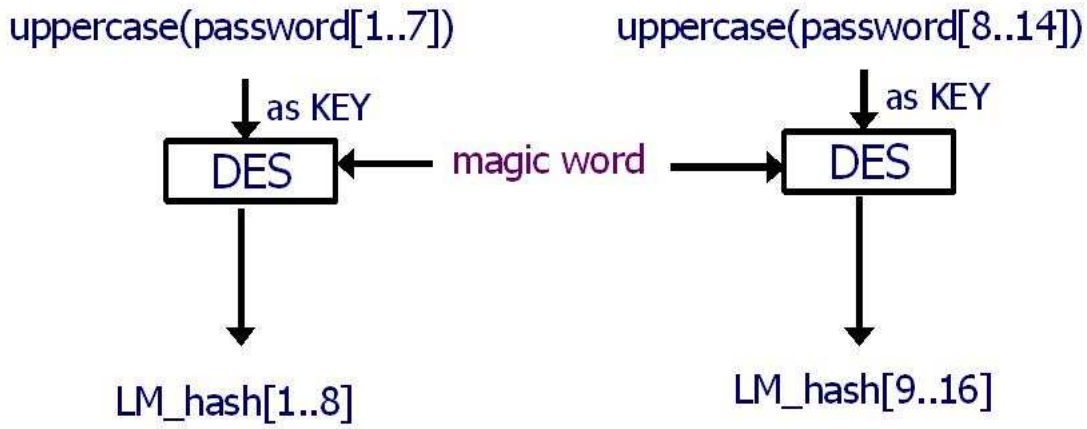


Abbildung 1.1: Generierung des LM Hash Wertes aus einem Passwort

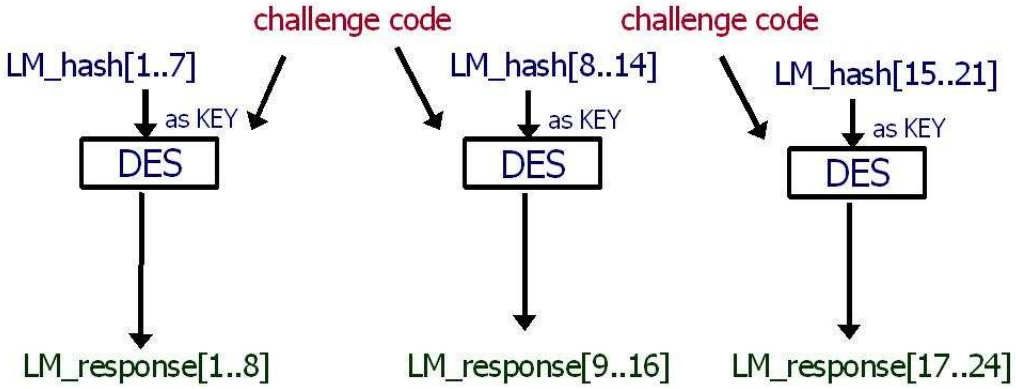


Abbildung 1.2: Erzeugen eines Response Codes

(= DES) zu verschlüsseln. Als Ergebnis erhält man dabei zwei jeweils acht Zeichen lange Hash Hälften. Die Abläufe der ersten Phase sind in Abbildung 1.1 dargestellt.

Die beiden Hash Hälften werden zu Beginn der zweiten Phase zu einem Hash Wert zusammengefasst und anschließend mit fünf “0”-Bytes aufgefüllt. Der nun 21 Byte lange Hash Wert wird in drei Teile zu je sieben Bytes aufgeteilt. Dann wird der Challenge Code dreimal mit der DES Funktion verschlüsselt. Als Schlüssel dienen dabei abwechselnd die drei Hash Teile. Man erhält drei Teile des Response Code mit einer Länge von je acht Bytes. Das Verfahren wird in Abbildung 1.2 skizziert.

### 1.2.2 NT LAN Manager

Mit der Einführung von Windows NT wurde auch ein neues **Challenge-And-Response**-Verfahren eingeführt. Das **NT LAN Manager** (= NTLM) benannte Verfahren ähnelt dem LM Verfahren

sehr. In der ersten Phase des Verfahrens gibt es lediglich zwei Änderungen.

