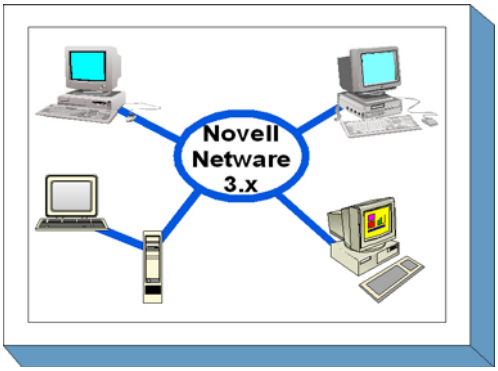
B 3.104 Server unter Novell Netware 3.x



Beschreibung

Betrachtet wird ein LAN mit PCs, die unter dem Netzbetriebssystem Novell Netware 3.x vernetzt sind. Die PCs können mit Festplatte, CD-ROM-Laufwerk, Diskettenlaufwerken und anderen Laufwerken für auswechselbare Datenträger sowie anderen Peripheriegeräten ausgestattet sein. An das Netz sind gegebenenfalls ein oder mehrere Netzdrucker als Warteschleifendrucker angeschlossen. Gegenstand dieses Kapitels ist das Novell 3.x Netz in einer Client-Server-Funktionalität. Damit ist dieser Baustein die betriebssystemspezifische Ergänzung des Bausteins B 3.101 *Allgemeiner Server*.

Die Funktionalitäten des sogenannten Accounting werden nicht betrachtet.

Bemerkung: Namen von Dateien und Programmen werden immer durch Großbuchstaben mit kursiver Schreibweise (z. B. *SYS:PUBLIC\SYSCON.EXE*) dargestellt.

Gefährdungen und die hieraus abgeleiteten Maßnahmen wurden anhand der Versionen Novell 3.11 und 3.12 erarbeitet. Aufgrund verschiedener Patchlevel im Netzbetriebssystem ist es möglich, dass nicht alle Gefährdungen auf jede Variante von Novell Netware 3.x zutreffen.

Gefährdungslage

Für den IT-Grundschutz werden die folgenden typischen Gefährdungen betrachtet:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.33 Nicht gesicherter Aufstellungsort von Novell Netware Servern
- G 2.34 Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung

Vorsätzliche Handlungen:
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.54 Vorsätzliches Herbeiführen eines Abnormal End
- G 5.55 Login Bypass
- G 5.56 Temporär frei zugängliche Accounts
- G 5.57 Netzanalyse-Tools
- G 5.58 "Hacking Novell Netware"
- G 5.59 Missbrauch von Administrationsrechten unter Novell Netware 3.x

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für die Clients sind die in den Bausteinen zu den jeweiligen Betriebssystemen beschriebenen Maßnahmen zu realisieren. Zu beachten ist, dass das hier vorgestellte Maßnahmenbündel, das nur die Besonderheiten des Netzbetriebssystems Novell Netware 3.x berücksichtigt, um die allgemeinen Netzsicherheitsmaßnahmen des Bausteins B 3.101 *Allgemeiner Server* ergänzt werden muss.

Für Server unter Novell Netware 3.x sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption bis zum täglichen Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Die Vorkehrungen, die bei der Planung des Einsatzes von Servern unter Novell Netware 3.x zu treffen sind, werden in der Maßnahme M 2.99 *Sichere Einrichtung von Novell Netware Servern* aufgeführt.

Umsetzung

Die Maßnahme M 2.98 *Sichere Installation von Novell Netware Servern* nennt die wesentlichen Schritte, die bei der Installation des Servers zu beachten sind.

Betrieb

Die Maßnahme M 2.100 *Sicherer Betrieb von Novell Netware Servern* nennt die wesentlichen Schritte, die beim Betrieb des Servers zu beachten sind. Die erreichte Sicherheit kann durch Umsetzung der Maßnahme M 2.101 *Revision von Novell Netware Servern* nachgewiesen werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Server unter Novell Netware 3.x" vorgestellt.

Planung und Konzeption

- M 2.99 (A) Sichere Einrichtung von Novell Netware Servern

Umsetzung

- M 1.42 (A) Gesicherte Aufstellung von Novell Netware Servern
- M 2.98 (A) Sichere Installation von Novell Netware Servern
- M 2.102 (Z) Verzicht auf die Aktivierung der Remote Console

Betrieb

- M 2.100 (A) Sicherer Betrieb von Novell Netware Servern
- M 2.101 (B) Revision von Novell Netware Servern

G 1.2 Ausfall des IT-Systems

Ausfall zentraler Komponenten

Der Ausfall einer Komponente eines IT-Systems kann zu einem Ausfall des gesamten IT-Betriebs führen. Insbesondere zentrale Komponenten eines IT-Systems sind geeignet, solche Ausfälle herbeizuführen, z. B. LAN-Server, Datenfernübertragungseinrichtung. Auch der Ausfall von Komponenten der technischen Infrastruktur, beispielsweise Klima- oder Stromversorgungseinrichtungen, kann zu einem Ausfall des IT-Systems beitragen.

Technisches Versagen/ menschliche Fehlhandlungen

Technisches Versagen (z. B. G 4.1 *Ausfall der Stromversorgung*) muss nicht zwingend als Ursache für den Ausfall eines IT-Systems angenommen werden. Ausfälle lassen sich auch oft auf menschliches Fehlverhalten (z. B. G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*) oder vorsätzliche Handlungen (z. B. G 5.4 *Diebstahl*, G 5.102 *Sabotage*) zurückführen. Auch durch höhere Gewalt (z. B. Feuer, Blitzschlag, Chemieunfall) können Schäden eintreten, allerdings sind diese Schäden meist um ein Vielfaches höher.

Werden auf einem IT-System zeitkritische IT-Anwendungen betrieben, sind die Folgeschäden nach Systemausfall entsprechend hoch, wenn es keine Ausweichmöglichkeiten gibt.

Beispiele:

- Durch Spannungsspitzen in der Stromversorgung wird das Netzteil eines wichtigen IT-Systems zerstört. Da es sich um ein älteres Modell handelt, steht nicht unmittelbar Ersatz bereit. Die Reparatur nimmt einen Tag in Anspruch, in dieser Zeit ist der gesamte IT-Betrieb nicht verfügbar.
- Es wird eine Firmware in ein IT-System eingespielt, die nicht für diesen Systemtyp vorgesehen ist. Das IT-System startet daraufhin nicht mehr fehlerfrei und muss vom Hersteller wieder betriebsbereit gemacht werden.
- Bei einem Internet Service Provider führte ein Stromversorgungsfehler in einem Speichersystem dazu, dass dieses abgeschaltet wurde. Obwohl der eigentliche Fehler schnell behoben werden konnte, ließen sich die betroffenen IT-Systeme anschließend nicht wieder hochfahren, da Inkonsistenzen im Dateisystem auftraten. Bis alle Folgeprobleme behoben waren, waren mehrere der vom ISP betriebenen Webserver tagelang nicht erreichbar.

Ausfall einer Archivkomponente

- In elektronischen Archiven kann der Zeitpunkt der erstmaligen Archivierung als Entstehungszeitpunkt von Dokumenten missinterpretiert werden, wenn keine anderweitigen Beweisverfahren, z. B. Zeitstempeldienste, zur Beglaubigung eingesetzt werden. Dies gilt vor allem für Geschäftsprozesse, in die die elektronische Archivierung von massenhaft anfallenden Belegdaten transparent eingebunden ist. Im vorliegenden Fall konnte aufgrund des Ausfalls einer Archivkomponente ein Teil von Belegdaten erst um einen Tag verzögert archiviert werden. Durch die Verwendung von WORM-Medien wurde die Reihenfolge der physikalischen Archivierung der Geschäftsbelege trotzdem nachweisbar dokumentiert, es wurde jedoch kein Nachweis für die ansonsten nicht auftretende Verzögerung durch die ausgefallene Archivkomponente geführt. Dadurch entstand bei einer späteren Prüfung der Eindruck einer nachträglichen Manipulation.

G 2.33 Nicht gesicherter Aufstellungsort von Novell Netware Servern

Die Aufstellung von Novell Netware Servern in einer nicht gesicherten Umgebung (z. B. Flure, nicht verschlossene Serverräume) stellt eine erhebliche Gefährdung für die IT-Sicherheit dar.

Direkte Eingaben an der Server-Konsole bzw. das Laden von NLMs (Netware Loadable Modules) am Server können dazu führen, dass die installierten Sicherheitsmechanismen außer Kraft gesetzt werden, ohne dass dieser Umstand dem Administrationspersonal bzw. dem IT-Sicherheitsmanagement bekannt wird.

Beispiel:

Durch das Laden spezieller NLMs ist es möglich, einen Supervisor-äquivalenten Benutzer zu generieren bzw. einen existierenden Benutzer mit Supervisor-äquivalenten Rechten zu versehen.

G 2.34 Fehlende oder unzureichende Aktivierung von Novell Netware Sicherheitsmechanismen

Das Netzbetriebssystem Novell Netware verfügt über eine Sammlung an Sicherheitsmechanismen, die den unerlaubten Zugriff auf Dateien des Servers abwehren.

Diese Sicherheitsmechanismen werden jedoch nicht automatisch aktiviert, sondern müssen durch die Systemadministration nach dem erstmaligen Start des Servers eingerichtet werden.

Werden die Sicherheitsmechanismen eines Novell Netware Servers nicht oder nur unzureichend installiert, so kann der unerlaubte Zugriff auf schützenswerte Dateien entscheidend erleichtert werden.

G 4.1 Ausfall der Stromversorgung

Trotz hoher Versorgungssicherheit kommt es immer wieder zu Unterbrechungen der Stromversorgung seitens der Verteilungsnetzbetreiber (VNB) bzw. Energieversorgungsunternehmen (EVU). Die größte Zahl dieser Störungen ist mit Zeiten unter einer Sekunde so kurz, dass der Mensch sie nicht bemerkt. Aber schon Unterbrechungen von mehr als 10 ms sind geeignet, den IT-Betrieb zu stören. Bei einer Messung mit ca. 60 Messstellen wurden 1983 in Deutschland rund 100 solcher Netzeinbrüche registriert. Davon dauerten fünf Ausfälle bis zu einer Stunde und einer länger als eine Stunde. Diese Unterbrechungen beruhten einzig auf Störungen im Versorgungsnetz. Dazu kommen Unterbrechungen durch Abschaltungen bei nicht angekündigten Arbeiten oder durch Kabelbeschädigungen bei Tiefbauarbeiten.

