



Die 20 kritischsten Internet-Schwachstellen (aktualisiert) ~ Der Expertenkonsens

Version 4.0, 8. Oktober 2003 Copyright (C) 2001-2003, SANS Institute
Fragen / Bemerkungen können an top20@sans.org geschickt werden.

-----[Zum Index der 20 kritischsten Schwachstellen](#)-----

Einleitung

Die SANS Top 20 Internet-Schwachstellen

Die überwiegende Mehrheit von Würmern und anderen erfolgreichen Cyberattacken werden durch Schwachstellen in einigen gebräuchlichen Betriebssystemen ermöglicht. Angreifer sind opportunistisch. Sie nehmen den einfachsten und bequemsten Weg und nutzen bekannte Fehler mit leistungsfähigen und weit verbreiteten Angriffswerkzeugen aus. Sie rechnen mit Organisationen, die ihre Probleme nicht lösen, und sie greifen wahllos an, indem sie einfach das Internet nach fehlerhaften Systemen durchsuchen. Die einfache und destruktive Verbreitung von Würmern, wie Blaster, Slammer und Code Red können auf Systeme zurückgeführt werden, die Patches nicht installiert haben.

Vor vier Jahren haben das SANS Institute, das Nationale Infrastruktur Projekt Center (NIPC) und das FBI ein Dokument veröffentlicht, in dem die 10 kritischsten Internet-Schwachstellen dokumentiert wurden. Tausende Organisationen haben diese Liste verwendet und die nachfolgende Version, die ein bis zwei Jahre später erschien, enthielt bereits die 20 kritischsten Internet-Schwachstellen. Damit wurde den Organisationen eine priorisierte Liste zur Verfügung gestellt, die es ermöglicht, die gefährlichsten Schwachstellen zuerst zu beheben. Die Schwachstellen, die zu den vorhin erwähnten Problemen wie Blaster, Slammer oder Code Red sowie NIMDA geführt haben, sind in dieser Liste enthalten.

Diese aktualisierte Top 20 Liste besteht eigentlich aus zwei Top 10 Listen: die zehn am häufigsten ausgenutzten Schwachstellen in Windows und die zehn am häufigsten ausgenutzten Schwachstellen in UNIX und Linux. Obwohl es jedes Jahr Tausende Sicherheitsvorfälle gibt, die diese Betriebssysteme betreffen, ist eine große Anzahl von erfolgreichen Angriffen auf eine oder mehrere dieser Schwachstellen zurückzuführen.

Die Top 20 Liste ist eine Konsensliste von Schwachstellen, die eine umgehende Behebung erfordern. Sie ist das Ergebnis von Dutzenden führenden Sicherheitsexperten. Diese Experten sind von den am sicherheitsbewusstesten Bundesstellen der USA, Großbritanniens und Singapur; den führenden Sicherheitssoftwareanbietern und Consultingunternehmen; den Top 10 Sicherheitsprogrammen von Universitäten; vielen anderen Benutzerorganisationen; und des SANS Institutes. Eine Liste der Beteiligten kann am Ende des Dokuments gefunden werden.

Das SANS Top 20 ist ein lebendes Dokument. Es inkludiert Schritt für Schritt Instruktionen und Hinweise für zusätzliche Informationsquellen um Sicherheitsschwachstellen zu beheben. Die Liste wird aktualisiert, sobald kritischere Sicherheitslücken bekannt werden. Dieses Dokument ist ein Gemeinschaftskonsensdokument - Ihre Erfahrung im der Bekämpfung von Angriffen und im Eliminieren von Schwachstellen kann anderen helfen. Bitte senden Sie Anregungen via e-Mail an top20@sans.org.

Anmerkungen für den Leser

CVE Nummern

Sie finden zu jeder Sicherheitsschwachstelle eine Referenz zu CVE Nummern (Common Vulnerabilities and Exposures). Sie können auch CAN Nummern sehen. CAN Nummern sind Kandidaten für CVE Einträge, sind aber noch nicht vollständig verifiziert. Zusätzliche Information bezüglich des ausgezeichneten CVE Projektes finden Sie unter <http://cve.mitre.org>.

Die CVE und CAN Nummern reflektieren die am höchsten priorisierten Schwachstellen, die für jedes Gerät überprüft werden sollen. Jede CVE Sicherheitsschwachstelle ist mit dem dazugehörigen ICAT Eintrag des National Institute of Standards and Technology verbunden (<http://icat.nist.gov>). ICAT stellt eine kurze Beschreibung, eine Liste von Charakteristiken (z.B. zugehörige Angriffe, Schadenspotenzial), eine Liste der betroffenen Software inklusive Versionsnummern und Links zu Schwachstellen-Advisories und Patches jeder Schwachstelle zur Verfügung.

Welche Ports sollen auf der Firewall gesperrt werden

---- Index - Ports die auf der Firewall oder dem Gateway gesperrt werden sollen ----

Am Ende des Dokumentes finden Sie eine Liste von Ports, die üblicherweise abgefragt bzw. attackiert werden. Wenn Sie diese Ports auf der Firewall oder anderen netzwerkbegrenzenden Sicherheitsgeräten blockieren, fügen Sie eine zusätzliche Sicherheitsebene ein, die z.B. vor Konfigurationsfehlern schützen kann. Es ist aber wichtig zu verstehen, dass das Sperren eines Ports auf der Firewall oder auf einem Router nicht vor verärgerten Mitarbeitern schützt, die sich innerhalb der Abgrenzung befinden oder vor Hackern, die möglicherweise bereits andere Zugänge zum internen Netzwerk gefunden haben. Es ist eine sicherere Praktik, standardmäßig alle Ports zu blockieren und nur die Ports zu öffnen, die unbedingt notwendig sind, als umgekehrt alle Ports zu öffnen und individuelle Ports zu blockieren.

[zum Anfang ^](#)

Top Schwachstellen in Windows Systemen

- [W1 Webserver und Services](#)
- [W2 Workstation Service](#)
- [W3 Windows Remote Access Service](#)
- [W4 Microsoft SQL Server \(MSSQL\)](#)
- [W5 Windows Authentifizierung](#)
- [W6 Web Browser](#)
- [W7 File Sharing Applikationen](#)
- [W8 LSASS](#)
- [W9 Mail Client](#)
- [W10 Instant Messaging](#)

Top Schwachstellen in UNIX Systemen

- [U1 BIND Domain Name System](#)
- [U2 Remote Procedure Calls \(RPC\)](#)
- [U3 Apache Web Server](#)

- U4 Allgemeine UNIX Benutzerkonten mit schwachen oder ohne Passwörtern
- U5 Klartext Dienste
- U6 Sendmail
- U7 Simple Network Management Protocol (SNMP)
- U8 Secure Shell (SSH)
- U9 Fehlkonfiguration der Enterprise Dienste NIS/NFS
- U10 Open Secure Sockets Layer (SSL)

[zum Anfang ^](#)

Top Schwachstellen in Windows Systemen (W)

W1 Webserver und Services

W1.1 Beschreibung

Die standardmäßige Installationen von verschiedenen HTTP Servern und Zusatzkomponenten die für HTTP Anfragen dienen wie auch Streaming Media zum Internet auf Windows Plattformen sind bekannter weise anfällig für eine Vielzahl von Attacken. Die Auswirkungen dieser Sicherheitsschwachstellen können Folgendes enthalten:

- Denial of Service
- Gefährdung und Aussetzung von sensible Dateien oder Daten
- Ausführen von beliebigen Befehlen auf dem Server
- Komplette Kompromittierung des Servers

HTTP Server wie IIS, Apache und iPlanet (jetzt SunOne) hatten eine Anzahl von Problemen, die erkannt und mittels Patch behoben wurden. Stellen Sie sicher, dass alle Systeme die aktuellen Patches installiert haben und dass die aktuellen Versionen verwendet werden. Die meisten HTTP Server sind in der Standardkonfiguration offen und bieten eine Vielzahl von Möglichkeiten um Sicherheitslücken auszunutzen zu können. Nehmen Sie sich die Zeit um zu gewährleisten, dass nur die Features, die für den Betrieb des Webserver absolut notwendig sind verfügbar sind.

IIS verwendet einen Anbindungsstelle für Software die als ISAPI bekannt ist und die Dateien mit bestimmten Dateierweiterungen mit DLLs verbindet (ISAPI Filter). Präprozessoren wie ColdFusion und PHP verwenden ISAPI. IIS enthält viele ISAPI Filter, um Funktionen wie Active Server Pages (ASP), Net web Services und webbasierendes Druckersharing zu verarbeiten. Viele der ISAPI Filter, die standardmäßig mit dem IIS installiert werden, werden nicht benötigt und viele dieser Filter sind ausnutzbar. Beispiele von bösartigen Programmcode, die diese Schwachstellen ausnutzen, sind die bekannten Würmer Code Red und Code Red 2.

Aktivieren Sie nur ISAPI Extensions die der Webserver unbedingt erkennen muss. Es wird auch empfohlen, die HTTP Optionen einzuschränken, die mit den ISAPI Extensions verwendet werden können.