Als erste Neuerung wird anstelle der DES Funktion bei der Hash Wert Generierung die **Message-Digest-4**-Funktion (= MD4) benutzt, welche in RFC 1320 beschrieben wird (vgl. [5]). Dadurch müssen Passwörter, die kürzer als 14 Zeichen sind, nicht mit Füllzeichen ergänzt werden um einen Hash Wert mit 16 Byte Länge zu erzeugen.

Außerdem wird das Passwort nicht in Grossbuchstaben konvertiert.

## 1.3 Erweiterungen des SMB Protokolls

Microsoft hat im Laufe der Jahre das Protokoll stetig weiterentwickelt und es schließlich in CIFS umbenannt. Dazu wurde auch ein Internet Draft bei der **Internet Engineering Task Force** (= IETF) eingereicht (vgl. [1]). Die grundlegendste Neuerung ermöglicht es, CIFS direkt über das TCP/IP Protokoll zu betreiben. In diesem Fall wird die NetBIOS Schnittstelle nicht mehr benötigt. Dazu wird der Namensdienst NBNS durch das **Domain Name System** (= DNS) ersetzt.

Es wurde außerdem ein neuer Authentisierungsalgorithmus eingeführt, der allgemein als **NT LAN Manager Version 2** (= NTLMv2) bezeichnet wird. Dieser benutzt den MD4 Algorithmus um einen Hash Wert und den MD5 Algorithmus um eine Response zu erzeugen.

Daneben existieren jedoch auch Erweiterungen, welche nicht ausreichend dokumentiert sind. Die Möglichkeit, SMB-Pakete zu signieren, wird beispielsweise von neueren Microsoft-Implementierungen angeboten, obwohl das Verfahren nicht in der Spezifikation erläutert wird.

# 2 Sicherheitsrisiken

Im Folgenden wird auf einzelne Sicherheitsrisiken eingegangen, die sich durch die Verwendung des **Common Internet File Systems** ergeben können. Einige Risiken lassen sich minimieren, andere jedoch nicht, ohne die Kommunikation zweier Hosts empfindlich zu stören oder gar unmöglich zu machen.

## 2.1 Ausspähen von Informationen über den NetBIOS Name Service

Die Informationen über Freigabedienste aller Hosts eines Netzes können mit Hilfe des NetBIOS Name Services verwaltet werden. Es existieren jedoch keine Mechanismen um einzelne Informationen eines Hosts zu verbergen oder einen Host gänzlich in der Liste zu verstecken. Folglich können beteiligte Rechner alle zur Verfügung gestellten Informationen einsehen und auswerten.

Die NetBIOS Namenstabelle, die jeder NetBIOS Netzteilnehmer lokal erzeugt, enthält neben allgemeinen Informationen, wie dem Rechnernamen und dem Namen der Arbeitsgruppe bzw. der Computerdomäne auch einige Informationen, die Aufschluss über die Arbeitsumgebung auf dem Rechner selbst geben können. So wird auch angezeigt, ob auf dem Rechner der Dateifreigabedienst oder der NetBIOS Nachrichtendienst aktiv ist. Bei aktiviertem Nachrichtendienst erfährt man außerdem den Namen des gegenwärtig angemeldeten Computerbenutzers. Es sind auch Informationen in den Namenstabellen zu finden, welche die Netztopologie betreffen. So können Rechner, welche die Funktion des Domänencontrollers übernehmen, ebenso eindeutig identifiziert werden. Ein Angreifer könnte auf diese Weise abstufen, welche Rechner im Netz ein lohnenswertes Ziel darstellen.

## 2.2 Schwächen der Authentisierungsverfahren

Wie bereits in Kapitel 1.2 auf Seite 5 erläutert wurde, garantiert das **Challenge-And-Response**-Verfahren, dass eine Authentisierung erfolgen kann, ohne Passwörter im Klartext zu übertragen. Die Schwächen der ursprünglichen **Challenge-And-Response**-Verfahren werden nun im Bezug auf ein Abhören der Kommunikation erläutert.

### 2.2.1 LAN Manager

Wenn man das LM Verfahren, welches bereits in Kapitel 1.2.1 auf Seite 5 erklärt wurde, näher betrachtet, stößt man auf mehrere Details, die es unsicher erscheinen lassen.

Eine Schwäche bildet die Konvertierung des Passwortes in Großbuchstaben. Dies geschieht in der ersten Phase und zwar vor der Erzeugung des Hash Wertes. Durch die Tatsache, dass keine Kleinbuchstaben als Basis für die DES Verschlüsselungsfunktion auftreten können, wird der Schlüsselraum reduziert. Je kleiner der Schlüsselraum jedoch ist, desto mehr kann ein Bruteforce-Angiff beschleunigt werden.