Von der Stromversorgung sind nicht nur die offensichtlichen, direkten Stromverbraucher (PC, Beleuchtung usw.) abhängig. Alle Infrastruktureinrichtungen sind heute direkt oder indirekt vom Strom abhängig, z. B. Aufzüge, Rohrpostanlagen, Klimatechnik, Gefahrenmeldeanlagen, Sprinkleranlagen, Telefonnebenstellenanlagen. Selbst die Wasserversorgung in Hochhäusern ist wegen der zur Druckerzeugung in den oberen Etagen erforderlichen Pumpen stromabhängig.

Die Liberalisierung des Strommarktes führte in einigen Industrieländern zu einer Verschlechterung des Versorgungsniveaus. Auch in Deutschland könnte daher die Gefahr wachsen, dass Probleme durch Ausfälle der Stromversorgung oder durch Schaltvorgänge an nationalen Versorgungsübergängen entstehen.

Beispiele:

- In einem großen süddeutschen Industriebetrieb war die gesamte Stromversorgung für mehrere Stunden unterbrochen, da technische Probleme beim Stromversorgungsunternehmen aufgetreten waren. Infolgedessen fielen sowohl die Produktion als auch sämtliche Rechner der Entwicklungsabteilungen aus, die über keine Ersatz-Stromversorgung verfügten.
- Durch einen Fehler in der USV eines Rechenzentrums schaltete diese nach einem kurzen Stromausfall nicht auf Normalbetrieb zurück. Nach Entladung der Batterien nach etwa 40 Minuten fielen alle Rechner im betroffenen Server-Saal aus.
- Anfang 2001 gab es über 40 Tage einen Strom-Notstand in Kalifornien. Die Stromversorgungslage war dort so angespannt, dass die Kalifornische Netzüberwachungsbehörde rotierende Stromabschaltungen anordnete. Von diesen Stromabschaltungen, die bis zu 90 Minuten andauerten, waren nicht nur Haushalte, sondern auch die High-Tech-Industrie betroffen. Weil mit dem Stromausfall auch Alarmanlagen und Überwachungskameras ausgeschaltet wurden, hielten die Energieversorger ihre Abschaltpläne geheim.

G 5.23 Computer-Viren

Computer-Viren gehören zu den Programmen mit Schadensfunktionen. Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Daten oder Programmen sicherlich von größter Tragweite. Solche Funktionen von Programmen können sowohl unbeabsichtigt als auch bewusst gesteuert auftreten.

Die Definition eines Computer-Virus bezieht sich nicht unmittelbar auf eine möglicherweise programmierte Schadensfunktion:

Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)

Die Eigenschaft der Reproduktion führte in Analogie zum biologischen Vorbild zu der Bezeichnung "Virus". Die Möglichkeiten der Manipulation sind sehr vielfältig. Besonders häufig sind das Überschreiben oder das Anlagern des Virus-Codes an andere Programme und Bereiche des Betriebssystems.

Computer-Viren können im Prinzip bei allen Betriebssystemen auftreten. Die größte Bedrohung ist jedoch im Bereich der IBM-kompatiblen Personalcomputer (PC) vorhanden. Bei den hier am meisten verbreiteten Betriebssystemen (MS-DOS, PC-DOS, DR DOS, NOVELL DOS etc.) werden derzeit weltweit rund 20.000 Viren (einschließlich Varianten) gezählt.

Spezielle Computer-Viren für die Betriebssysteme Windows 3.x, Windows NT, Windows 95, OS/2 und Unix spielen in der Praxis eine untergeordnete Rolle. Bei PC-typischer Hardware können jedoch die Festplatten dieser Rechner von DOS-Boot-Viren infiziert werden, wenn die Boot-Reihenfolge zuerst ein Booten von Diskette vorsieht.

Für Apple-Computer sind ca. 100 spezielle Computer-Viren bekannt, für die es auch entsprechende Suchprogramme gibt.

Arten von Computer-Viren

Es werden drei Grundtypen von Computer-Viren unterschieden:

- Boot-Viren
- Datei-Viren
- Makro-Viren

Es sind auch Misch- und Sonderformen dieser drei Typen bekannt. Weitere Unterteilungsmerkmale sind die Tarnmechanismen, mit denen die Viren oft gegen die Erkennung durch Benutzer und Suchprogramme geschützt sind.

Boot-Viren

Als "Booten" bezeichnet man das Laden des Betriebssystems. Hierbei werden u. a. Programmteile ausgeführt, die zwar eigenständig sind, sich aber in sonst

nicht zugänglichen und im Inhaltsverzeichnis der Disketten und Festplatten nicht sichtbaren Sektoren befinden. Boot-Viren überschreiben diese mit ihrem Programm. Der originale Inhalt wird an eine andere Stelle auf dem Datenträger verlagert und dann beim Start des Computers anschließend an den Virus-Code ausgeführt. Dadurch startet der Computer scheinbar wie gewohnt. Der Boot-Virus gelangt jedoch bereits vor dem Laden des Betriebssystems in den Arbeitsspeicher des Computers und verbleibt dort während der gesamten Betriebszeit. Er kann deshalb den Boot-Sektor jeder nicht schreibgeschützten Diskette infizieren, die während des Rechnerbetriebs benutzt wird. Boot-Viren können sich nur durch Booten oder einen Boot-Versuch mit einer infizierten Diskette auf andere Computer übertragen.

Datei-Viren

Die meisten Datei-Viren (auch File-Viren genannt) lagern sich an Programmdateien an. Dies geschieht jedoch so, dass beim Aufruf auch hier der Virus-Code zuerst ausgeführt wird und erst anschließend das originale Programm. Dadurch läuft das Programm anschließend scheinbar wie gewohnt und der Virus wird nicht so schnell entdeckt. Es sind jedoch auch primitivere, überschreibende Viren bekannt, die sich so an den Anfang des Wirtsprogramms setzen, so dass dieses nicht mehr fehlerfrei läuft. Datei-Viren verbreiten sich durch Aufruf eines infizierten Programms.

Bei den Mischformen von Boot- und Datei-Viren haben so genannte multipartite Viren eine größere Bedeutung erlangt. Sie können sich sowohl durch Aufruf eines infizierten Programms als auch durch Booten (oder einen Boot-Versuch) von einer infizierten Diskette verbreiten.

Makro-Viren

Auch Makro-Viren sind in Dateien enthalten, diese infizieren jedoch nicht die Anwendungsprogramme, sondern die damit erzeugten Dateien. Betroffen sind alle Anwendungsprogramme, bei denen in die erzeugten Dateien nicht nur einzelne Steuerzeichen, sondern auch Programme und andere Objekte eingebettet werden können. Davon sind insbesondere Microsoft Word- und Excel-Dateien betroffen. Bei diesen steht eine leistungsfähige Programmiersprache für Makros zur Verfügung, die auch von weniger geschulten Benutzern leicht zur Programmierung von Viren missbraucht werden kann (siehe auch G 5.43 *Makro-Viren*).

Makros sind Programme, mit deren Hilfe das Anwenderprogramm um zusätzliche Funktionen erweitert werden kann, die auf den Anwendungsfall zugeschnitten sind (z. B. Erzeugen einer Reinschrift aus dem Entwurf eines Textes). Diese Makros laufen erst mit dem jeweiligen Anwendungsprogramm (Microsoft Word, Excel etc.) bei der Bearbeitung des Dokuments ab, indem der Benutzer das Makro aktiviert oder das Makro automatisch gestartet wird. Wird z. B. eine Word-Datei über einen WWW-Browser empfangen, der das Dokument automatisch mit Microsoft Word öffnet, kann hierdurch ein enthaltenes Makro aktiviert werden. Da Datendateien auch häufiger als herkömmliche Programmdateien über Datenträger und vernetzte IT-Systeme verteilt werden, ist die Gefährdung durch Makro-Viren inzwischen größer als durch Boot- und Datei-Viren.

Beispiele für Schadensfunktionen von Computer-Viren

- Der Boot-Virus Michelangelo überschreibt an jedem 6. März die ersten Spuren der Festplatte mit stochastischem Inhalt und macht sie dadurch unbrauchbar.
- Der multipartite Virus Onehalf verschlüsselt maximal die Hälfte des Inhalts der Festplatte. Wird der Virus entfernt, sind die verschlüsselten Daten nicht mehr verfügbar.
- Der Microsoft Word-Makro-Virus WAZZU fügt bei den befallenen Dokumenten an zufälligen Stellen das Wort "Wazzu" ein.
- Der Microsoft Word-Makro-Virus Melissa erschien am 26.3.1999 und verbreitete sich über das Wochenende weltweit. Er ist in einer Datei von Word 97 oder Word 2000 enthalten, die von einem befallenen Computer mittels Microsoft Outlook an bis zu 50 gespeicherte Einträge aus jedem Adressbuch verschickt wird. Dies hat bei einigen größeren Organisationen das Mail-System überlastet.
- W32.Mypics.Worm ist ein in Visual Basic geschriebener Computerwurm, der sich automatisch auf Windows 95/98 und Windows NT Rechnern verbreitet. Er enthält eine zerstörerische Schadenswirkung, die aktiv wird, sobald die Jahreszahl 2000 ist. Dann wird u. a. das BIOS des Rechners verändert, so dass der Rechner nicht mehr korrekt bootet.

G 5.43 Makro-Viren

Mit dem Austausch von Dateien (z. B. per Datenträger oder E-Mail) besteht die Gefahr, dass neben der eigentlichen Datei (Textdatei, Tabelle etc.) weitere, mit dem Dokument verbundene Makros bzw. eingebettete Editorkommandos übersandt werden. Diese Makros laufen erst mit dem jeweiligen Anwendungsprogramm (Winword, Excel etc.) bei der Bearbeitung des Dokuments ab, indem der Benutzer das Makro aktiviert bzw. das Makro automatisch gestartet wird. Wird ein Dokument über einen WWW-Browser empfangen, der das Dokument automatisch öffnet, kann hierdurch ein (Auto-) Makro aktiviert werden.

Da die Makrosprachen über einen sehr umfangreichen Befehlssatz verfügen, besteht auch die Gefahr, dass einem Dokument ein Makro beigefügt wird, das eine Schadfunktion enthält (z. B. einen Virus).