Die meisten Webserver enthalten auch Applikationsbeispiele oder Webseiten, die dazu dienen, die Funktionalität des Webserver zu demonstrieren. Diese Applikationen wurden nicht dafür entwickelt, um in einer Produktionsumgebung sicher zu funktionieren. Einige dieser IIS Applikationsbeispiele erlauben Lesen oder Überschreiben von beliebigen Dateien sowie Remotezugriff auf andere sensible Serverinformationen, inklusive des Administratorkennwortes. Entfernen Sie diese Applikationen bevor Sie den Server produktiv schalten.

Eine IIS Installation die nicht regelmäßig und ordnungsgemäß instand gehalten wird, ist ebenfalls anfällig für Schwachstellen, die seit der Softwareveröffentlichung bekannt geworden sind. Beispiele dafür sind die PCT und SLL Schwachstelle, die im Microsoft Patch MS04-011 beschrieben sind, die einen Denial of Service Angriff ermöglichen könnten. Ein Angreifer könnte auch die Kontrolle über den Server erlangen. Die zeitgerechte Aktualisierung von öffentlich

zugängigen Webservern ist unbedingt notwendig.

Webzusatzprogramme von Dritten, wie ColdFusion oder PHP können zusätzlich Schwachstellen in die IIS Installation bringen, entweder durch falsche Konfiguration oder durch Schwachstellen in den Produkten.

W1.2 Betroffene Betriebssysteme

Jedes Microsoft Windows System mit einem installierten Webserver kann betroffen sein. Das inkludiert, ist aber nicht beschränkt auf:

- Microsoft IIS: Windows NT4.0 und neuere Versionen, auch Windows XP Professional
- Apache HTTP Server: Windows NT4.0 SP3 und neuere Versionen sind unterstützt, es wird jedoch angenommen, dass auch Win95 und Win98 verwendet werden kann
- Sun Java System/Sun One/iPlanet Web Server: Windows NT4.0 SP6 und neuere Versionen

Wichtiger Hinweis: Windows 2000 Server haben standardmäßig den IIS installiert, wie viele Administratoren bei den Nimda und Code Red Attacken festgestellt haben. Darüber hinaus benötigen einige Produkte von Drittfirmen die IIS Funktionalität, wodurch der Administrator unwissentlich den IIS installiert. Nehmen Sie nie an, dass ein Netzwerk gegen Web Server Attacken immun ist, nur weil kein Server wissentlich installiert wurde; überprüfen Sie regelmäßige das Netzwerk auf Webserver, die eigentlich nicht installiert sein sollten. Lesen Sie „Wie Sie herausfinden, ob Sie betroffen sind“ für zusätzliche Information.

W1.3 Zugehörige CVE/CAN Einträge

a. IIS

[CVE entries for IIS 2.0](#)
[CVE entries for IIS 3.0](#)
[CVE entries for IIS 4.0](#)
[CVE entries for IIS 5.0](#)

b. Apache

[CAN-2001-0729](#), [CAN-2002-0249](#), [CAN-2002-0654](#), [CAN-2002-0661](#), [CAN-2002-0661](#),
[CAN-2003-0016](#), [CAN-2003-0017](#), [CAN-2003-0460](#), [CAN-2003-0844](#), [CAN-2004-0492](#),
[CAN-2004-0493](#)

[CVE-1999-0448](#), [CVE-2000-0505](#), [CVE-2001-1342](#), [CVE-2001-1342](#)

Apache modules: [CAN-2003-0844](#), [CAN-2004-0492](#)

c. iPlanet/Sun

[CAN-2002-0686](#), [CAN-2002-1042](#), [CAN-2002-1315](#), [CAN-2002-1315](#), [CAN-2002-1316](#),
[CAN-2003-0411](#), [CAN-2003-0412](#), [CAN-2003-0414](#), [CAN-2003-0676](#), [CAN-2003-0676](#)

[CVE-2000-1077](#), [CVE-2000-1077](#), [CVE-2001-0252](#), [CVE-2001-0327](#), [CVE-2001-0327](#),
[CVE-2002-0845](#), [CVE-2002-0845](#)

d. Add-Ons

[CAN-1999-0455](#), [CAN-1999-0477](#), [CAN-1999-1124](#), [CAN-2001-0535](#), [CAN-2001-1120](#),
[CAN-2002-1309](#), [CAN-2003-0172](#)

[CVE-1999-0756](#), [CVE-1999-0922](#), [CVE-1999-0924](#), [CVE-2000-0410](#), [CVE-2000-0538](#)

ColdFusion: [CVE-1999-0756](#), [CVE-1999-0760](#), [CVE-1999-0922](#), [CVE-1999-0924](#), [CAN-2002-1309](#), [CAN-2004-0407](#), [CVE-2000-0189](#), [CVE-2000-0382](#), [CVE-2000-0410](#), [CVE-2000-0538](#), [CVE-2002-0576](#)

PHP: [CAN-2002-0249](#), [CAN-2003-0172](#)

e. Andere Services

[CAN-1999-1369](#), [CAN-2003-0227](#), [CAN-2003-0349](#), [CAN-2003-0725](#), [CAN-2003-0905](#)

[CVE-1999-0896](#), [CVE-1999-1045](#), [CVE-2000-0211](#), [CVE-2000-0272](#), [CVE-2000-0474](#),
[CVE-2000-1181](#), [CVE-2001-0083](#)

eEye SecureIIS: [CAN-2001-0524](#)

Jakarta Tomcat: [CAN-2003-0045](#)

W1.4 Wie Sie herausfinden, ob Sie betroffen sind

Standardmäßig installierte oder nicht aktualisierte Webserver Installationen können als anfällig eingestuft werden.

Die meisten Webserver- und Serviceanbieter stellen eine Fülle von Informationen bezüglich der derzeitigen Sicherheitsprobleme zur Verfügung. Beispiele inkludieren:

- Apache HTTP Server [Main Page & Security Report](#)
- [Microsoft TechNet Security Centre](#)
- [Microsoft Internet Information Server \(IIS\) Security Centre](#)
- [Sun Web, Portal, & Directory Servers Download Centre](#)
- [Macromedia Security Zone](#)
- [Real Networks Security Issues](#)
- PHP [Home Page](#) und [Downloads](#)

Vergleichen Sie auch regelmäßig jeden Webserver und in Verbindung stehende Service Patches und Softwareversionen, inklusive Konfigurationen, mit den vom Hersteller zur Verfügung gestellten Sicherheitsinformationen und der CVE Datenbank um potentielle Sicherheitsschwachstellen zu erkennen. Es ist wichtig zu erkennen, dass neue Probleme immer wieder erkannt werden und es ist „best practice“ die CVE Datenbank zu konsultieren, um potentielle Sicherheitsschwachstellen abrufen zu können.

Es existieren einige Tools die remote oder lokal verwendet werden können um Webserver Administratoren zu helfen, das Netzwerk zu überprüfen:

- [Nessus](#) (Open-Source)
- [SARA](#) (Open-Source)
- [Nikto](#) (Open-Source)
- [eEye Free Utilities & Commercial Scanners](#)
- [Microsoft Baseline Security Analyzer](#) (IIS-spezifisch)

Es wird empfohlen, dass remote Tools zur Sicherheitsschwachstellenerkennung im Netzwerk

verwendet werden, nicht nur gegen bekannte Webserver. So können auch nicht bekannte Webserver gefunden werden..

Administratoren sollen die vielen Checklisten ([checklists](#)), Härtungsvorschriften ([hardening guides](#)) und Schwachstellenbehebungsdokumente ([vulnerability remediation](#)), die von Microsoft zur Verfügung gestellt werden, lesen und mit den eigenen Systemen vergleichen. Dadurch kann abgeschätzt werden, wie sehr die eigenen Systeme von Schwachstellen betroffen sind.

W1.5 Wie Sie sich gegen diese Sicherheitsschwachstellen schützen können

Für die meisten Systeme

Installieren Sie die relevanten Patches für das HTTP Service und für das Betriebssystem und jede Applikation, die auf dem System installiert ist. Nachdem die Patches aktuell sind, halten Sie das System auch aktuell.

Installieren Sie Host-basierend Antivirenprogramme und Intrusion Detection Software. Stellen Sie sicher, dass beide aktuell sind und überprüfen Sie die Logdateien regelmäßig.

Schalten Sie Script Interpreter, die nicht verwendet werden ab und entfernen Sie die dazugehörigen Binaries. Z.B. Perl, Perlscript, Vbscript, Jscript, Java und PHP.

Schalten Sie Logging ein, wenn es diese Option gibt und überprüfen Sie die Logdateien regelmäßig, am besten mit einem automatisierten Prozess, der die Vorfälle zusammen fasst und Ausnahmen und suspekte Vorfälle meldet.

Verwenden Sie ein Syslog ähnliches System um Betriebssystem- und HTTPd-Logs sicher auf einem anderen System zu speichern.

Entfernen Sie oder begrenzen Sie den Zugang zu Systemtools, die von Angreifern gern verwendet werden um das System zu kompromittieren oder um weitere Systeme anzugreifen. Z.B. tftp(.exe), ftp(.exe), CMD.exe, bash, net.exe, remote.exe und telnet(.exe).

Limitieren Sie die Applikationen, die auf dem Host laufen auf HTTP Service/Daemon und unterstützende Services.

Wenn möglich, lassen Sie keine Domains oder andere Authentifizierungssysteme auf diesem Host laufen.

Sein Sie sich bewusst über und minimieren Sie jeden Vektor in das innere Netzwerk, der durch den öffentlichen Webserver passiert. Z.B. NetBIOS Shares, Trust Beziehungen und Datenbankinteraktionen.