Eine weitere Schwäche bildet die Teilung des Passwortes vor der Erzeugung des Hash Wertes. Bei Passwörtern, die kürzer als 14 Zeichen sind, werden “0”-Bytes aufgefüllt. Falls auf diese Weise eine ganze Passworthälfte aufgefüllt wird, entsteht in der korrespondierenden Hash Hälfte eine konstante Bytefolge. Ferner werden in der zweiten Phase fünf weitere “0”-Bytes hinzugefügt. Nun wird ein Problem des LM Verfahrens sichtbar. Wenn die Passwortlänge sieben Zeichen oder weniger beträgt, besitzen 13 Bytes von insgesamt 21 Bytes, die zur Erzeugung der LM Response benutzt werden, einen konstanten, bekannten Wert. Diverse Sicherheitsprogramme nutzten diese Tatsache, um den Schlüsselraum zu minimieren und einen Angriff zu beschleunigen.

Eine weitere Schwäche ergibt sich aus der Tatsache, dass der LM Hash Wert aus zwei jeweils sieben Zeichen langen Passworthälften erzeugt wird und nicht aus einem 14 Zeichen langen Passwort. Dies ermöglicht es, beide Passworthälften unabhängig voneinander mit sieben Zeichen langen Zeichenketten anzugreifen. Bei einem Bruteforce-Angriff müssen so weniger Möglichkeiten durchprobiert werden als für ein 14 Zeichen langes Passwort.

### 2.2.2 NT LAN Manager

Der NTLM Algorithmus ist dem LM Algorithmus sehr ähnlich. Es wurden jedoch Veränderungen eingebaut, welche einige Schwächen des LM Verfahrens beheben.

So wird anstelle der DES Funktion bei der Hash Wert Generierung die MD4 Funktion benutzt. Dadurch entfällt das Auffüllen oder Abschneiden eines Passwortes auf eine spezifische Länge. Dies hat auch zur Folge, dass in dem erzeugten NTLM Hash Wert keine konstanten Zeichenfolgen auftreten. Aus dem Hash Wert können dadurch keine Rückschlüsse mehr über die Länge des zugrunde liegenden Passwortes gewonnen werden.

Neu hinzugekommen ist außerdem, dass bei der Generierung des NTLM Hash Wertes das Passwort nicht in Grossbuchstaben konvertiert wird. Dadurch erhöht sich die Sicherheit in Bezug auf Bruteforce- oder Wörterbuch-Angriffe erheblich. Es müsste jeder Buchstabe sowohl in der Groß- als auch in der Klein-Schreibung durchprobiert werden.

Insgesamt ist der erzeugte NTLM Hash Wert robuster gegen Angriffe als der LM Hash Wert und folglich ist es der daraus erzeugte NTLM Response Code auch. Allerdings wird in der zweiten Phase des Verfahrens der Response Code wie im LM Algorithmus mit Hilfe einer DES Verschlüsselungsfunktion generiert, und besitzt somit eine Schlüsselstärke von lediglich 56 Bit, welche heutzutage nicht mehr als sicher gilt.

## 2.3 Schwächen im Protokolldesign

Trotz der vielen Sicherheitserweiterungen, die in dem SMB bzw. CIFS Protokoll realisiert worden sind, haben sich einige Risiken nicht minimiert. Im Folgenden sollen die wesentlichen Gefahren erläutert werden, welche direkt mit der Grundfunktionsweise des Protokolls zusammenhängen.

### 2.3.1 Anonymer Zugriff auf “IPC$” Freigabe

Ein wichtiger Bestandteil des CIFS Protokolls bildet die Freigabe mit dem Namen “IPC$”. Diese muss auf jedem Rechner existieren, der Freigabedienste anbietet. Des weiteren muss ein anonymer Zugriff darauf möglich sein, damit der Freigabedienst einwandfrei funktioniert. Zwischen zwei Hosts wird diese Freigabe größtenteils dazu benutzt, um die Liste aller Rechnerfreigaben in Erfahrung zu bringen. Ein weiterer Nutzungsaspekt ist die Überprüfung der Domänenzugehörigkeit eines Benutzers. Dies kann beispielsweise in zwei benachbarten Computerdomänen sinnvoll sein, wenn ein Domänencontroller prüfen will, ob ein Benutzer der Nachbardomäne angehört. Dazu wird die Liste der Benutzerkonten mit Hilfe der “IPC$” Freigabe des Nachbardomänencontrollers in Erfahrung gebracht.