In der Praxis hat diese Gefährdung insbesondere bei den Dateien der Programme Word für Windows und Excel der Firma Microsoft weltweit beträchtlich zugenommen. Für den Benutzer ist dabei nicht transparent, dass Dateien für Word-Vorlagen (*.DOT), in denen Makros enthalten sein können, durch Umbenennen in *.DOC-Dateien scheinbar zu Datendateien werden, die keine Makros enthalten. Von Microsoft Word werden solche Dateien jedoch ohne Hinweis auf diese Tatsache in nahezu gleicher Weise verarbeitet (Ausnahme: Winword ab Version 7.0a).

Die Word-Makro-Viren haben inzwischen die Spitzenstellung bei gemeldeten Infektionen eingenommen. Hervorzuheben ist, dass Makro-Viren auf verschiedenen Betriebssystem-Plattformen auftreten können, nämlich auf allen, auf denen Winword läuft (Windows Versionen 3.1 und 3.11, Windows 95, Windows NT, Apple-Computer).

Beispiel:

- Der Winword-Makro-Virus "Winword.Nuclear" wurde im Internet über die Datei WW6ALERT.ZIP verbreitet. Der Makro-Virus bewirkt einerseits, dass an Ausdrucken der Text "STOP ALL FRENCH NUCLEAR TESTIN IN PACIFIC!" angehängt wird, andererseits aber auch den Versuch, Systemdateien zu löschen.

G 5.54 Vorsätzliches Herbeiführen eines Abnormal End

Ein Netware ABEND (Abnormal End) wird hervorgerufen, wenn das Netware Betriebssystem aufgrund von Hard- und/oder Softwareproblemen nicht mehr in der Lage ist, Netzprozesse ordnungsgemäß weiterzuführen bzw. zu steuern. Der Fileserver wird in diesen Fällen gestoppt und muss neu gestartet werden.

Hat ein Angreifer Zugriff auf die Konsole des Novell Netware Servers, so kann ein Netware ABEND durch die Eingabe bestimmter Parameter vorsätzlich herbeigeführt werden.

Der ABEND eines Novell Netware Servers kann sogar von jedem, der Zugriff auf das Netz hat, herbeigeführt werden, ohne das ein autorisiertes Login auf dem Novell Netware Server erfolgen muss. Durch den Aufruf des Programms *SYS:\PUBLIC\RENDIR.EXE* mit zusätzlichen Parametern kann jede Workstation im Status "Attached" den ABEND eines Novell Netware Servers provozieren.

G 5.55 Login Bypass

Die Login-Scripts (System-Login-Script, User-Login-Script) eines Novell Netware Servers erstellen, nach erfolgter Anmeldung am Novell Netware Server, die persönliche Netzumgebung für den Benutzer.

Durch die Verwendung von Optionen beim Ausführen von *LOGIN.EXE* unter Novell Netware werden weder das System-Login-Script noch das User-Login-Script des ausgewählten Novell Netware Servers ausgeführt. Sicherheitseinstellungen die in die Login-Scripts implemetiert wurden werden somit umgangen. Hierdurch ist es dem Benutzer nach dem autorisierten Login möglich, sich mit Hilfe des Map Kommandos unabhängig von den in den Login-Scripts (System-Login-Script, User-Login-Script) festgelegten Parametern auf dem Novell Netware Server zu "bewegen". In Verbindung mit einer unzureichenden Rechtevergabe kann dies dazu führen, dass Informationen, die nicht für den Benutzer zugänglich sein sollen, diesem zugänglich werden.

G 5.56 Temporär frei zugängliche Accounts

Bei der Einrichtung eines neuen User-Accounts wird dieser standardmäßig ohne Passwort eingerichtet. Von Seiten des Netzbetriebssystems besteht hierbei keinerlei Zwang, ein Passwort zu vergeben, obwohl dieses in den Standardeinstellungen ("Default Account Balance/Restrictions") eingestellt werden kann. Diese neu eingerichteten Accounts sind somit für jederman frei zugänglich, ohne dass eine Passwortabfrage erfolgt. Die Gefährdung des sogenannten "race on new accounts" ist hierbei umso höher einzuschätzen, je privilegierter der neue Account auf dem Novell Netware Server ist.

In diesem Zusammenhang wird darauf hingewiesen, dass verschiedene Versionen (z. B. Vers. 3.75, Vers. 3.76) des Netware Utilities *SYS:\PUBLIC\SYSCON.EXE* bei der Vergabe eines neuen Passwortes durch einen Systemverwalter dieses Passwort unverschlüsselt über das Netz übertragen.

G 5.57 Netzanalyse-Tools

Werden die im Netzsegment übertragenen Informationen nicht verschlüsselt, so können diese Informationen mit Hilfe von Netzanalyse-Tools, den sogenannten "Sniffern", im Klartext ausgelesen werden. Hierbei ist auch zu beachten, dass diese "Sniffer" keineswegs immer als "Hackingsoftware" betrachtet werden können, da viele Produkte, die dem Management des Netzes dienen, eine derartige Funktion beinhalten.

Trace-Funktionen des z/OS-Betriebssystems

Trace-Funktionen unter z/OS

Unter z/OS stehen dem Bediener sogenannte Trace-Funktionen zur Verfügung. Mit Hilfe der *Generalized Trace Facility (GTF)* lassen sich in SNA- oder TCP/IP-Netzen unter anderem Terminal-Sessions überwachen. Wird die Trace-Funktion auf die Session des RACF-Administrators angewandt, kann unter Umständen dessen Passwort ermittelt werden, wenn die Inhalte der Session nicht verschlüsselt sind. Eine ähnliche Trace-Funktion ist in der *Network Logical Data Manager*-Komponente (*NLDM)* des Produktes *NetView* enthalten.

G 5.58 "Hacking Novell Netware"

"Hacking Novell Netware" kann prinzipiell auf zwei Arten durchgeführt werden.

Zum einen kann, ausgehend von einer Workstation, eine gezielte Attacke gegen einen User Account erfolgen, um dessen Passwort in Erfahrung zu bringen.

Die gezielte Attacke gegen einen User Account kann hierbei über einen sogenannten Brute Force Angriff erfolgen, bei dem eine Workstation (Status: Attached) Login-Versuche unter einem zuvor festgelegten User Account durchführt und hierbei mit Hilfe eines Algorithmus oder eines mitgelieferten Wörterbuches Passwörter generiert bzw. ausprobiert.

Mit Hilfe des Programms *HACK.EXE* kann ein autorisierter Benutzer einen Angriff gegen den Account des Supervisors durchführen. Es kann, eine Schwachstelle im Betriebssystem ausnutzend, alle Benutzer des Novell Netware Servers in einen Supervisor-äquivalenten Zustand versetzten, den Supervisor ausloggen sowie dessen Passwort verändern, vorausgesetzt der Account des Supervisors ist zum Zeitpunkt der Aktivierung von *HACK.EXE* auf dem Novell Netware Server eingeloggt.

Weiterhin kann eine Attacke durch eine direkte Manipulation am Server durchgeführt werden, um beispielsweise einen Supervisor-äquivalenten Account zu generieren.

Durch das Einspielen und Aktivieren von NLMs (Netware Loadable Modules), die als Notfalltools entwickelt worden sind, besteht beispielsweise die Möglichkeit, einen speziellen Benutzer zu erzeugen, dessen Rechte auf dem Novell Netware Server äquivalent zu denen des Supervisors sind.

Diese Tools, wie z. B. *SETPWD.NLM*, arbeiten auch in Netware 4 Netzen. Deshalb sei an dieser Stelle noch einmal auf M 1.42 *Gesicherte Aufstellung von Novell Netware Servern* hingewiesen.

Die meisten dieser Programme sind frei über das Internet erhältlich. Sie sind, hinsichtlich ihrer Handhabung, auch von "Computer-Laien" zu bedienen, da sie keine spezifischen Novell Netware Kenntnisse erfordern.

G 5.59 Missbrauch von Administratorrechten unter Novell Netware 3.x

Der Supervisor Account bzw. ein Supervisor-äquivalenter Account besitzt, mit Ausnahme der Bindery Informationen (z. B. Passwörter), die vollständige Kontrolle über einen Novell Netware Server.

Hierdurch ist es einem Account der Sicherheitsstufe "Supervisor" möglich, auf alle gespeicherten Informationen des Servers zuzugreifen, wenn diese nicht durch zusätzliche Sicherheitsmechanismen, wie z. B. Verschlüsselung geschützt werden. Damit haben autorisierte Benutzer dieser Accounts die Möglichkeit, Daten anderer Benutzer zu lesen, zu löschen bzw. zu verändern.

M 1.42 Gesicherte Aufstellung von Novell Netware Servern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um den manipulationssicheren Betrieb von Novell Netware Servern sicherzustellen, ist es zwingend erforderlich, die Novell Netware Server in einer gesicherten Umgebung aufzustellen. Dies kann entweder ein Serverraum sein (siehe Baustein B 2.4 *Serverraum*) oder ein Serverschrank, wenn kein separater Serverraum zur Verfügung steht (siehe Baustein B 2.4 *Serverraum*). Unbefugte dürfen zum Aufstellungsort von Novell Netware Servern keinen unbeaufsichtigten Zugang erhalten. Das Diskettenlaufwerk von Novell Netware Servern ist darüber hinaus standardmäßig mit einem Diskettenschloss zu verschließen.

M 2.98 Sichere Installation von Novell Netware Servern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Im Vorfeld der Installation sowie bei der Einrichtung eines Novell Netware Servers sollten die folgenden Aspekte beachtet werden, um eine möglichst reibungslose und sichere Installation gewährleisten zu können.

Dokumentation der Installation

Die Installation von Novell Netware Servern sollte nachvollziehbar dokumentiert werden, damit im Vertretungsfall sowohl Außenstehende wie auch Neueinsteiger diese nach kurzer Einarbeitungszeit verstehen und nachvollziehen können.

In der Dokumentation sollte insbesondere die Parametrisierung des Servers (Netzeinbindung, Treiber), zusätzliche NLMs (Netware Loadable Modules, z. B. zur Datensicherung) und deren Konfiguration, sowie die eingespielten Patches aufgeführt werden. Weiterhin sollte die Installation und Einbindung zusätzlicher Hardware (z. B. Netzdrucker, Bandlaufwerke) ausführlich dokumentiert werden.

Desweiteren sollte die Dokumentation eine detaillierte Beschreibung der Server-Hardware und der installierten Peripheriegeräte (z. B. Netzdrucker) beinhalten. In Abhängigkeit der Komplexität des Novell-Netzes ist der Einsatz von Administrationstools für Dokumentations- und Revisionszwecke erstrebenswert.