Verwenden Sie unterschiedliche Account Namenskonventionen und einzigartige Passwörter auf öffentlich zugänglichen Systemen im Vergleich zu internen Systemen.

a. IIS

Sicherheitspatches nach der IIS Installation zu installieren, ist notwendig, aber nicht genug. Nachdem neue Sicherheitsschwachstellen erkannt werden, müssen die Systeme entsprechend aktualisiert werden. Windows Update und Automatischer Update sind Möglichkeiten für Einzelinstallationen. [HFNetChk](http://www.microsoft.com/technet/security/tools/hfnetchk.asp), der Netzwerk Sicherheits-Hotfix-Checker ermöglicht dem Administrator, lokale und Remote Systeme zu überprüfen und festzustellen, welche Hotfixes installiert sind und welche nicht. Das Programm funktioniert mit Windows NT4, Windows 2000 und Windows XP. Die aktuelle Version kann von der Microsoft Website <http://www.microsoft.com/technet/security/tools/hfnetchk.asp> heruntergeladen werden.

Zusätzlich kann ein sehr hilfreicher Artikel [Securing a Windows 2000 IIS Web Server – Lessons Learned](#) von Harpal im SANS Reading Room gefunden werden.

Verwenden von IIS Lockdown Wizard um die Installation zu härten

Microsoft hat ein einfaches Werkzeug veröffentlicht, mit dem die IIS Installation sicher gemacht werden kann, den IIS Lockdown Wizard. Die aktuelle Version kann von der Microsoft Webseite <http://www.microsoft.com/technet/security/tools/locktool.asp> heruntergeladen werden.

Wenn Sie den Lockdown Wizard im "custom" oder "expert" Modus ausführen können die folgenden empfohlenen Änderungen der IIS Installation durchgeführt werden:

- WebDAV abschalten (außer die Umgebung benötigt es unbedingt für Contentveröffentlichung).
- Alle nicht benötigten ISAPI Extensions entfernen (inklusive .htr, .idq, .ism und .printer im speziellen).
- Applikationsbeispiele entfernen.
- Verboten Sie dem Webserver, Befehle auszuführen, die üblicherweise für Angriffe verwendet werden (z.B. cmd.exe und tftp.exe).

Der SANS Reading Room enthält einen Artikel [Using Microsoft's IISlockdown tool to protect your IIS Web Server](#) von Jeff Wichman, in dem speziell das IIS Lockdowntool beschrieben wird.

Verwenden Sie URLScan um HTTP Requests zu filtern

Viele IIS Angriffe inklusive Code Blue und Code Red verwenden speziell verformte HTTP Requests in Directory traversal oder Buffer Overflow Attacken. Der URLScan Filter kann so konfiguriert werden, dass solche Anfragen abgelehnt werden, bevor der Server sie bearbeitet. Die letztgültige Version wurde in den Lockdown Wizard integriert, kann aber separat von der Microsoft Webseite <http://www.microsoft.com/technet/security/tools/urlscan.mspx> heruntergeladen werden.

b. Apache

Die Frage der Zugriffskontrolle, Restriktion bei IP und das Apache Sicherheitsmodul sind mit vielen anderen Topics auf der [Apache Tutorials](#) Seite zu finden.

Zusätzlich kann der sehr nützliche Artikel [Securing Apache: Step-by-Step](#) von Artur Maj im SANS Reading Room gefunden werden, der sehr detailliert beschreibt, wie der Apache Server sicher gemacht werden kann.

c. iPlanet/Sun One

Im SANS Reading Room gibt es auch den Artikel von Edmundo Farinas [Security Considerations for the iPlanet Enterprise Web Server on Solaris](#) der über die Sicherheit von iPlanet schreibt.

Zusätzlich hat Sun den Artikel [Sun ONE Application Server Security Goals](#) mit detaillierten Informationen veröffentlicht, der beschreibt, welche Schritte notwendig sind um den iPlanet Server sicher zu machen.

d. Add-Ons

Wenn Produkte von Drittfirmen wie ColdFusion, Perl/IIIS, oder PHP verwendet werden prüfen Sie auf den Seiten der Drittfirmen ob Patches verfügbar sind und ob es Konfigurationstipps gibt. Microsoft inkludiert natürlich keine Patches für Produkte von Drittfirmen in den Windows Updates und relevanten Updateservices.

Für Informationen, wie ColdFusion sicher gemacht werden kann lesen Sie den Artikel [Web Application Security, with a Focus on ColdFusion](#) von Joseph Higgins im SANS Reading Room.

Auch im SANS Reading Room ist der Artikel [Securing PHP: Step-by-step](#) von Artur Maj, der den Prozess beschreibt, wie PHP Applikationen sicher geschrieben werden können.

Eine zusätzliche Informationsquelle ist das [PHP Manual, Chapter 16. Security](#), welches PHP Sicherheit im Detail beschreibt.

e. Andere Services

Obwohl die grundlegenden Schritte, wie die meisten Webserver sicher gemacht werden können oben beschrieben sind, hat jeder Webserver üblicherweise eine eigene Anzahl von Updates und Patches, Konfigurationen und Logging Features des jeweiligen Herstellers.

Lesen Sie die Dokumentation und die Informationen auf der Webseite des Herstellers und stellen Sie sicher, dass Sie sich beim Hersteller für das Informationsservice und den Newsletter eingetragen haben. Das wird Ihnen helfen, über neue Sicherheitslücken und Patches rasch und effizient informiert zu werden.

[zum Anfang](#) ^

W2.1 Beschreibung

Das Windows Workstation Service ist dafür verantwortlich, Useranfragen zu bearbeiten um auf Ressourcen wie Dateien und Drucker zugreifen zu können. Das Service stellt fest, ob sich die Ressource lokal oder auf einen Netzwerkshare befindet und leitet die Anfrage dementsprechend weiter.

Die Netzwerkmanagementfunktion die von diesem Service verwendet wird kann über die folgenden Mechanismen abgerufen werden.

- DCE/RPC Aufrufe über das SMB Protokoll nachdem eine Verbindung zu dem Service mit `\\pipe\wkssvc` named Pipe hergestellt wurde.
- DCE/RPC Aufrufe direkt über einen UDP Port (> 1024)
- DCE/RPC Aufrufe direkt über einen TCP Port (> 1024)

Das Service bindet sich an den ersten verfügbaren TCP oder UDP Port über 1024.

Das Workstation Service beinhaltet einen Stack basierenden Buffer Overflow, der durch einen speziell geschriebenen DCE/RPC Aufruf ausgelöst werden kann. Das Problem entsteht dadurch, dass Parameter an die Logging Funktion weiter geleitet werden ohne überprüft zu werden. Dieser Overflow kann von einem nicht autorisierten Remoteangreifer ausgenutzt werden um beliebigen Code auf dem anfälligen System mit SYSTEM Rechten auszuführen. Der Angreifer kann die totale Kontrolle über das kompromittierte System erlangen. Der Code der diesen Fehler ausnutzt wurde im Internet veröffentlicht und wurde in einigen Varianten des Phatbot/Gaobot Wurms verwendet, der weltweit Millionen von Computern infizierte.

W2.2 Betroffene Betriebssysteme

Windows 2000 SP2, SP3 und SP4

Windows XP

Windows XP 64 Bit Version

W2.3 CVE/CAN Einträge

[CAN-2003-0812](#)

W2.4 Wie Sie herausfinden, ob Sie betroffen sind

Systeme mit dem Betriebssystem Windows 2000 ohne dem Patch MS03-049 und Windows XP ohne dem Patch MS03-043 sind betroffen.

Überprüfen Sie die folgenden Registrierungseinträge:

KB828035: Unter HKLM\Software\Microsoft\Updates\Windows XP (Windows XP)

KB828749: Unter HKLM\Software\Microsoft\Updates\Windows 2000 (Windows 2000)

Wenn diese Registrierungseinträge nicht vorhanden sind ist das Windowssystem betroffen.

Alternativ dazu kann ein Netzwerkscanner wie der Microsoft Baseline Analyzer (MBSA) verwendet werden um zu überprüfen ob die Patches installiert sind. MBSA kann von der Webseite <http://www.microsoft.com/technet/security/tools/mbsahome.msp> heruntergeladen werden.

W2.5 Wie Sie sich dagegen schützen können

Sicherstellen, dass Windows Systeme die letzten Sicherheitspatches installiert haben. Stellen Sie sicher dass Windows 2000 Systeme den Patch MS03-049 und Windows XP Systeme den Patch MS03-043 Patch installiert haben.

Blockieren Sie die Ports 139/tcp und 445/tcp am Netzwerkperimeter. Dadurch wird eine Remote Overflow-Attacke via SMB verhindert.

Öffnen Sie nur die notwendigen TCP Ports über 1024 am Netzwerkperimeter. Dadurch wird

eine Remote Overflow-Attacke via DCE/RPC Aufrufe verhindert. Beachten Sie das es schwer ist UDP Ports über 1024 auf der Firewall zu blockieren da diese als Ephemeral-Ports verwendet werden.

Verwenden Sie die in Windows 2000 und Windows XP verfügbaren TCP/IP Filter oder die Internet Connection Firewall in Windows XP Systemen um Zugriff auf die betroffenen Ports zu blockieren.