Ein Ausspähen der Benutzerkonten bietet jedoch Angreifern Ansatzpunkte für weitere Aktivitäten. Es kann auch eine **Denial-of-Service-**Attacke (= DoS) durchgeführt werden, indem

die Benutzerkonten durch zu viele fehlgeschlagene Anmeldeversuche vom System gesperrt werden. Deswegen stellt der anonyme Zugriff auf die “IPC$” Freigabe ein Sicherheitsrisiko für jeden Rechner dar.

### 2.3.2 Kein Aushandeln des Authentisierungsverfahrens

In der Geschichte des CIFS Protokolls wurde eine Reihe von inkompatiblen Authentisierungsalgorithmen eingeführt. Es wurde jedoch kein Mechanismus entwickelt, der ein Aushandeln des Authentisierungsverfahrens ermöglicht. Lediglich an einer Stelle wird in den SMB Paketen angezeigt, ob das **Challenge-And-Response**-Verfahren unterstützt wird. Der verwendete Algorithmus ist vielmehr von der Protokollversion abhängig. Ältere Hosts, welche eine der ersten Protokollvarianten benutzen, verwenden keine Verschlüsselung und somit auch kein **Challenge-And-Response-**Verfahren. Spätere Implementierungen benutzen standardmäßig das LAN Manager oder das NT LAN Manager Verfahren. Dies hat in der Praxis Sicherheitseinschränkungen zur Folge.

Ein Großteil aller weltweit vorhandenen Clients erzeugt beim **Challenge-And-Response**-Verfahren sowohl eine LM- als auch eine NTLM-Response. Dies erfolgt aus Gründen der Abwärtskompatibilität zu Implementierungen älterer Clients. Es soll damit sichergestellt werden, dass mindestens eine Response auf dem älteren Client korrekt verarbeitet werden kann. Da bereits in Kapitel 2.2.1 auf Seite 9 die Schwächen des LM Verfahren erläutert wurden, stellt dieser Sachverhalt ein Sicherheitsrisiko dar. Es existieren sogar Sicherheitsprogramme, welche das großgeschriebene Passwort mit Hilfe einer LM Response in Erfahrung bringen können, um anschließend mit Hilfe der NTLM Response die korrekte Groß- und Klein-Schreibung zu erfahren. Das NTLM2 Verfahren wird standardmäßig nicht angewendet, um eine Response zu generieren. Damit eine NTLM2 Response erzeugt wird, müssten Veränderungen an jedem beteiligten Host PC durchgeführt werden.

### 2.3.3 Hash Wert ist Passwortäquivalent

Im **Challenge-And-Response**-Verfahren wird mit Hilfe des Hash Wertes und des Challenge Codes eine Response generiert. Dieses Verfahren verhindert, dass Passwörter im Klartext übertragen werden. Bei genauerer Betrachtung des zugrunde liegenden **Challenge-And-Response**-Verfahrens ist jedoch auffällig, dass der gespeicherte Hash Wert passwortäquivalent ist. Deswegen muss er genauso beschützt werden, wie das Passwort selbst. Des Weiteren ist die Erzeugung des Hash Wertes für jeden Freigabezugriff sehr ressourcenaufwändig. Deshalb wird dieser vom Großteil der Implementierungen einmalig erzeugt und lokal auf dem Rechner

oder Domänencontroller gespeichert. Ein Angreifer kann allerdings durch Kenntnis des Hash Wertes eine gültige Response erzeugen, obwohl ihm das Passwort unbekannt ist. Eine lokale Speicherung des Hash Wertes bedeutet deshalb eine Erhöhung des Sicherheitsrisikos. Durch einen erfolgreichen Systemeinbruch könnten die Hash Werte aller Benutzer, die sich je an dem Rechner angemeldet haben, missbraucht werden.

## 2.4 Mängel in der Implementierung

Nach genauerer Betrachtung der CIFS Spezifikation (vgl. [1]) ist auffällig, dass alle von Microsoft stammenden Implementierungen sich in gewissen Punkten nicht protokollkonform verhalten. Dadurch können jedoch auch Angreifer profitieren, wie nun näher erläutert wird.