Die zur Installation und Konfiguration eines Novell Netware Servers erforderliche Software sollte vollständig an einem gesicherten Ort hinterlegt werden, um im Bedarfsfall unnötige Verzögerungen zu vermeiden. Dies sollte insbesondere bei den aufzuspielenden Patches des Netzbetriebssystems, zusätzlichen NLMs sowie den einzusetzenden Treibern beachtet werden.

Das Laden des NLM-Utilities *SYS:SYSTEM\CONLOG.NLM* bewirkt, dass alle Meldungen, die am Monitor des Servers erscheinen, gleichzeitig in die Datei *SYS:ETC\CONSOLE.LOG* umgeleitet werden. Dieses NLM sollte bereits in der Startdatei *AUTOEXEC.NCF* geladen werden, um Fehler, die in der Startphase des Servers gemeldet werden, nachvollziehen zu können.

Hardwareausstattung

Bei der Festlegung der erforderlichen Hauptspeicherkapazität (RAM) von Novell Netware Servern ist neben der Festplattenkapazität, den eingesetzten Betriebssystemen der Novell Netware Clients auch die RAM-Speicherbelegung durch zusätzlich geladene NLMs zu berücksichtigen.

Hinsichtlich der Festplattenkapazität beim Einrichten einzelner Volumes auf einem Novell Netware Server ist insbesondere das SYS: Volume ausreichend zu dimensionieren, da alle Netware Prozesse standardmäßig auf diesem Volume ausgeführt werden. Eine zu kleine Dimensionierung des SYS: Volumes kann unter Umständen dazu führen, dass nach einer gewissen Betriebszeit temporäre Prozesse, wie z. B. Druckjobs, die Kapazitäten des Volumes

erschöpfen und somit einen vermeidbaren ABEND (Abnormal End - Absturz des Servers) hervorrufen.

Anforderungen an die Verfügbarkeit

Zur Erhöhung der Verfügbarkeit von Novell Netware Servern bzw. der gespeicherten Daten stellt das Netzbetriebssystem Novell Netware 3.x drei hierarchische Fehlertolerierungsstufen (System Fault Tolerance Level) zur Verfügung, die nachfolgend kurz aufgezeigt werden. Jede der hier aufgezeigten Fehlertolerierungsstufen beinhaltet dabei die Funktionalitäten der vorherigen Stufe.

- **SFT I (System Fault Tolerance I)**

  Novell Netware 3.x unterstützt standardmäßig SFT I. Hierbei werden Datenverluste aufgrund physikalischer Festplattenfehler verhindert. Nach einem Schreibzugriff auf eine Datei erfolgt ein Vergleich zwischen den veränderten Daten auf der Festplatte mit den Originaldaten, die sich noch im Arbeitsspeicher des Novell Netware Servers befinden. Ist dieses Ergebnis fehlerhaft, so wird der entsprechende Sektor der Festplatte als defekt markiert und für zukünftige Zugriffe gesperrt.

  Weiterhin werden die Daten des Arbeitsspeichers im Anschluss in dem zuvor beschriebenen Fehlerfall in den so genannten "Hot Fix Bereich" der Festplatte umgeleitet, für den Novell Netware standardmäßig zwei Prozent der Festplattenkapazität beansprucht.

- **SFT II (System Fault Tolerance II)**

  Die Fehlertolerierung der Stufe II (SFT II) kann auf zwei unterschiedliche Arten realisiert werden.

  - Disk Mirroring

    Beim Disk Mirroring werden an einen Festplattencontroller des Servers zwei identische Festplatten angeschlossen. Die zu speichernden Daten werden gleichzeitig auf beiden Festplatten gespeichert. Fällt eine der Festplatten durch einen Fehler aus, wird ohne Ausfallzeit und Datenverlust mit der zweiten Festplatte weitergearbeitet.

  - Disk Duplexing

    Beim Disk Duplexing werden zwei Festplatten und zwei Festplattencontroller von gleicher Art bzw. Größe im File Server installiert. Disk Duplexing gewährleistet somit eine Fortführung des Betriebes nicht nur beim Ausfall einer Festplatte, sondern auch beim Ausfall eines Festplattencontrollers.

- **SFT III (System Fault Tolerance III)**

  SFT III stellt die höchste Stufe der Toleranz gegen im Betrieb auftretende Hardware-Fehler dar. Zwei identische Novell Netware Server arbeiten hierbei gleichzeitig und parallel im Netz.

  Die beiden Novell Netware Server sind hierbei durch ein eigenes Hochgeschwindigkeitsnetz miteinander verbunden. Fällt einer der beiden Server

aus, so wird der Netzbetrieb, fast ohne Zeit- und Datenverlust, durch den zweiten Novell Netware Server weitergeführt.

Die Entscheidung, ob zusätzlich zur Stufe SFT I weitere Maßnahmen (SFT II, SFT III) ergriffen werden müssen, ist abhängig vom angestrebten Grad der Verfügbarkeit des Netzes.

Notstromversorgung

Durch den Einsatz einer Notstromversorgung (UPS=Unterbrechungsfreie Stromversorgung) können die Folgen eines plötzlichen Stromausfalles abgefangen werden. Novell Netware unterstützt den Einsatz geeigneter Geräte durch das so genannte UPS-Monitoring. Im Falle eines plötzlichen Stromausfalles wird der File Server am Ende der Überbrückungszeit der UPS geregelt heruntergefahren, d. h. die sich im Cache des Servers befindlichen Daten werden auf die Festplatten übertragen, Verbindungen zum Server ordnungsgemäß terminiert sowie die Serverprozesse geregelt beendet.

Ergänzende Kontrollfragen:

- Genügt die Dokumentation auch dem Vertretungsfall des Administrators?
- Wie wurde die Auswahl des SFT-Levels begründet?

M 2.99 Sichere Einrichtung von Novell Netware Servern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die im Lieferumfang von Novell Netware 3.x enthaltenen Sicherheitsfeatures sind nach dem erstmaligen Start der Datei *SERVER.EXE* nicht automatisch aktiviert, sondern müssen, jeweils einzeln durch die Systemadministration installiert und konfiguriert werden.

Mit Hilfe des Programms *SYS:PUBLIC\SETPASS.EXE* sollte der Supervisor nach dem erstmaligen Login sofort ein Passwort für diesen Account vergeben. Der standardmäßig vorhandene Guest-Account sollte ebenfalls mit einem Passwort versehen werden. Wird der Guest-Account im späteren Betrieb nicht benötigt, so sollte er entfernt werden.

Mittels DISABLE LOGIN (Serverkonsole) sollten während der Einrichtungsphase unautorisierte Login-Versuche unterbunden werden.

Mit Hilfe des Novell Utilities *SYS:PUBLIC\SYSCON.EXE* können im Anschluss, unter dem Menüpunkt **Supervisor Options** die meisten der Novell Sicherheitsmechanismen installiert und konfiguriert werden. Hierbei ist zu beachten, dass die unter **Default Time Restrictions** vorgenommenen Einstellungen nur dann für alle Accounts des Novell Netware Servers Gültigkeit haben, wenn diese Einstellungen vor der Einrichtung von Benutzern und Gruppen getroffen werden.

Nachfolgend werden sicherheitsrelevante Menüpunkte aufgeführt.

Default Account Balance/Restrictions

Mit Hilfe dieses Menüpunktes werden folgende Sicherheitseinstellungen auf dem Novell Netware Server aktiviert.

- **Account has Expiration Date**: Hiermit kann die Gültigkeitsdauer eines Accounts zeitlich limitiert werden. Da ein Account normalerweise auf Dauer angelegt ist, wird dieses Feature im Regelfall nur für einen Guest Account aktiviert.
- **Limit Concurrent Connections**: Hierdurch kann die Anzahl der gleichzeitigen Verbindungen eines Accounts zu dem Novell Netware Server limitiert werden. Im Regelfall sollte hierbei der Wert "Eins" gewählt werden.
- **Create Home Directory for User:** Optionale Erstellung eines persönlichen Verzeichnisses für jeden Benutzer. Es sollte die Option "Yes" gewählt werden.
- **Require Password:** Require Password installiert die Passwortabfrage für jeden Benutzer und bietet bei Aktivierung die Möglichkeit, Passwortregeln zu installieren. Für Require Password sollte die Option "Yes" gewählt werden.
- **Minimum Password Lenght:** Hierbei wird die erforderliche Mindestlänge eines Passwortes eingestellt. Die Mindestlänge eines Passwortes sollte

hierbei sechs Zeichen sein (siehe unter M 2.11 *Regelung des Passwortgebrauchs*). Wird die erforderliche Mindestlänge auf weniger als fünf Zeichen eingestellt, so wird dieses beim Ausführen von *SYS:\SYSTEM\SECURITY.EXE* angezeigt (siehe M 2.101 *Revision von Novell Netware Servern*).

- **Force Periodic Password Changes:** Durch die Einstellung "Yes" wird festgelegt, dass die Benutzer ihre Passwörter regelmäßig ändern müssen. Dies sollte der Regelfall sein.
- **Days Between Password Changes:** Unter diesem Menüpunkt wird die generelle Gültigkeitsdauer von Passwörtern festgelegt. Die Gültigkeitsdauer von Passwörtern muss für das jeweilige System festgelegt werden.