Für Applikationen von Drittfirmen die auf angepassten Windows 2000/XP Plattformen laufen sollten Sie sicher stellen, dass die entsprechenden Patches der Hersteller installiert sind. Z.B. hat Cisco einen Artikel veröffentlicht, der beschreibt, dass eine Anzahl von Cisco Produkten diesen Overflow Fehler haben. Cisco hat die entsprechenden Patches zur Verfügung gestellt.

Wenn das System Stand-Alone betrieben wird, d.h. nicht in einer Windows Netzwerkumgebung, kann das Workstation Service ohne Konsequenzen abgeschaltet werden.

Zusätzliche Informationen:

Microsoft Advisory

<http://www.microsoft.com/technet/security/bulletin/MS03-049.msp>

eEye Advisory

<http://www.eeye.com/html/Research/Advisories/AD20031111.html>

CERT Advisories

<http://www.cert.org/advisories/CA-2003-28.html>

<http://www.kb.cert.org/vuls/id/567620>

CORE Security Advisory

<http://archives.neohapsis.com/archives/vulnwatch/2003-q4/0066.html>

Cisco Advisory

<http://www.cisco.com/warp/public/707/cisco-sa-20040129-ms03-049.shtml>

Gaobot Worm

<http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.gen.html>

[zum Anfang ^](#)

W3 Windows Remote Access Service

W3.1 Beschreibung

Die Windows Betriebssysteme unterstützen eine Anzahl von unterschiedlichen Netzwerkmöglichkeiten und -technologien. Es gibt Support für die meisten Industriestandard-Netzwerkprotokolle und eingebaute Funktionalität für Microsoft spezifische Netzwerkmethoden und Techniken. Nicht nur diese Microsoft spezifischen Netzwerktechnologien enthalten bekannter Weise Sicherheitsprobleme, sondern auch schlecht konfigurierte Dinge wie NETBIOS, Netzwerk Shares, anonyme Logon NULL Sessions, entfernter Registrierungszugang und Remote Procedure Calls können zu Sicherheitsproblemen führen. Diese Dinge stellen den Großteil der bekannten Sicherheitsschwachstellen auf Netzwerkebene in Windows Betriebssystemen dar und werden im folgenden Text beschrieben.

NETBIOS -- Ungeschützte Windows Netzwerk Shares Microsoft Windows stellt

Computern die Möglichkeit zur Verfügung, Dateien und Verzeichnisse über das Netzwerk für andere freizugeben. Der Mechanismus dieser Möglichkeit ist das Server Message Block (SMB) Protokoll oder das Common Internet Dateien System (CIFS). Diese Protokolle erlauben einen Computer Dateien auf entfernten Systemen so zu manipulieren, als wären sie auf dem lokalen Computer. Obwohl dies eine leistungsfähige und nützliche Eigenschaft von Windows darstellt, kann unsachgemäße Konfiguration von Netzwerkfreigaben kritische Dateien offen legen. Es kann auch böartigen Angreifern oder Programmen ermöglicht werden, das System komplett zu kontrollieren. Einer der Wege, über die sich der I-Worm.Klez.a-h ([Klez Familie](#)) Wurm, der Sircam Virus ([siehe CERT Advisory 2001-22](#)) und der Nimda Wurm ([siehe CERT Advisory 2001-26](#)) rasch verbreitet haben war über ungeschützte Netzwerkfreigaben, auf denen Kopien abgelegt wurden. Viele Computerbesitzer öffnen aus Unwissenheit Hackern ihre Computersysteme, in dem sie versuchen die Konvenienz für die Mitarbeiter zu vergrößern indem sie Netzwerkshares mit Schreib- und Leserechten freigeben. Wenn aber Netzwerkshares sorgfältig konfiguriert wird kann das Risiko einer Kompromittierung gering gehalten werden.

Anonymous Logon --Eine NULL Session ist eine Session ohne Berechtigungsnachweis (z.B. kein Username und kein Kennwort). NULL Sessions können dazu verwendet werden, um Userinformationen, Gruppen, Shares und Kennwortrichtlinien auszulesen. Microsoft Windows NT Services, die als der lokale Systemaccount ausgeführt werden und die am lokalen Computer laufen kommunizieren mit anderen Services über das Netzwerk indem sie NULL Sessions verwenden. Windows 2000 und spätere Services die im lokalen Systemaccount ausgeführt werden und auf dem lokalen System laufen verwenden den lokalen Computeraccount um mit anderen Services über das Netzwerk zu kommunizieren. Active Directory (native mode) akzeptiert keine NULL Session Anfragen. Im gemischten Modus erlaubt das Active Directory NULL Session Anfragen aus Kompatibilitätsgründen (vor Windows 2000) und setzt sich dadurch der NULL Session Sicherheitsschwachstelle aus.

Remote Registry Access--Microsoft Windows 9x, Windows CE, Windows NT, Windows 2000, Windows 2003, Windows ME und Windows XP verwenden eine hierarchische Datenbank (Registrierung) um Software zu managen und um Gerätekonfigurationen und User Einstellungen zu verwalten. Falsche Rechtevergabe oder Sicherheitseinstellungen können zu entfernten Registrierungszugriffen führen. Angreifer können diese Besonderheit ausnutzen um das System zu kompromittieren oder um Dateitypen oder Rechte so zu verändern, dass böartiger Programmcode ausgeführt werden kann.

Remote Procedure Calls --Viele Microsoft Windows Versionen (Windows NT 4.0, 2000, XP und 2003) bieten einen Interprozess-Kommunikationsmechanismus an, der es ermöglicht, dass Programme die auf einem System laufen, auf anderen Systemen Programme ausführen können. Drei Schwachstellen wurden veröffentlicht, die es einem Angreifer ermöglichen, böartigen Code auf anfälligen Systemen mit lokalen Systemrechten auszuführen. Eine dieser Schwächen wurde von den Blaster/MSblast/LovSAN Wurm und vom Nachi/Welchia Wurm ausgenutzt. Es gibt auch andere Schwachstellen, die es einem Angreifer ermöglichen, Denial of Service Attacken gegen RPC Komponenten durchzuführen.

W3.2 Betroffene Betriebssysteme

Windows 95, Windows 98, Windows NT Workstation und Server, Windows 2000 Workstation und Server, Windows XP Home und Professional und Windows 2003 sind betroffen.

W3.3 CVE/CAN Einträge

NETBIOS

[CVE-2000-0979](#)

[CAN-1999-0518](#), [CAN-1999-0519](#), [CAN-1999-0621](#), [CAN-2000-1079](#)

Anonymous Logon

[CVE-2000-1200](#)

Remote Registry Access

[CVE-2000-0377](#), [CVE-2002-0049](#)

[CAN-1999-0562](#), [CAN-2001-0045](#), [CAN-2001-0046](#), [CAN-2001-0047](#), [CAN-2002-0642](#), [CAN-2002-0649](#), [CAN-2002-1117](#)

Remote Procedure Calls

[CAN-2002-1561](#), [CAN-2003-0003](#), [CAN-2003-0352](#), [CAN-2003-0528](#), [CAN-2003-0605](#), [CAN-2003-0715](#)

[CAN-1999-0518](#), [CAN-1999-0519](#), [CAN-1999-0621](#), [CAN-2000-1079](#)

W3.4 Wie Sie herausfinden, ob Sie betroffen sind

Wie Sie herausfinden, ob Ihre Systeme auf NETBIOS bezogene Schwachstellen anfällig sind

Eine Anzahl von Tools sind verfügbar, die es ermöglicht festzustellen, ob Systeme auf NETBIOS bezogene Schwachstellen anfällig sind.

NbtScan - NetBIOS Name Network entdeckt ob NETBIOS File-Sharing Services auf Zielsystemen verfügbar ist. NbtScan ist erhältlich auf:

<http://www.inetcat.org/software/nbtscan.html>.

NLtest – ein extrem leistungsfähiges Tool, inkludiert in [Windows 2000 and 2003 Support Tools](#) (kann auf der Produkt CD gefunden werden) und [Windows NT4 Resource Kit](#). NLtest kann eine Fülle von Informationen über potentielle Konfigurationsschwachstellen erkennen.

Windows 95/98/ME Anwender können Legion v2.11 verwenden, die letztgültige Version des Dateifreigabescanners von Rhino9, um nach Windows Netzwerkshares zu suchen.

Windows 2000 Administratoren können Security Fridays Share Password Checker (SPC) verwenden, um Windows 95/98/ME Systeme mit freigegebenen Shares nach Share Level Password Schwachstellen zu durchsuchen. Durch diese Schwachstelle

kann ein Angreifer das Share Level Password auslesen.

Für Windows NT (SP4), Windows 2000, Windows XP und Windows 2003 kann der [Microsoft Baseline Security Analyser](#) verwendet werden. Dieser überprüft Systeme auf SMB Sicherheitsschwachstellen und meldet die betroffenen Systeme. Der Test kann lokale und entfernte Systeme überprüfen.

Windows NT, Windows 2000, Windows XP und Windows 2003 Anwender können einfach *net share* im Command-Prompt eintippen um die freigegebenen Ressourcen anzuzeigen. Für zusätzliche Information über den "net share" Befehl tippen Sie *net share /?*.