### 2.4.1 Freigaben mit "$"-Endung sind unsichtbar

Ausnahmslos alle bisherigen Microsoft-Implementierungen des Protokolls zeigen Freigaben eines Servers, die mit einem "$" Zeichen enden, nicht an. Dieser undokumentierte Mechanismus beschreibt lediglich eine clientseitige Ausprägung der Freigabedarstellung. Es existieren jedoch auch Client Implementierungen von Drittanbietern, die sich protokollkonform verhalten und auch diese Freigaben darstellen. Die Server-Komponenten aller Implementierungen verhalten sich wiederum protokollkonform und übertragen alle Freigaben eines Systems in der Freigabeliste.

Ein Computerbenutzer könnte dazu verleitet werden, Freigaben, die eine "$"-Endung besitzen, mit schwächeren Zugriffsbeschränkungen zu erstellen, da diese augenscheinlich nicht sichtbar sind. Andererseits können solche Freigaben auch leicht in Vergessenheit geraten, da sie in dem Client nicht angezeigt werden. Beide Szenarien stellen ein nicht zu unterschätzendes Sicherheitsrisiko für die freigegebenen Daten dar.

### 2.4.2 Sensible Daten in Paketen

Beim näheren betrachten von SMB Paketen ist auffällig, dass sich oft auch Informationen in ihnen befinden, die für den Freigabedienst unerheblich sind. Neben der Systemzeit und Zeitzone sind das verwendete Betriebssystem und die Betriebssystemversion aufgeführt. Falls Verzeichnisfreigaben existieren, wird in den SMB Paketen sogar das verwendete Dateisystem übermittelt. Bei diesen Informationen handelt es sich jedoch zum Teil um sensible Daten des Computers, die einem Angreifer dienen könnten, um weitere Aktionen durchzuführen.

# 3 Abschließende Betrachtung

Das Mitschneiden des Datenverkehrs, so genanntes **Sniffen**, stellt im CIFS Protokoll ein großes Sicherheitsrisiko dar. Die gesammelten Daten können als Basis für erfolgreiche Computereinbrüche dienen. Durch die Infrastruktur des Internet ist jedoch die Wahrscheinlichkeit, dass jemand den Datenverkehr mitprotokolliert, höher als in einem privaten Netz. Von der Nutzung des Freigabedienstes über das Internet, wie es der Name impliziert, wird daher abgeraten. Der Einsatz von CIFS kann nur eingeschränkt in einem vertrauenswürdigen Netz empfohlen werden, falls für bestehende Sicherheitsmängel Gegenmaßnahmen getroffen worden sind. Da CIFS jedoch einen sehr hohen Verbreitungsgrad besitzt und immer häufiger von unerfahrenen Benutzern eingesetzt wird, ist davon auszugehen, dass oft keine Sicherheitsmaßnahmen ergriffen werden. Somit ist diese Gruppe von unerfahrenen Benutzern ein beliebtes Ziel für Angreifer. Dies wird auch durch einige Security Advisories des **Computer Emergency Response Teams** (= CERT) bestätigt (vgl. [6, 7])

Außerdem sind einige Mechanismen des Protokolls nicht ausreichend dokumentiert, so dass eine umfassende Sicherheitseinschätzung nicht erfolgen kann, solange die Protokollspezifikation nicht vervollständigt wird.

# Literaturverzeichnis


[1] CIFS: IETF: Paul J. Leach, Microsoft, Dilip C. Naik, Microsoft INTERNET-DRAFT: A Common Internet File System (CIFS/1.0) Protocol

[2] SMB: IETF: X/Open Company Ltd., "X/Open CAE Specification - Protocols for X/Open PC Interworking: SMB, Version 2", X/Open Document Number: CAE 209, September 1992.

[3] NetBIOS: IETF: Karl Auerbach, "Protocol Standard For A Netbios Service On A Tcp/Udp Transport: Detailed Specifications", RFC 1002, March 1987

[4] NetBIOS: IETF: Karl Auerbach, "Protocol Standard For A Netbios Service On A Tcp/Udp Transport: Concepts and Methods", RFC 1001, March 1987

[5] IETF: R. Rivest,“The MD4 Message-Digest Algorithm”, RFC 1320, April 1992

[6] CERT® Advisory CA-2003-08 Increased Activity Targeting Windows Shares

[7] CERT® Incident Note IN-2000-02 Exploitation of Unprotected Windows Networking Shares