  Hinweis: Ist die Gültigkeitsdauer des Passwortes auf einen Wert eingestellt, der mehr als 60 Tage beträgt, so wird dieses durch das Novell Utility *SYS:SYSTEM\SECURITY.EXE* "beanstandet".
- **Limit Grace Logins:** Grace Logins ("Gnaden-Logins") sind die Logins, die nach Ablauf der Gültigkeitsdauer eines Passwortes erfolgen. Die Anzahl der Grace Logins sollte durch die Einstellung "Yes" grundsätzlich limitiert werden.
- **Grace Logins Allowed:** Die Anzahl der erlaubten Grace Logins sollte auf den Wert "Eins" eingestellt werden, damit ein Benutzer, dessen Passwort ungültig geworden ist, dieses sofort ändern muss.
- **Require Unique Passwords:** Die Aktivierung der Passworthistorie (REQUIRE UNIQUE PASSWORDS) hat zur Folge, dass die letzten neun Passwörter eines Accounts mit dem neu eingegebenen Passwort verglichen werden und bei Übereinstimmung das neue Passwort durch den Novell Netware Server zurückgewiesen wird.
- **Account Balance:** Novell Netware Accounting Funktion
- **Allow Unlimited Credit:** Novell Netware Accounting Funktion
- **Low Balance Limit:** Novell Netware Accounting Funktion

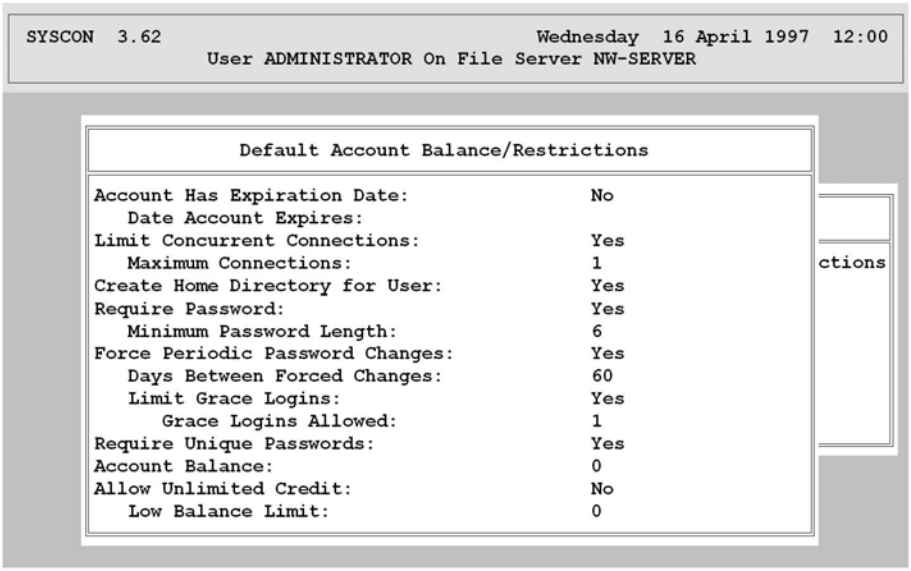


Abbildung 1: Menu *SYS:PUBLIC\SYSCON.EXE* "Default Account Balance/Restrictions"

Default Time Restrictions

Mit Hilfe der Time Restrictions werden die erlaubten Arbeitszeiten für Accounts auf einem Novell Netware Server definiert. Außerhalb der hier festgelegten Zeiten, die im Regelfall den üblichen Arbeitszeiten entsprechen sollten, ist es keinem Benutzer gestattet, sich am Novell Netware Server anzumelden.

Hinweis: Für die standardmäßig installierten Accounts Supervisor und Guest ist der Netware-Default-Wert (keine Zeitbeschränkungen) eingestellt. Es ist empfehlenswert, zumindest den Guest-Account mit Hilfe von *SYS:PUBLIC\SYSCON.EXE* (User Information - Time Restrictions) hinsichtlich der erlaubten Zugriffszeiten einzuschränken.

Nachträgliche Änderungen der "Default Time Restrictions" bei der Einrichtung bzw. Pflege von Benutzer Accounts haben keine Auswirkungen auf die erlaubten Zugangszeiten bereits eingerichteter Benutzer. Abweichende Zugangszeiten einzelner Benutzer müssen mit Hilfe von *SYS:\PUBLIC\SYSCON.EXE* (User Information - Time Restrictions) eingerichtet werden.

Edit System AUTOEXEC File

Durch die Server Startdatei *AUTOEXEC.NCF* werden die Parameter (z. B. Volumes, NLMs, zusätzliche Protokolle etc.) eines Novell Netware Servers konfiguriert.

Weiterhin können in der *AUTOEXEC.NCF* zusätzliche Sicherheitseinstellungen vorgenommen werden.

Das Novell Netware Konsolenkommando SECURE CONSOLE, das in die *AUTOEXEC.NCF* eingebunden sein sollte, bewirkt dabei, dass NLMs nur noch aus dem Serververzeichnis *SYS:SYSTEM* gestartet werden können, sowie die Deaktivierung des Novell Netware Debuggers. Weiterhin wird

durch SECURE CONSOLE das DOS aus dem Hauptspeicher des Novell Netware Servers entfernt, sowie die definierten Serversuchpfade außer Kraft gesetzt, die zudem nicht erneut definiert werden können.

File Server Console Operators

Mit Hilfe des Menu-Utilities *SYS:\PUBLIC\FCONSOLE.EXE* kann, ausgehend von einer Workstation, die begrenzte Kontrolle über einen Novell Netware Server übernommen werden.

Der File Server Operator, der neben der ausdrücklichen Berechtigung zur Nutzung von *SYS:\PUBLIC\FCONSOLE.EXE* keine weiteren Privilegien benötigt, kann hiermit Konsolennachrichten an die Benutzer versenden, den Novell Netware Server wechseln sowie den Server herunterfahren. Weiterhin können Statusanzeigen des Novell Netware Servers eingesehen und verändert werden (Datum, Uhrzeit, etc.) sowie Informationen zu den aktuellen Verbindungen eingesehen werden. Das Programm *SYS:\PUBLIC\FCONSOLE.EXE* kann standardmäßig durch den Supervisor bzw. einen äquivalenten Account aufgerufen werden. Andere Benutzer sollten auf diese Dateien keine Rechte besitzen.

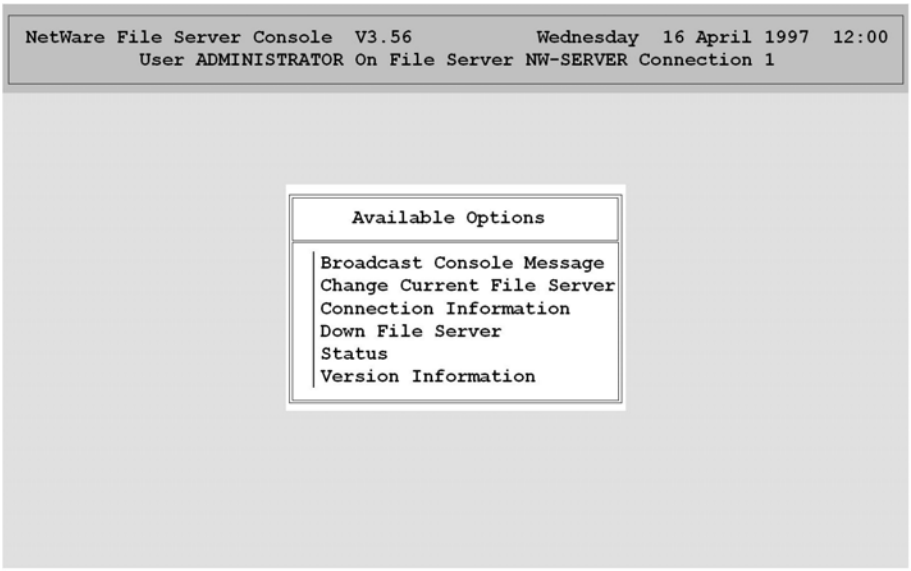


Abbildung 2: Menu *SYS:PUBLIC\FCONSOLE.EXE*

Intruder Detection/Lockout

Durch die Aktivierung des "Detect Intruders" werden unautorisierte Login-Versuche am Novell Netware Server erkannt und die hiervon betroffenen Accounts ggf. gesperrt.

Die Aktivierung des "Detect Intruders" sowie die weitere Parametrisierung dieses Menüpunktes beugt somit einer "Brute Force Attacke" unter Novell Netware vor.

Incorrect Login Attempts gibt hierbei die Anzahl der zulässigen Login Fehlversuche an; üblicherweise sollte hierbei der Wert "Drei" eingestellt werden.

Mit Hilfe von **Bad Login Count Retention Time** kann die zeitliche Zurückverfolgung von fehlgeschlagenen Login-Versuchen eines Accounts aktiviert werden. Übersteigt die Anzahl der Login-Fehlversuche eines Accounts innerhalb des definierten Zeitraumes den unter **Incorrect Login Attempts** eingestellten Wert, so wird der Benutzer Account auf dem Novell Netware Server gesperrt.

Der Menupunkt **Lock Account After Detection** sollte auf "Yes" eingestellt sein, um einen Account, der die Anzahl der ungültigen Login Versuche überschritten hat, zu sperren.

Der Zeitwert für **Length of Account Lockout** sollte keinesfalls zu gering gewählt werden (> 1 Stunde) um sicherzustellen, dass die Ursache für einen Intruder Lockout durch die Systemadministration und den betroffenen Benutzer aufgeklärt werden kann.

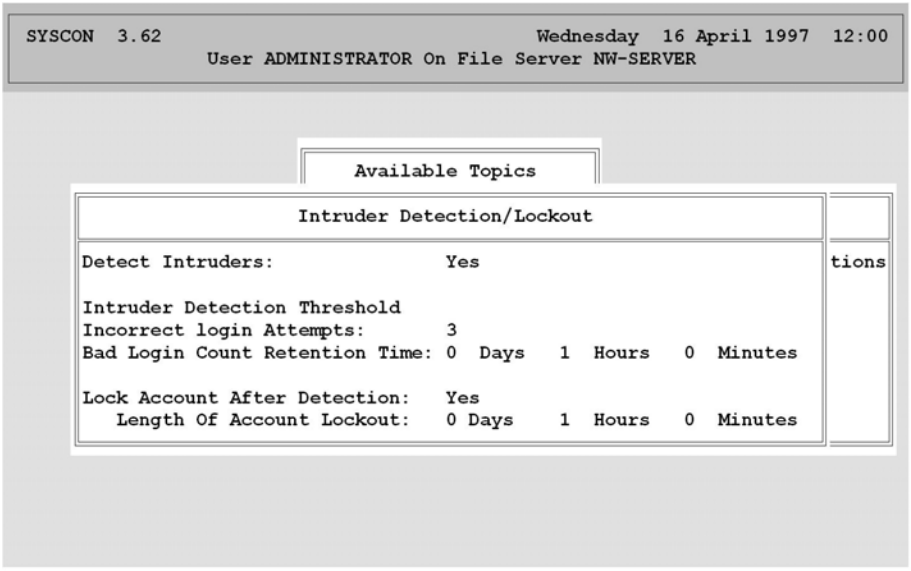


Abbildung 3: Menu *SYS:PUBLIC\SYSCON.EXE* "Supervisor Options - Intruder Detection Logout"

System Login Script

In dem System Login Script werden die Einstellungen vorgenommen, die für alle Benutzer nach deren Anmeldung auf dem Novell Netware Server existieren sollen. Das System Login Script wird, im Gegensatz zum User Login Script, für jeden Benutzer des Novell Netware Servers ausgeführt. Es ist daher sinnvoll, die Einstellungen, die für alle Benutzer des Novell Netware Servers gelten sollen, wie z. B. Laufwerkzuordnungen oder der Aufruf von externen Programmen, im System Login Script des Novell Netware Servers einzustellen.