Wichtiger Hinweis: Dieser Artikel enthält Information über das Verändern von freigegebenen Ressourcen. Bevor freigegebene Ressourcen verändert werden, muss sicher gestellt sein, wie diese Freigaben wieder aktiviert werden können falls Probleme auftreten. Es ist empfohlen, dass Änderungen ausgiebig getestet werden, bevor sie im Produktionsnetzwerk umgesetzt werden. Für zusätzliche Informationen über freigegebene Ressourcen, lesen Sie folgende Artikel in der Microsoft Knowledge Base:

[125996 - Saving and Restoring Existing Windows Shares](#)

[308419 - HOW TO Set, View, Change, or Remove Special Permissions for Files and Folders in Windows XP](#)

[307874 - HOW TO Disable Simplified Sharing and Password-Protect a Shared Folder in Windows XP](#)

[174273 - How to Copy Files and Maintain NTFS and Share Permissions](#)

Die standardmäßigen Rechte auf neuen Shares sind:

Windows NT, Windows 2000, and Windows XP (vor Service Pack 1)

- Jeder - Vollzugriff

Windows XP SP1

- Jeder - Lesen

Windows XP hat standardmäßig das Verzeichnis "SharedDocs" freigegeben, dieses Verzeichnis ist unter "C:\Dokumente und Einstellungen\All Users\Dokumente".

- Jeder - Vollzugriff

Die meisten kommerziellen Scanner erkennen freigegebene Ressourcen. Ein schneller, kostenloser und sicherer Test um zu überprüfen, ob Systeme SMB Freigaben verwenden und ob diese Systeme Schwachstellen haben (für Windows

Betriebssysteme) ist auf der Webseite von [Gibson Research Corporation](#) verfügbar. Folgen Sie dem Link *ShieldsUP* um eine Echtzeitauswertung zu erhalten. Bitte beachten Sie, dass, wenn Sie den Test von einem System durchführen, dass hinter einem Gerät ist das SMB blockiert, *ShieldsUP* meldet, das System ist nicht anfällig, obwohl das System vielleicht doch anfällig ist. Das gilt auch für DSL Anwender, bei denen die ISP SMB am DSL Netzwerk blockiert. Obwohl *ShieldsUP* meldet, dass Ihr System nicht anfällig ist, kann das System noch immer von anderen DSL Anwendern ausgenutzt werden.

Automatische Tools die Freigabeschwachstellen erkennen:

- [Nessus](#)-- ein freiverfügbares, leistungsstarkes und aktuelles Programm, dass einfach in der Handhabung ist
- [Winfingerprint](#) von vacuum - Win32 Host/Network Enumeration Scanner

Wie Sie herausfinden, ob Ihre Systeme auf Anonymous Logon bezogene Schwachstellen anfällig sind.

Versuchen Sie eine NULL Session zu Ihrem Computer herzustellen. Hier die Schritte:

Start - Ausführen - cmd

```
C:\>net use \\ipaddress\ipc$ "" /user:""
```

Die vorangehende Syntax versucht eine Verbindung über eine verborgene Interprozesskommunikation zu „Share“ (IPC\$) zu öffnen. Auf dem System mit der angegebenen IP Adresse wird mit dem Anonymous User (*/user: ""*) eine Session ohne Kennwort gestartet.

Wenn Sie System Error 5 als Meldung bekommen, wurde der Zugriff verweigert. Das System ist nicht anfällig.

Wenn Sie die Meldung "Der Befehl wurde erfolgreich ausgeführt." bekommen ist das System anfällig.

Die vorhin erwähnten Tools - Nessus und Winfingerprint können ebenfalls NULL Session Sicherheitsschwächen erkennen.

Wie Sie herausfinden, ob Ihre Systeme auf Remote Registry Access bezogene Schwachstellen anfällig sind.

Der „NT Resource Kit“ (verfügbar von Microsoft) enthält das Programm *Regdump.exe*. Dieses Programm testet passiv die Remote Registrierungszugangsrechte von einem Windows NT System gegen andere Windows NT / Windows 2000 oder Windows XP Systeme im internen Netzwerk oder im Internet.

Es gibt auch eine Anzahl von Shell Scripts, die diese Registrierungszugangsrechte und andere Sicherheitsprobleme überprüfen. Die Scripts sind unter <http://www.afentis.com/top20> verfügbar.

Wie Sie herausfinden, ob Ihre Systeme auf Remote Procedure Call bezogene Schwachstellen anfällig sind.

Microsoft stellt ein Tools zur Verfügung, das Systeme auf Hotfix-, Konfigurations- und Patchschwachstelle überprüft. Das ist wahrscheinlich auch die beste Möglichkeit, die Systeme auf die RPC-Anfälligkeit hin zu überprüfen. Das Tool heißt Microsoft Baseline Security Analyzer (MBSA) und kann von <http://www.microsoft.com/technet/security/tools/mbsahome.msp> heruntergeladen werden. Es gibt auch ein Stand-Alone Testprogramm, das überprüft, ob die Sicherheitspatches für CAN-2003-0352, CAN-2003-0528, CAN-2003-0605 und CAN-2003-0715 installiert wurden. Dieses Programm ist unter <http://support.microsoft.com/?kbid=827363> verfügbar. Es ist aber empfohlen, den Microsoft Baseline Security Analyzer zu verwenden, da damit eine umfassendere Überprüfung der Systeme möglich ist. Für Heimanwender und für Anwender mit nur einigen PCs ist es einfacher, die Windows Update Site unter <http://windowsupdate.microsoft.com/> zu besuchen und die Computer einzeln überprüfen zu lassen, welche Updates verfügbar sind.

W3.5 Wie Sie sich dagegen schützen können

Microsoft adressiert Sicherheitsschwachstellen für Betriebssysteme und Applikationen in Service Packs und Sicherheitshotfixes. Es ist extrem wichtig, immer die aktuellen Service Packs installiert zu haben.

Zum Beispiel infiziert der Sasserwurm und seine Abarten (eine Sicherheitsschwachstelle in LSASS wird dabei ausgenutzt) eine Vielzahl von ungepatchten Computern weltweit während Systeme, die den Hotfix MS04-011 installiert haben nicht für diese extrem gefährliche Sicherheitsschwachstelle anfällig sind. Microsoft hat den Hotfix MS04-011 einige Wochen vor dem Erscheinen von Sasser zur Verfügung gestellt.

Hinweis: Windows 95 und Windows NT4 Workstation werden nicht mehr von Microsoft unterstützt. Der Support für Windows NT4 Server endet am 31. Dezember 2004.

Um mehr über den Lifecycle von unterstützten Betriebssystemen zu erfahren lesen Sie [Product Lifecycle Dates - Windows Product Family](#).

Um relevante Sicherheitshotfixes zu finden verwenden Sie:

Windows Update Service (*Start – Windows Update*). Es werden alle notwendigen Sicherheitspatches gefunden und installiert, nachdem der User die notwendigen Hotfixes selektiert (erlaubt) die installiert werden sollen.

Windows Security Bulletin Search Online Service ist unter:

<http://www.microsoft.com/technet/security/current.aspx>

Die aktuellen Service Packs und Hotfixes adressieren viele Softwaredesignprobleme (wie Buffer Overflow, Code Design Fehler, etc.). Es gibt jedoch eine Anzahl von gefährlichen Features im Windows Betriebssystem, die gut dokumentiert sind und auch ihre Berechtigung haben, die aber ausgeschaltet oder sicher gemacht werden können um die Systeme zu härten.

Wie schützen Sie Ihre Systeme vor NETBIOS bezogene Angriffe?

Es können verschiedene Schritte unternommen werden, um das Risiko zu verringern, dass die Schwachstellen ausgenutzt werden:

Service Alerter und Messenger ausschalten (sind bei Windows 2003 standardmäßig ausgeschaltet, werden aber bei Windows 2000/XP/NT4 automatisch gestartet).

Um diese Services auszuschalten:

Selektieren *Start – Einstellungen – Systemsteuerung – Verwaltung - Dienste*;

- Selektieren Dienst *Warndienst* – doppel-klicken – stellen Sie *Starttyp* auf *Disabled* – klicken Sie *Übernehmen* – klicken Sie den *Beenden* Knopf – und *OK*.
- Selektieren Sie *Nachrichtendienst* – doppel-klicken - stellen Sie *Starttyp* auf *Disabled* – klicken Sie *Übernehmen* – klicken Sie den *Beenden* Knopf – und *OK*.

Freigaben immer ausschalten, wenn nicht benötigt. Wenn keine Datei- und Druckerfreigaben benötigen werden (typischer Fall für Geschäftslösungen und Heimarbeitsplätze) kann der Dienst Server für Windows NT4/2000/2003/XP disabled werden. Um diesen Dienst auszuschalten sind folgende Schritte notwendig:

Selektieren *Start – Einstellungen – Systemsteuerung – Verwaltung - Dienste*;

Selektieren Dienst *Server* – doppel-klicken – stellen Sie *Starttyp* auf *Disabled* – klicken Sie *Übernehmen* – klicken Sie den *Beenden* Knopf – und *OK*.

Wenn der Server Dienst nicht benötigt wird, können folgende Schritte durchgeführt werden um Windows NT4/2000/XP/2003 sicherer zu machen:

Listen Sie alle versteckten Shares auf (C\$, D\$, E\$,...) mit dem Befehl:
Net share

Notieren Sie alle Shares

Löschen Sie die standardmäßigen versteckten Shares mit dem Befehl:
Net share C\$ /delete

In den meisten Fällen können alle alphabetischen Shares (C\$, D\$,...) und das ADMIN\$ gelöscht werden. Es wird nicht empfohlen, das IPC\$ Share zu löschen.