Soll vermieden werden, dass ein Benutzer durch Verwendung des eigenen UER-Login-Scripts die Standardeinstellungen verändert, muss beim Verlassen des System-Login-Scripts der Befehl EXIT aufgenommen werden

Hinweis: Weiterhin ist für jeden Benutzer ein User-Login-Script zu erstellen. Dies ist erforderlich, da jeder Benutzer über das Zugriffsrecht "Create" im Verzeichnis *SYS:MAIL* verfügt. Einem Benutzer ohne User-Login-Script kann daher in seinem *SYS:MAIL*-Verzeichnis eine Datei *LOGIN* erzeugt werden, die Schadfunktionen ausführen kann.

View File Server Error Log

Das File Server Error Log ist das Fehlerprotokoll eines Novell Netware Servers. In ihm werden alle Fehler und Warnmeldungen des Servers gespeichert und können durch den Supervisor ausgewertet werden.

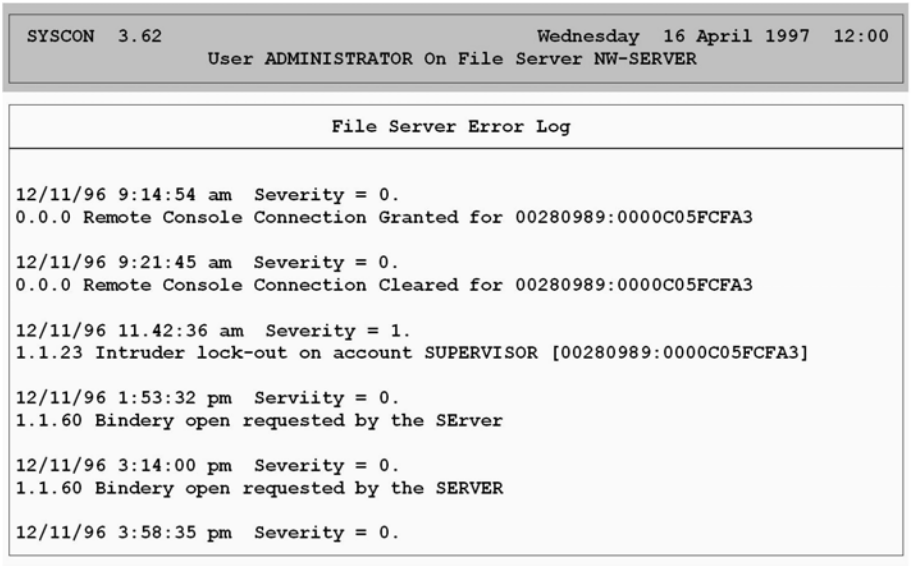


Abbildung 4: Menu *SYS:PUBLIC\SYSCON.EXE* "Supervisor Options - File Server Error Log"

Workgroup Managers

Ein Arbeitsgruppenverwalter (Workgroup Manager) ist ein eingeschränkter Supervisor Account, der das Recht zum Erstellen und Löschen von Bindery Objekten (Benutzer, Benutzergruppen, Druckerwarteschlangen) sowie deren Verwaltung hat. Die Rechte, die ein Arbeitsgruppenverwalter hierbei einsetzt bzw. an Benutzer und Benutzergruppen weitergeben darf, richten sich nach den durch den Supervisor zugestandenen Rechten.

Arbeitsgruppenverwalter können keine neuen Arbeitsgruppenverwalter oder einen Benutzer einrichten, dessen Sicherheitsstufe "Supervisor-äquivalent" ist, es sei denn, der Arbeitsgruppenverwalter verfügt über Supervisor-äquivalente Rechte.

Station Restrictions

Mit Hilfe des Menüpunktes Station Restrictions können die Netzadressen festgelegt werden, von denen aus sich ein Benutzer am Novell Netware Server anmelden darf. Informationen über die jeweilige Adresse einer Workstation im Netz lassen sich z. B. mit *SYS:PUBLIC\USERLIST.EXE /A* in Erfahrung bringen. Die Festlegung von erlaubten Netzadressen ist insbesondere für den Supervisor bzw. für äquivalente Accounts empfehlenswert. Dieses sollte jedoch vor Ort, je nach Gegebenheit, entschieden werden.

Standardisierte Einrichtung von Benutzern und Benutzergruppen

Neben der Einrichtung von Benutzern unter Einsatz des Menu-Utilities *SYS:PUBLIC\SYSCON.EXE* besteht zudem die Möglichkeit, Benutzer mit Hilfe der Utilities *SYS:\PUBLIC\MAKEUSER.EXE* und *SYS:\PUBLIC\USERDEF.EXE* einzurichten.

Diese eignen sich besonders für die gleichzeitige Einrichtung einer größeren Anzahl von Benutzern.

SYS:\PUBLIC\MAKEUSER.EXE erzeugt eine Art Batch-Datei, mit deren Hilfe mehrere Benutzer mit unterschiedlichen Rechten eingerichtet werden können.

SYS:\PUBLIC\USERDEF.EXE dient zur Einrichtung mehrerer Benutzer mit gleichen Rechten. Zu diesem Zweck wird eine Schablone (Template) erstellt, in der eingetragen wird, nach welchen Vorgaben die Benutzer einzurichten sind.

Diese Menu-Utilities sollten insbesondere in größeren Netzen aus Gründen einer vereinfachten und einheitlichen Administration eingesetzt werden.

M 2.100 Sicherer Betrieb von Novell Netware Servern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der sichere Betrieb eines Novell Netware Netzes setzt verschiedene Aktionen voraus, die nachfolgend beschrieben werden.

Vergabe von Zugriffsrechten auf Verzeichnisse und Dateien

Die Vergabe von Zugriffsrechten (Trustee Assignments) auf Verzeichnisse und Dateien von Novell Netware Servern spielt eine zentrale Rolle für die Sicherheit eines Novell Netware Servers.

Zugriffsrechte werden im Gegensatz zur Vergabe von Attributen einzelnen Benutzern bzw. Benutzergruppen zugewiesen.

Verzeichnisse und Dateien können über die Steuerung der Zugriffsrechte aufgabenbezogen zugewiesen werden. Hierdurch kann sichergestellt werden, dass Benutzergruppen bzw. Benutzer nur die Zugriffsrechte auf Verzeichnisse und Dateien haben, die sie zur Durchführung ihrer Aufgaben benötigen.

Aus Gründen der Übersichtlichkeit, einer vereinfachten Administration sowie einer verbesserten Revisionsfähigkeit sollte die Vergabe von Zugriffsrechten vorrangig über die Zuweisung von Rechten an Benutzergruppen erfolgen.

Um die versehentliche Freigabe von Verzeichnissen durch einen Benutzer zu verhindern, sollte die Systemadministration Benutzergruppen und Benutzern in den ihnen zugewiesenen Verzeichnissen die Rechte "Supervisory" (S) und "Access Control" (A) nicht erteilen.

Werden ausgewählten Verzeichnissen oder Dateien mit Hilfe von Netware-Attributen bestimmte Eigenschaften (z. B. schreibgeschützte Dateien) zugewiesen, so sollte beachtet werden, dass Benutzer, die das Zugriffsrecht "Modify (M)" auf die entsprechenden Verzeichnisse und Dateien besitzen, in der Lage sind, diese Attribute zu verändern. Daher sollte der Kreis der Benutzer mit diesem Zugriffsrecht eingeschränkt werden (s. u. Vergabe von Netware-Attributen auf Verzeichnisse und Dateien).

Vergabe von Netware-Attributen auf Verzeichnisse und Dateien

Neben der Benutzer- bzw. gruppenbezogenen Erteilung von Zugriffsrechten auf Verzeichnisse und Dateien kann durch die Vergabe von Netware-Attributen auf Verzeichnisse und Dateien die Datensicherheit erhöht werden. Attribute sind immer verzeichnis- bzw. dateibezogen, d. h. sie sind unabhängig von den zugewiesenen Zugriffsrechten und gelten für alle Benutzer einschließlich des Supervisors.

Benutzer, denen das Zugriffsrecht "Modify (M)" auf die in Frage kommenden Verzeichnisse und Dateien eingeräumt wurde, können die vergebenen Netware-Attribute ändern und somit jede Aktion, die sich aus ihren effektiven Rechten ergibt, ausführen.

Die Sicherheit durch den Einsatz von Netware-Attributen stellt sich somit als ein Subsystem in der Verzeichnis- und Dateisicherheit dar.

Bei der Vergabe von Netware-Attributen auf Verzeichnisse und Dateien sollten die folgenden Eigenschaften von Netware-Attributen beachtet werden.

- **Verzeichnis-Attribute:**

  Hidden (H): Das Verzeichnis wird als versteckt gekennzeichnet; es erscheint weder in einem Inhaltsverzeichnis unter DOS, noch kann es gelöscht oder kopiert werden.

  System (Sy): Das Verzeichnis (z. B. *SYS:SYSTEM\DELETED.SAV)* wird vom System benutzt; es erscheint ebenfalls nicht in einem Inhaltsverzeichnis unter DOS und kann weder kopiert noch gelöscht werden.

  Rename Inhibit (R): Das Verzeichnis kann nicht umbenannt werden.

  Delete Inhibit (D): Das Verzeichnis kann nicht gelöscht werden.

  Purge (P): Das Verzeichnis sowie die in ihm befindlichen Dateien werden beim Löschen sofort, auch physikalisch, gelöscht. Eine Wiederherstellung des Verzeichnisses mit Hilfe von *SYS:\PUBLIC\SALVAGE.EXE* ist nicht möglich.

- **Datei Attribute:**

  Read write (Rw): Auf die Datei ist sowohl Lese- wie auch Schreibzugriff möglich.

  Read only (Ro): Die Datei kann nur gelesen werden. Ein Schreibzugriff ist nicht möglich. Um Datenverluste bei einer gemeinsamen Benutzung zu vermeiden, sollten diese Dateien ebenfalls das Attribut "Shareable" (S) besitzen.

  Ausführbare Programmdateien (*.exe, *.com) sollten mit dem Attribut "Read only" versehen werden, um einem möglichen Befall durch Computer-Viren vorzubeugen.

  Shareable (S): Diese Dateien können von mehreren Benutzern gleichzeitig benutzt werden. Dateien, die mit dem Attribut "Shareable" versehen worden sind, sollten gleichzeitig das Attribut "Read Only" (RO) besitzen. Das Attribut "Shareable" ist nur relevant für Programme, die Dateien nicht netzfähig öffnen.

  Purge (P): Dateien mit dem Attribut "Purge" werden beim Löschen nicht nur logisch, sondern sofort physikalisch gelöscht. Dies hat zur Folge, dass die Datei nicht wiederhergestellt werden kann (*SYS:PUBLIC\SALVAGE.EXE*).

  In diesem Zusammenhang wird darauf hingewiesen, dass die physikalische Löschung von Dateien nicht nur durch das Netware-Attribut "Purge" erfolgen kann. Wenn das sichere Löschen von Verzeichnissen und Dateien gewünscht wird, dann kann hierzu das Netware Programm *SYS:PUBLIC\PURGE.EXE* eingesetzt werden.

  Transactional (T): Dateien mit diesem Attribut unterliegen der Transaktionskontrolle von Novell Netware. Als Transaktion wird hier eine zusammenhängende Folge von Veränderungen in einer oder mehreren

Dateien verstanden. Das Setzen dieses Attributes bewirkt, dass nur vollständig durchgeführte Transaktionen in den Datenbestand der Datei übernommen werden. Transaktionen, die unkorrekt abgebrochen wurden, werden von Novell Netware rückgängig gemacht.

Archive needed (A): Die so durch Novell Netware gekennzeichneten Dateien sind seit der letzten Datensicherung inhaltlich verändert oder neu auf dem Novell Netware Server aufgespielt worden. Datensicherungssoftware kann somit bei einer sequentiellen Datensicherung erkennen, dass die Datei erneut gesichert werden muss.

Copy Inhibit (C): Derartige Dateien können nicht kopiert werden. Dieses Netware-Attribut gilt allerdings nur für APPLE Macintosh Workstations.

Delete Inhibit (D): Die Datei kann nicht gelöscht werden.

Rename Inhibit (R): Die Datei kann nicht umbenannt werden.

Execute Only (X): Ausführbare Programmdateien (**.EXE*, **.COM*), die mit diesem Attribut versehen werden, können ausschließlich ausgeführt oder gelöscht werden. Ein Kopieren der Datei ist nicht möglich.

Hidden (H): Die Datei wird als versteckt gekennzeichnet. Sie erscheint nicht in einem Inhaltsverzeichnis unter DOS und kann weder kopiert noch gelöscht werden.

System (S): Die Datei (z. B. Bindery Dateien -*NET$OBJ.SYS*, *NET$PROP.SYS*, *NET$VAL.SYS)* wird vom Netzbetriebssystem verwendet; sie erscheint ebenfalls nicht in einem Inhaltsverzeichnis unter DOS und kann weder kopiert noch gelöscht werden.

Sicherung wichtiger Systemdateien

Die Server Startdateien *AUTOEXEC.NCF* und *STARTUP.NCF* sollten, in ihrer jeweils aktuellen Fassung, durch den Systemadministrator auf Diskette gesichert werden und vor unbefugtem Zugriff gesichert hinterlegt werden. Es ist sinnvoll, diese Dateien durch Kommentierungszeilen zu ergänzen, damit beim Auftreten von Problemen die jeweils eingestellten Parameter nachvollzogen werden können.

Weiterhin sollte die Bindery (*NET$OBJ.SYS*, *NET$PROP.SYS*, *NET$VAL.SYS*) eines Novell Netware Servers regelmäßig mit Hilfe des Programms *SYS:SYSTEM\BINDFIX.EXE* gesichert werden. Die gesicherte Bindery (*SYS:SYSTEM*.OLD*) sollte im Anschluss auf einen Datenträger gesichert und vor unbefugten Zugriff geschützt hinterlegt werden.

Nach der Ausführung von *SYS:SYSTEM\BINDFIX.EXE* sollte die Integrität der neuen Bindery auf jeden Fall getestet werden. Im Zweifelsfalle kann die alte Bindery durch *SYS:SYSTEM\BINDREST.EXE* wiederhergestellt werden.

Da die aktuelle Bindery während der Ausführung von *SYS:SYSTEM\BINDFIX.EXE* dem Zugriff der Benutzer entzogen wird, sollte aus Gründen der Betriebssicherheit bei der Sicherung der Bindery eines Novell Netware Servers außer dem Supervisor bzw. dem Supervisor-äqui-

valenten Benutzer kein Benutzer auf dem Novell Netware Server eingeloggt sein.

Eingeschränkte Nutzung des Supervisor Account bzw. eines Supervisor-äquivalenten Account

Der Account des Supervisors sollte bei der täglichen Administrationsarbeit nicht verwendet werden, sondern nur in Notfällen benutzt werden. Um dennoch die Systemadministration zu gewährleisten, sollte daher für jeden Benutzer mit der Netware-Sicherheitsstufe "Supervisor" ein Supervisor-äquivalenter Account eingerichtet werden, mit dem die Systemadministration normalerweise erfolgt. Werden die Administrationsarbeiten nicht hauptamtlich wahrgenommen, so sollten für die nicht-administrativen Aufgaben zusätzlich aufgabenbezogene Accounts eingerichtet werden.

Der Account des Supervisors bzw. eines Supervisor-äquivalenten Account sollte weiterhin nur auf hierzu definierten Workstations verwendet werden, da die Integrität anderer Workstations u. U. durch Benutzer manipuliert sein könnte.

Delegierung der Systemverwaltung

In größeren Netzen (mehrere Novell Netware Server oder verschiedene Liegenschaften) bzw. bei einer größeren Anzahl von Benutzern empfiehlt es sich, bestimmte Aufgaben der Systemadministration zu delegieren. Novell Netware 3.x bietet hierzu die Möglichkeit, Benutzer zu User-Account-Managern bzw. Workgroup-Managern zu bestimmen.

User-Account-Manager können die Benutzer und Gruppen verwalten, die ihnen vom Systemverwalter zugewiesen wurden. Dabei sind sie in der Lage, neben der Änderung der Benutzerdaten (Passwort, Benutzungszeiten usw.) alle Rechte, über die sie selbst verfügen, weiter zu geben. Des weiteren kann der User-Account-Manager einzelne Benutzer einer Gruppe zuweisen. Dabei müssen sowohl die Gruppen als auch die Benutzer vom entsprechenden User-Account-Manager verwaltet werden. Der User-Account-Manager ist nicht in der Lage neue Benutzer oder Gruppen einzurichten. Allerdings kann er ihm zugewiesene Benutzer oder Gruppen löschen.

Ein Workgroup-Manager hat alle Rechte eines User-Account-Managers. Darüber hinaus ist er in der Lage, neue Benutzer und Gruppen einzurichten. Eine weitere Aufgabe des Workgroup-Managers ist das Einrichten von Druckerwarteschlangen.

Nutzung von NCP-Paket-Signatur

Die Kommunikation eines Novell Netware Clients mit einem Novell Netware-Server wird durch das Netware Core Protokoll (NCP) gesteuert. Client und Server tauschen hierbei einzelne Pakete aus, in denen die Daten enthalten sind. Ein potentieller Angreifer kann diese Pakete mittels spezieller Programme (siehe G 5.58 *"Hacking Novell Netware"*) überwachen und die Datenpakete höher privilegierter Benutzer manipulieren.

Um dieser Bedrohung entgegenzuwirken, wurde die Paket-Signatur entwickelt. Bei der Anmeldung eines Benutzers am Server wird ein geheimer Schlüssel ermittelt. Wann immer die Workstation daraufhin eine Anfrage über

NCP an den Server sendet, wird diese mit einer Signatur versehen, die aus dem geheimen Schlüssel und der Signatur des vorherigen Pakets gebildet wird. Diese Signatur wird an das betreffende Paket angehängt und zum Server gesandt. Bevor die eigentliche Anfrage bearbeitet wird, verifiziert der Server die Paket-Signatur.

Durch die Option *Set NCP Packet Signature* -Wert- kann die Paket-Signatur am Server aktiviert werden.

Es sind folgende NCP-Paket-Signatur Level möglich:

Wert "0":	Es findet keine NCP-Paket-Signatur statt.
Wert "1":	Der Novell Netware Server arbeitet auf Anforderung des Clients mit der NCP-Paket-Signatur.
Wert "2":	Der Novell Netware Server fordert vom Client NCP-Paket-Signatur an. Sollte der Client dieses nicht realisieren können, so wird die Kommunikation zwischen Client und Novell Netware Server trotzdem zugelassen.
Wert "3":	Die NCP-Paket-Signatur ist zwingend vorgeschrieben.

Tabelle: NCP-Paket-Signatur Level

Zur Gewährleistung der IT-Sicherheit sollte die NCP-Paket-Signatur mit dem Wert "3" gewählt werden. Da sich jedoch die Netzlast beim Einsatz der NCP-Paket-Signatur um bis zu 30% erhöht, sollte im Vorfeld des Einsatzes geklärt werden, ob die Performance hierdurch nicht unzumutbar eingeschränkt wird.

Beschränkung des nutzbaren Festplattenspeichers

Mit Hilfe des Programms *SYS:PUBLIC\DSPACE.EXE* sollte der auf einem Volume oder einem Verzeichnis zur Verfügung stehende Festplattenspeicher limitiert werden, da erfahrungsgemäß die Inanspruchnahme des zur Verfügung stehenden Festplattenspeichers mit der Kapazität des Festplattenspeichers steigt.

Alternativ hierzu kann auch, soweit eingerichtet, die Kapazität des jeweiligen persönlichen Verzeichnis eines Benutzers beschränkt werden, wenn für die Arbeitsdaten eigene Verzeichnisse eingerichtet wurden.

Sperrung von nicht benötigten Programmen

Die meisten der unter *SYS:PUBLIC* bereitgestellten Novell Netware Programme werden durch die Netware-Benutzer im Regelfall nicht benötigt, da viele der Funktionen (Druckerkonfigurationen, Änderung des Passwortes, Laufwerkszuweisungen) durch die Client- Software gehandhabt werden können. Aus diesem Grund sowie der meist ungewohnten Handhabung der Novell Netware Dienstprogramme empfiehlt es sich, nicht benötigte Programme in das Verzeichnis *SYS:SYSTEM* zu verschieben. Insbesondere das Programm *SYS:PUBLIC\RENDIR.EXE* sollte wegen der erkannten Gefährdung (G 5.54 *Vorsätzliches Herbeiführen eines Abnormal End*) den Benutzern nicht zur Verfügung gestellt werden.