Um die Löschung der default Shares permanent durchzuführen (werden automatisch beim nächsten Neustart gestartet) muss in der Registrierung folgende Änderung durchgeführt werden:

Öffnen des Registrierungs-Editors;

Navigieren zu dem Registrierungsschlüssel:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

Neuen Wert unter diesem Schlüssel kreieren:

Value name: *AutoShareWks*

Value type: *DWord*

Value: *00000000*

Neuen Wert unter diesem Schlüssel kreieren:

Value name: *AutoShareServer*
Value type: *Dword*
Value: *00000000*

Überprüfen Sie auch die existierenden nicht standardmäßigen Shares auf den Systemen. Das kann folgendermaßen durchgeführt werden:

Grafische Oberfläche (Arbeitsplatz – rechte Maustaste – Verwalten – Freigegebene Ordner – Freigaben. Selektieren Sie die Shares die Sie ausschalten wollen – rechte Maustaste – Freigabe aufheben.

Von der Command Line (vom Prompt oder als Teil eines Scripts):

Um Shares aufzulisten:

Net Share

Notieren Sie alle Shares

Löschen Sie nicht benötigte Shares

Net Share Sharename /delete

Dadurch werden alle nicht standardmäßigen Shares permanent gelöscht. Um standardmäßige Shares permanent zu löschen lesen Sie den vorigen Absatz.

Bei Windows 95/98/ME Systemen, die Teil einer NT Domäne sind wird empfohlen, die Zugriffskontrolle der Dateifreigabe einzurichten.

Die Freigabe mit Systemen im Internet ist zu verbieten. Stellen Sie sicher, dass alle Systeme, die ein Interface zum Internet haben, Freigaben deaktiviert haben (Eigenschaften Netzwerkumgebung). Das gemeinsame Benutzen von Dateien sollte über das Internet nur über SCP, HTTP oder FTP erfolgen.

Erlauben Sie keine Freigaben ohne Authentifizierung. Wenn Freigaben erforderlich sind, sollen Zugriffe immer authentifiziert erfolgen. Konfigurieren Sie die Freigaben, dass ein Kennwort notwendig ist, um auf diese zugreifen zu können.

Die Freigaben sollten auf ein absolutes Minimum an Verzeichnissen und Dateien beschränkt werden. Wenn möglich sollte die Freigabe nur ein Verzeichnis und mögliche Unterverzeichnisse enthalten.

Die Rechte für diese Freigaben minimieren. Die Rechte für die Freigaben sollten sehr restriktiv vergeben werden. Schreibrechte sollten nur wenn absolut notwendig vergeben werden.

Zusätzliche Sicherheit kann erlangt werden, in dem Freigaben nur für bestimmte IP Adressen erlaubt wird. DNS Namen können verfälscht werden.

Wie schützen Sie Ihre Systeme vor Anonymous Logon bezogene Angriffe?

WICHTIGER Hinweis: Dieser Artikel enthält Informationen über Änderungen in der Registrierung. Bevor die Registrierung geändert wird, sollte ein Backup der Registry durchgeführt werden und verstanden werden, wie ein Restore durchzuführen ist, falls Probleme auftreten. Diese Änderungen sollten ausgiebig getestet werden, bevor sie in Produktionssystemen verwendet werden. Informationen, wie ein Backup, Restore und Edit der Registrierung durchgeführt

werden, finden Sie in folgenden Microsoft Knowledge Base Artikeln:

[256986 - Description of the Microsoft Windows Registry](#)

[323170 - HOW TO Backup, Edit, and Restore the Registry in Windows NT 4.0](#)

[322755 - HOW TO Backup, Edit, and Restore the Registry in Windows 2000](#)

[322756 - HOW TO Backup, Edit, and Restore the Registry in Windows XP Windows Server 2003](#)

Windows NT Domain Controller benötigen NULL Sessions zur Kommunikation. Wenn Windows NT Domänen oder Windows 2000/2003 Active Directory im gemischten Modus verwendet werden, kann der Registrierungsschlüssel RestrictAnonymous nicht auf 1 gesetzt werden um dadurch die Schwachstelle auszuschalten. Sie können aber die Information, die ein Angreifer erlangen kann, minimieren. Zum Beispiel umgeht GetAcct (von Security Friday) RestrictAnonymous=1 und verwendet die SID und UserID. Die ideale Lösung dafür wäre, wenn ein natives Windows 2000/2003 Active Directory verwendet wird, den Wert in der Registrierung für RestrictAnonymous auf 2 zu setzen.

Für Informationen über NULL Sessions lesen Sie die folgenden Artikel in der Microsoft Knowledge Base:

[143474 - Restricting Information Available to Anonymous Logon Users in Windows NT](#)

[246261 - How to Use the RestrictAnonymous Registry Value in Windows 2000](#)

Zur Fehlerbehebung der Einstellung des Wertes von RestrictAnonymous lesen Sie folgenden Artikel:

[296405 - The RestrictAnonymous Registry Value May Break the Trust to a Windows 2000 Domain](#)

Wie schützen Sie Ihre Systeme vor Remote Registry Access bezogene Angriffe?

Um diese Gefahr zu minimieren müssen Zugriffe auf die Registrierung eingeschränkt und die Rechte für kritische Einstellungen in der Registrierung überprüft werden. Für Windows NT 4.0 Systeme sollte das Service Pack 4 (SP4) installiert sein, bevor die Registrierung verändert wird.

WICHTIGER Hinweis: Dieser Artikel enthält Informationen über Änderungen in der Registrierung. Bevor die Registrierung geändert wird, sollte ein Backup der Registry durchgeführt werden und verstanden werden, wie ein Restore durchzuführen ist, falls Probleme auftreten. Diese Änderungen sollten ausgiebig getestet werden, bevor sie in Produktionssystemen verwendet werden. Informationen, wie ein Backup, Restore und Edit der Registrierung durchgeführt werden, finden Sie in folgenden Microsoft Knowledge Base Artikeln:

[256986 - Description of the Microsoft Windows Registry](#)
[323170 - HOW TO Backup, Edit, and Restore the Registry in Windows NT 4.0](#)
[322755 - HOW TO Backup, Edit, and Restore the Registry in Windows 2000](#)
[322756 - HOW TO Backup, Edit, and Restore the Registry in Windows XP Windows Server 2003](#)

Netzwerkzugriffe einschränken. Um den Netzwerkzugriff auf die Registrierung einzuschränken, sind folgende Schritte durchzuführen und folgender Registrierungsschlüssel zu erstellen:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
- Description: REG_SZ
- Value: Registry Server

Die Sicherheitseinstellung auf diesem Schlüssel definiert User oder Gruppen, die Zugriff auf die Registrierung über das Netzwerk erhalten. Eine standardmäßige Installation erstellt diesen Schlüssel und vergibt Vollzugriff für den Administrator und Administratorengruppen (in Windows 2000 auch Backup Operator).

Eine Änderung in der Registrierung wird erst durch einen Neustart des Systems effektiv. Um einen Schlüssel zu erstellen, der den Zugriff auf die Registrierung einschränkt sind folgende Schritte durchzuführen:

1. Starten Sie den Registrierungs-Editor ("regedt32.exe" oder "regedit.exe") und selektieren Sie den Schlüssel:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
2. Unter Bearbeiten klicken Sie auf Schlüssel hinzufügen
3. Geben Sie folgendes ein: Key Name: ◦SecurePipeServers ◦Class: REG_SZ
4. Selektieren Sie den neu erstellten Schlüssel:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers
5. Unter Bearbeiten klicken Sie auf Wert hinzufügen
6. Geben Sie die folgenden Werte ein: ◦Key Name: winreg ◦Class: REG_SZ
7. Selektieren Sie den neu erstellten Unterschlüssel:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
8. Unter Bearbeiten klicken Sie auf Wert hinzufügen
9. Geben Sie folgende Werte ein: ◦Value Name: Description ◦Data Type: REG_SZ ◦String: Registry Server
10. Selektieren Sie den Unterschlüssel:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
11. Klicken Sie auf winreg, dann unter Sicherheit - Berechtigungen geben Sie User oder Gruppen ein, die Sie berechtigen wollen.
12. Schließen Sie den Registrierungs-Editor und starten Sie Windows neu.
13. Wenn zu einem späteren Zeitpunkt die Liste der User oder Gruppen geändert wird, sind die Schritte ab Punkt 10. durchzuführen.

Schränken Sie den autorisierten Zugang ein. Die Durchsetzung von strikten Rechten auf die Registrierung kann sich nachteilig auf abhängige Dienste

auswirken, wie der Directory Replicator und das Netzwerk Print Spooler Service.

Es ist deshalb möglich, eine gewisse Feinabstimmung durchzuführen, in dem Accountnamen zu "winreg" hinzugefügt werden unter denen bestimmte Dienste ausgeführt werden. Es besteht auch die Möglichkeit, die Einschränkungen für bestimmte Schlüssel zu umgehen, in dem Sie zu den AllowedPath Schlüssel im System oder User Wert hinzugefügt werden:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths
Value: Machine
Value Type: REG_MULTI_SZ - Multi string
Default Data: System\CurrentControlSet\Control\ProductOptionsSystem\CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\

Services\EventlogSoftware\Microsoft\WindowsNT\CurrentVersionSystem\CurrentControlSet\Services\Replicator
Valid Range: (Ein gültiger Pfad zu einer Stelle in der Registrierung)
Description: Erlaubt Maschinenzugriff auf bestimmte Stellen in der Registrierung, wenn keine ausdrücklichen Zugriffsbeschränkungen für diese Stellen bestehen.
Value: Users
Value Type: REG_MULTI_SZ - Multi string
Default Data: (none)
Valid Range: (Ein gültiger Pfad zu einer Stelle in der Registrierung)
Description:

In der Microsoft Windows 2000 und Windows XP Registrierung:

Value: Machine
Value Type: REG_MULTI_SZ - Multi string
Default Data: System\CurrentControlSet\Control\ProductOptionsSystem\CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\control\Server ApplicationSystem\CurrentControlSet\Services\Eventlog\Software\Microsoft\Windows NT\CurrentVersion
Value: Users (ist standardmässig nicht erstellt)

Üblicherweise besteht ein Zeitraum zwischen dem Bekannt werden einer Sicherheitsschwäche und der Veröffentlichung eines Patches zur Behebung dieser Schwäche. Mit anderen Worten, müssen Sie die Schwachstelle eine gewisse Zeit erlauben. Um das Risiko zu verringern, kann ein Unternehmen den Zugriff durch Firewall und Router einschränken. Eine zusätzliche Möglichkeit wäre, neue Regeln für IDS (Intrusion Detection System) Systeme wie z.B. [Snort](#) zu schreiben. Beispiele für dokumentierte Regeln für Snort gibt es hier.

Wie schützen Sie Ihre Systeme vor Remote Procedure Call bezogene Angriffe?

Der beste Weg Ihre Systeme zu schützen ist Aktualisieren. Installieren Sie die Patches, die der MBSA als fehlend erkannt hat, oder die durch Windows Update angezeigt werden. Siehe auch: Sind Ihre Systeme auf Remote Procedure Call bezogene Schwachstellen anfällig? Einige der RPC Funktionen können nicht eingeschränkt oder abgeschaltet werden können. Eine hervorragende Zusammenfassung kann unter <http://www.ntbugtraq.com/dcomrpc.asp> gefunden

werden.

Wichtiger Hinweis: Durch das Ausschalten oder Einschränken der RPC Funktionalität können eventuell wichtige Windows Dienste nicht mehr richtig funktionieren. Sie sollten diese Änderungen immer zuerst in einer Testumgebung testen.

Wenn Systeme nicht aktualisiert werden können, dann sollten die diversen Ports, die mit RPC in Verbindung stehen (TCP 135, 139, 445 und 593; UDP 135, 137, 138 und 445) an den Netzwerkgrenzen blockiert werden. Es ist natürlich immer "Best Practice" alle nicht verwendeten Services an den Netzwerkgrenzen zu blockieren.

Für zusätzliche Informationen:

[Microsoft Knowledge Base Article 153183. How to Restrict Access to NT Registry from a Remote Computer.](#)

Eine andere Quelle ist [Microsofts Hotfix & Security Bulletin Service](#).

[Welcome to the MSDN Library](#) (suchen Sie nach Securing Registry)

[Microsoft Knowledge Base Article 310426 : HOW TO: Use the Windows XP and Windows Server 2003 Registry Editor](#)

[Network Access: Remotely accessible registry paths and subpaths](#)

[Windows Server 2003 Security Guide](#)

[zum Anfang ^](#)

W4 Microsoft SQL Server (MSSQL)

W4.1 Beschreibung

Der Microsoft SQL Server enthält mehrere gravierende Schwachstellen, die Angreifern erlauben, sensible Informationen zu lesen, Datenbankinhalte zu verändern, SQL Server zu übernehmen und in einigen Konfigurationen, den kompletten Server zu übernehmen.

MSSQL Schwachstellen sind sehr gut publiziert und werden ständig für Angriffe ausgenutzt. Zwei MSSQL Würmer haben im Mai 2002 und im Jänner 2003 mehrere bekannte Schwachstellen im MSSQL Server ausgenutzt. Systeme, die von diesen Würmern befallen waren, generierten einen gewaltigen Netzwerkverkehr, da die Würmer andere anfällige SQL Server automatisch suchten. Zusätzliche Information zu diesen Würmern kann auf folgenden Webseiten gefunden werden:

SQLSnake/Spida Worm (Mai 2002)

- <http://isc.incidents.org/analysis.html?id=157>
- <http://www.eeye.com/html/Research/Advisories/AL20020522.html>
- http://www.cert.org/incident_notes/IN-2002-04.html

SQL-Slammer/SQL-Hell/Sapphire Wurm (Jänner 2003)

- <http://isc.incidents.org/analysis.html?id=180>

- <http://www.nextgenss.com/advisories/mssql-udp.txt>
- <http://www.eeye.com/html/Research/Flash/AL20030125.html>
- <http://www.cert.org/advisories/CA-2003-04.html>

Die Ports 1433 und 1434 (MSSQL Server und MSSQL Monitor Standardports) werden immer wieder vom [Internet Storm Center](#) als die am häufigsten attackierten Ports aufgeführt.

SQLSnake nutzt eine Sicherheitsschwäche mit den Administratoraccount SA aus, der standardmäßig kein Passwort hat. Für eine ordnungsgemäße Konfiguration ist es essenziell, dass alle Systemaccounts durch ein Kennwort geschützt sind, oder, wenn sie nicht verwendet werden, komplett abgeschaltet werden. Mehr Information über Einstellungen und Handhabung des SA Account Kennwörter können in der Microsoft Development Network Dokumentation unter [Changing the SQL Server Administrator Login](#) und unter [Verify and Change the System Administrator Password by Using MSDE](#) nachlesen. Der SA Account soll ein komplexes, schwer zu erratendes Kennwort haben, selbst wenn der Account nicht für SQL/MSDE Implementierungen verwendet wird.

Der SQL Slammer nutzte eine Buffer Overflow Schwachstelle im SQL Server Resolution Service aus. Dieser Buffer Overflow wirkt sich dann aus (und damit ist die Host Security gefährdet), wenn der Wurm speziell angefertigte Angriffspakete an gefährdete Zielsysteme (Zielport UDP 1434) schickt. Wenn SQL Dienste auf einem Computer laufen, der für diese Schwachstelle anfällig ist, und solche Pakete werden empfangen, ist eine Serverkompromittierung und damit auch eine Beeinträchtigung der Sicherheit die Folge. Der beste Schutz gegen diesen Wurm bedeutet sorgfältiges Aktualisieren des Systems, proaktive Systemkonfiguration und Filterung des Ports 1434/UDP in beiden Richtungen an den Netzwerkgateways.

Die Microsoft Server 2000 Desktop Engine (MSDE 2000) entspricht in etwa einem "SQL Server Lite". Viele Anwender wissen nicht, das MSDE auf ihren Systemen aktiviert ist und dadurch ein SQL Server auf den Computern läuft. MSDE wird installiert, wenn Sie eines der folgenden Produkte installiert haben:

SQL/MSDE Server 2000 (Developer, Standard und Enterprise Edition)

Visual Studio .NET (Architect, Developer und Professional Edition)

ASP.NET Web Matrix Tool

Office XP

Access 2002

Visual Fox Pro 7.0/8.0

Es gibt noch einige andere Softwarepakete, die MSDE verwenden. Eine aktuelle Liste können Sie unter <http://www.SQLsecurity.com/forum/applicationslistgridall.aspx> finden. Nachdem diese Softwarepakete MSDE als ihre Kerndatenbank Engine verwenden, gelten die gleichen Bedrohungen wie bei einem SQL/MSDE Server. MSDE 2000 kann so konfiguriert werden, dass auf eingehende Clientverbindungen auf verschiedene Arten gehört werden kann. Es kann konfiguriert werden, dass Clients Named Pipes über NetBIOS Session (Ports TCP 139 und 445) verwenden oder Sockets, wobei die Clients eine Verbindung auf Port 1433 verwenden, oder beides. Egal welche Variante gewählt wird, SQL Server und MSDE hören immer auf Port

1434/UDP. Dieser Port wird als Monitorport bezeichnet. Die Clients senden eine Anfrage an diesen Port, wie die Verbindung zum Server aufgebaut werden soll.

Die MSDE 2000 Engine retourniert Informationen über sich wenn ein einzelnes Byte Paket mit 0x02 auf dem UDP Port 1434 empfangen wird. Andere einzelne Byte Pakete führen zu einem Buffer Overflow ohne überhaupt authentifiziert worden zu sein. Zusätzlich erschwerend ist, dass der Angriff über UDP erfolgt. Egal ob MSDE 2000 im Sicherheitskontext eines Domainusers oder lokalen Anwenders ausgeführt wird, eine erfolgreiche Ausnutzung dieser Sicherheitsschwachstelle bedeutet eine totale Kompromittierung des angegriffenen Computers.

Der SQL Slammer nutzte einen bekannten Buffer Overflow aus, der durch "Best Practice", durch rechtzeitiges Aktualisieren der Systeme und richtige Konfiguration, verhindert werden hätte können. Mit einem Tool wie [Microsoft SQL Critical Update Kit](#) können lokale Systeme auf Schwachstellen und Angriffspunkte überprüft werden. Es können auch ganze Domänen und Netze auf Systeme mit Schwachstellen überprüft werden und automatisch Aktualisierungen durchgeführt werden.