Keinesfalls sollten, wie oftmals beobachtet, die unter *SYS:SYSTEM* gespeicherten Programme in das Verzeichnis *SYS:PUBLIC* verlagert werden.

Information über Patches von Novell Netware

Im Verlauf der Entwicklung des Netzbetriebssystems Novell Netware 3.x haben sich diverse Schwachstellen bzw. Unzulänglichkeiten herausgestellt, die durch den Hersteller mit Hilfe von so genannten Patches größtenteils behoben wurden. Diese Patches werden durch den Hersteller im Internet zur Verfügung gestellt (http://www.novell.com, ftp.novell.com bzw. http://www.novell.de, ftp.novell.de). Informationen über die Funktionalität sowie das ggf. erforderliche Einspielen der zur Verfügung gestellten Patches können daher Schwachstellen im laufenden Produktionsbetrieb beseitigen. Insbesondere zusätzlich installierte Softwareprodukte, wie z. B. zur Datensicherung, erfordern oftmals einen bestimmten Patchlevel des Netzbetriebssystems. Hierbei ist jedoch zu beachten, dass die angebotenen Patches keineswegs blind aufgespielt werden sollten, sondern nur im Bedarfsfall ("never change a running system") sowie nach gründlicher Information.

Soweit vorhanden, sollten diese Patches zunächst auf einer Testkonfiguration ausgetestet werden.

Im Internet (Usenet) ist, neben den internationalen Diskussionsforen zum Thema Novell Netware (z. Z. comp.os.netware.announce, comp.os.netware.misc, comp.os.netware.security, bit.listserv.novell), für die deutschsprachigen Benutzer ein deutsches Novell Forum (z. Z. de.comp.sys.novell) vorhanden, in dem einige versierte Novelladminstratoren aktiv sind, die oftmals auch die schwierigsten Probleme zu lösen helfen. Außerdem werden zu den im Internet am häufigsten gestellten Fragen Dateien (so genannte FAQs - Frequently Asked Questions) zur Verfügung gestellt, die die häufigsten Probleme thematisieren und Lösungen anbieten.

Patches und Informationen über Novell Netware werden darüber hinaus auch über andere Anbieter von Netzdiensten, wie z. B. Compuserve, Fidonet und Mailboxen bereitgestellt.

Für die Richtigkeit und Vollständigkeit der jeweiligen Informationen in den Usenet Diskussionsforen sowie in den FAQs kann an dieser Stelle jedoch keine Garantie gegeben werden. Es sei darauf hingewiesen, dass eine vollständige Beschreibung des aufgetretenen Problems, sowie eine Beschreibung der jeweiligen Konfiguration des Netzes (Client, Server) besonders vorteilhaft bei der Hilfesuche im Internet (Usenet) ist.

Schwierigkeiten während des Netzbetriebes können darüber hinaus oftmals durch die Nachfrage bei dem Verkäufer des Netzbetriebssystems oder im Informationsaustausch mit Kollegen behoben werden; wobei auch hier die Problemlösung durch eine vollständige Konfigurationsbeschreibung erleichtert wird.

Prüfung auf Computer-Viren

Computer-Viren, die sich in den auf einem Novell Netware Server gespeicherten Programmen und Dateien befinden, können, aufgrund der zentralen Verteilung durch den Novell Netware Server an die Workstations, erhebliche Schäden im Netzverbund hervorrufen.

Aus diesem Grund sollten die Programme und Dateien eines Novell Netware Servers regelmäßig mit einem aktuellen Virensuchprogramm auf evtl. vorhandene Computer-Viren überprüft werden.

Zu diesem Zweck empfiehlt es sich einen speziellen Benutzer-Account auf dem Novell Netware Server einzurichten, der über die Zugriffsrechte "Read" (R) und "File Scan" (F) auf alle Dateien des Servers verfügt. Die Prüfung auf Computer-Viren sollte keinesfalls mit den Rechten des Supervisors, bzw. Supervisor-äquivalenten Rechten durchgeführt werden, da ein Computer-Viren-Checkprogramm, welches selbst mit einem Computer-Virus infiziert ist, diesen auf alle Programme und Dateien des Novell Netware Servers übertragen würde.

Die Benutzer bzw. Benutzergruppen sollten auf die Verzeichnisse und Dateien mit ausführbarem Programmcode lediglich die effektiven Rechte "Read" (R) und "File scan" (F) erhalten, zudem sollten ausführbare Programme mit dem Netware-Attribut "Read only" (RO) versehen werden.

M 2.101 Revision von Novell Netware Servern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die vollständige Revision eines Novell Netware 3.x Servers dürfte in der Praxis im Rahmen IT-Grundschutz kaum möglich sein. Folgende Revisionsansätze sollten dennoch beachtet werden:

Durch das Programm *SYS:SYSTEM\SECURITY.EXE* werden die Bindery-Dateien eines Novell Netware Servers auf die nachfolgenden Sicherheitsschwachstellen hin untersucht und die erkannten Schwachstellen aufgelistet.

No password assigned

Benutzer, die kein Passwort für das Login auf dem Novell Netware Server benötigen, werden aufgelistet.

Insecure passwords

Hierbei wird die Bindery des Novell Netware Servers auf mehrere Aspekte hin untersucht.

Zum einen werden die Benutzer angezeigt, deren Passwort gleich dem Anmeldenamen auf dem Novell Netware Server ist; weiterhin werden alle Benutzer aufgeführt, deren Passwort weniger als fünf Zeichen lang sein darf. Es wird weiterhin für jeden Benutzer geprüft, ob die Gültigkeitsdauer eines Passwortes mehr als 60 Tage beträgt und ob eine unbegrenzte Anzahl von "Frei-Anmeldungen" (Grace Logins) möglich ist.

Supervisor equivalence

SYS:SYSTEM\SECURITY.EXE überprüft die Bindery eines Novell Netware Servers dahingehend, ob Benutzer die Sicherheitsstufe "Supervisor" (Supervisor equivalence) auf dem Novell Netware Server haben, und führt diese auf.

Root directory privileges

Aufgrund der nach "unten" gerichteten Vererbung von Zugriffsrechten werden alle Benutzer eines Novell Netware Servers dahingehend geprüft, ob sie Zugriffsrechte im Hauptverzeichnis (Volume Ebene) haben.

Login scripts

Es werden alle Benutzer ermittelt, die über kein eigenes Login Script (User Login Script) verfügen.

Da alle Benutzer, um elektronische Nachrichten austauschen zu können, standardmäßig über das Zugriffsrecht "Create" in dem Verzeichnis *SYS:MAIL* verfügen, könnte ein "Angreifer" einem Benutzer, der über kein User Login Script verfügt, in dessen *SYS:MAIL* Verzeichnis eine Datei *LOGIN* (User-Login-Script) kopieren, mit dem dessen Novell Netware Umgebung verändert würde.

Excessive rights

Novell Netware 3.x stellt im Rahmen der Installation standardmäßig mehrere Verzeichnisse zur Verfügung (*SYS:SYSTEM, SYS:PUBLIC, SYS:LOGIN*). SYS:SYSTEM*SECURITY.EXE* überprüft die Bindery des Novell Netware Servers, ob Benutzer in diesen Verzeichnissen größere Rechte haben, als die standardmäßig vorgegebenen. Weiterhin werden die *SYS:MAIL* Verzeichnisse aller Benutzer auf das alleinige Verfügungsrecht (Ausnahme "Create" für die Gruppe "Everyone") des jeweiligen Inhabers geprüft.

Ergänzende Kontrollfragen:

- Wann wurde die letzte Revision durchgeführt?
- In welchen Intervallen erfolgt eine Revision?

M 2.102 Verzicht auf die Aktivierung der Remote Console

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Das Netzbetriebssystem Novell Netware ermöglicht mittels des Programmes *SYS:\SYSTEM\RCONSOLE.EXE* die Fernsteuerung der Novell Netware Serverkonsole durch eine Workstation. Der Novell Netware Server wird hierzu in der *AUTOEXEC.NCF* durch das Laden von *REMOTE.NLM* mit dem dazugehörenden Passwort und *RSPX.NLM* eingerichtet. Dabei muss vermieden werden, dass das Passwort im Klartext in der *AUTOEXEC.NCF* enthalten ist. Dazu kann nach Ausführen des Programms *REMOTE.NLM* der Befehl *REMOTE ENCRYPT* an der Serverkonsole eingegeben werden. Das dann abgefragte Passwort wird verschlüsselt und auf Wunsch mit dem dazugehörigen Befehl in der Datei *LDREMOTE.NCF* abgelegt. Der Befehl in der Datei *LDREMOTE.NCF* sieht z. B. wie folgt aus:

LOAD REMOTE -E 0613BB68060099

Netzanalyse-Tools, so genannte Sniffer, können die Daten, die zwischen der Workstation und dem Novell Netware Server ausgetauscht werden, auslesen und speichern. Hierzu gehört auch das verschlüsselte Passwort, welches zur Fernsteuerung des Novell Netware Servers eingegeben werden muss. Spezielle Software ist in der Lage, das verschlüsselte Passwort zu entschlüsseln. Unbefugte können hierdurch in die Lage versetzt werden, mittels der Fernsteuerung Zugriff auf die Konsole des Novell Netware Servers zu erlangen.

Um zudem zu verhindern, dass Remote-Sitzungen mit Netzanalyse-Tools aufgezeichnet und danach einfach wieder ins Netz eingespielt werden können, sollte darauf geachtet werden, dass Signaturen bei den RSPX-Paketen aktiviert sind. Dies kann überprüft werden, indem der Befehl *RSPX* an der Konsole des Servers ausgeführt wird. Die Antwort sollte wie folgt aussehen:

RSPX Packet Signatures:

All packets must contain signatures.

Sollten hier keine Signaturen aktiviert sein, kann dies durch den Befehl *RSPX SIGNATURES ON* veranlasst werden. Da diese Funktion erst ab Netware 3.12 unterstützt wird, sollte unbedingt auf die aktuelle Netware Version zurückgegriffen werden.

Soweit die örtlichen Gegebenheiten und die betrieblichen Abläufe dieses zulassen, sollte aus Sicherheitserwägungen auf die Fernsteuerung von Novell Netware Servern verzichtet werden.

Generell gilt jedoch, wenn C2-Sicherheit umgesetzt werden soll (siehe auch M 4.102 *C2-Sicherheit unter Novell 4.11*), dann darf das Programm *SYS:\SYSTEM\RCONSOLE.EXE* nicht eingesetzt werden.