Bitte lesen Sie auch die Reports und Analysen auf [incidents.org](#) bezüglich des SQL Slammer Wurmes. Diese spezielle Attacke am Morgen des 25. Jänner 2003 betraf das Internet Backbone für ein paar Stunden.

W4.2 Betroffene Betriebssysteme

Jedes Microsoft Windows System, das Microsoft SQL/MSDE Server 7.0, Microsoft SQL/MSDE Server 2000 oder Microsoft SQL/MSDE Server Desktop Engine 2000 installiert hat sowie alle Systeme, die MSDE getrennt verwenden.

W2.3 CVE/CAN Einträge

[CVE-1999-0999](#), [CVE-2000-0202](#), [CVE-2000-0402](#), [CVE-2000-0485](#), [CVE-2000-0603](#), [CVE-2001-0344](#), [CVE-2001-0879](#)

[CAN-2000-0199](#), [CAN-2000-1081](#), [CAN-2000-1082](#), [CAN-2000-1083](#), [CAN-2000-1084](#), [CAN-2000-1085](#), [CAN-2000-1086](#), [CAN-2000-1087](#), [CAN-2000-1088](#), [CAN-2000-1209](#), [CAN-2001-0509](#), [CAN-2001-0542](#), [CAN-2002-0056](#), [CAN-2002-0154](#), [CAN-2002-0186](#), [CAN-2002-0187](#), [CAN-2002-0224](#), [CAN-2002-0624](#), [CAN-2002-0641](#), [CAN-2002-0642](#), [CAN-2002-0643](#), [CAN-2002-0644](#), [CAN-2002-0645](#), [CAN-2002-0649](#), [CAN-2002-0650](#), [CAN-2002-0695](#), [CAN-2002-0721](#), [CAN-2002-0729](#), [CAN-2002-0859](#), [CAN-2002-0982](#), [CAN-2002-1123](#), [CAN-2002-1137](#), [CAN-2002-1138](#), [CAN-2002-1145](#), [CAN-2003-0118](#)

W4.4 Wie Sie herausfinden, ob Sie betroffen sind

Microsoft hat ein Set von Programmen unter

<http://www.microsoft.com/sql/downloads/securitytools.asp> zur Verfügung gestellt. Der SQL Critical Update Kit enthält wertvolle Tools wie SQL Scan, SQL Check und SQL Critical Update.

Chip Andrew von [sqlsecurity.com](#) hat das Programm SQLPingv2.2 veröffentlicht. Dieses sendet ein UDP Paket, das ein Byte lang ist und den Wert 0x02 hat, an ein System oder ein ganzes Subnetz, Zielport ist UDP 1434. SQL Server die auf diesem Port hören, antworten und senden Details wie Versionsnummer, Instanzen usw. SQLPingv2.2 ist ein Scan- und Erkennprogramm wie SQL Scan von Microsoft, die Systeme und die Netzwerksicherheit werden nicht bedroht. Zusätzliche SQL-Sicherheitsprogramme können auf der Website von Chip Andrews [SQL/MSDE Security Web Site](#) gefunden werden.

W4.5 Wie Sie sich dagegen schützen können

Zusammenfassung:

Das Monitor-service für SQL/MSDE auf UDP Port 1434 ausschalten.

Die letztgültigen Service Packs für Microsoft SQL/MSDE Server und/oder MSDE 2000 installieren.

Die letztgültigen Sammelpatches installieren, die nach dem letzten Service Pack erschienen sind.

Die letztgültigen Patches installieren, die nach dem letzten Sammelpatch erschienen sind.

SQL Server Authentication Logging einschalten.

Die Server auf System- und Netzwerkebene sicher einstellen.

Die Rechte des MSSQL/MSDE-Server Dienstes und des SQL/MSDE Server Agents minimieren.

Im Einzelnen:

1. Das Monitor-service für SQL/MSDE auf UDP Port 1434 ausschalten.

Das kann einfach durchgeführt werden, in dem die Funktionalität innerhalb des [SQL Server 2000 Service Pack 3a](#) verwendet wird. Die Datenbank Engine MSDE 2000 von Microsoft hat zwei Buffer Overflow Fehler die es einem Angreifer ermöglichen, diese Schwachstellen ohne Authentifizierung am System auszunutzen. Erschwerend kommt hinzu, dass diese Angriffe über UDP erfolgen. Unabhängig davon ob der MSDE 2000 Prozess im Sicherheitskontext eines Domainusers oder eines lokalen Users ausgeführt wird, kann ein erfolgreicher Angriff die Kompromittierung des gesamten Systems bedeuten. Der MS-SQL/MSDE Slammer sendet ein 376 Byte langes UDP Packet an verschiedenen Zieladressen und den Zielport 1434 und das in rascher Reihenfolge. Erfolgreich eroberte Systeme senden sofort nach der Infektion diese 376 Byte langen Pakete. Der Wurm sendet die Pakete an unterschiedliche zufällige IP Adressen, inkludiert auch Multicast Adressen die zu einem Denial of Service führen. Infizierte Einzelsysteme können bis zu 50 MByte/sec Datenverkehr generieren.

2. Die letztgültigen Service Packs für Microsoft SQL/MSDE Server und/oder MSDE 2000 installieren.

Die derzeitige Version des Microsoft SQL/MSDE Service Packs ist:

- o SQL/MSDE Server 7.0 Service Pack 4
- o MSDE/SQL Server 2000 Service Pack 3a

Um die Patches immer am aktuellen Stand zu halten, sollten Sie [Make Your SQL/MSDE Servers Less Vulnerable](#) von Microsoft Technet lesen.

3. Die letztgültigen Sammelpatches installieren, die nach dem letzten Service Pack erschienen sind.

Der letztgültige Sammelpatch für alle SQL/MSDE/MSDE-Server Versionen ist unter [MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks \(Q316333/Q327068\)](#) zu finden.

Um immer am letzten Stand zu sein sollten Sie regelmäßig überprüfen, ob neue Sammelpatches für Microsoft SQL/MSDE Server erschienen sind, und zwar unter:

- o [Microsoft SQL/MSDE Server 7.0](#)
 - o [Microsoft SQL Server 2000](#)
 - o [MSDE Server Desktop Engine 2000 \(MSDE 2000\)](#)
4. Die letztgültigen Patches installieren, die nach dem letzten Sammelpatch erschienen sind.

Zurzeit gibt es keinen neuen Patch, der nach [MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks \(Q316333/Q327068\)](#) erschienen ist. Um immer über die neuesten Patches informiert zu sein, lesen Sie:

- o [Microsoft SQL/MSDE Server 7.0](#)
 - o [Microsoft SQL Server 2000](#)
 - o [MSDE Server Desktop Engine 2000 \(MSDE 2000\)](#)
5. SQL Server Authentication Logging einschalten.

SQL Server Authentication Logging ist üblicherweise nicht eingeschaltet. Das kann mittels Enterprise Manager (Server Properties; Security) durchgeführt werden.

6. Die Server auf System- und Netzwerkebene sicher einstellen.

Eine MSSQL/MSDE Schwachstelle, die am häufigsten ausgenutzt wird, ist der Administrator "sa", der ohne Kennwort betrieben werden kann. Wenn der "sa" Account keinen Kennwortschutz aufweist, verfügt das System über keinen Schutz und ist jeglicher Wurmattake oder anderen Angriffen ausgeliefert. Daher ist daher sinnvoll, den Empfehlungen über "System Administrator (SA) Login" auf [SQL/MSDE Server Books Online](#) zu folgen und um sicher zu stellen, dass alle SA-Accounts starke Kennwörter verwenden, selbst wenn der SQL/MSDE Server diesen Account nicht verwendet. Das Microsoft Developer Network hat Unterlagen über [Changing the SQL Server Administrator Login](#) und [How to Verify and Change the System Administrator Password by Using MSDE](#) veröffentlicht.

7. Die Rechte des MSSQL/MSDE-Server Service and des SQL/MSDE Server Agent minimieren.

Führen Sie das MSSQL/MSDE Server-Service und den SQL/MSDE Agent unter einen Domainuser aus, der über minimale Rechte verfügt und nicht als Domainadministrator oder SYSTEM (unter NT) oder LocalSystem (Windows 2000 oder XP). Ein kompromittiertes Service, das mit lokalen oder Domänenrechten ausgeführt wird, gibt dem Angreifer die komplette Kontrolle über das System oder das gesamte Netzwerk.

- a. Windows Authentifizierung (Überwachungsrichtlinien) einschalten, erfolgreiche und fehlgeschlagenen Anmeldeversuche mitprotokollieren, danach MSSQL/MSDE Server-Service stoppen und neu starten. Wenn möglich, sollen die Clients so konfiguriert werden, dass sie NT Authentifizierung verwenden.
- b. Paketfilterung sollte an den Netzwerkgrenzen durchgeführt werden, um unerlaubten eingehenden und ausgehenden Verbindungsaufbau von und zu MSSQL spezifischen Services zu unterbinden. Die Filterung (eingehend und ausgehend) der TCP/UDP Ports 1433 und 1434 kann verhindern, dass interne oder externe Angreifer nach anfälligen Microsoft SQL/MSDE Servern suchen und diese infizieren können (im eigenen Netzwerk und außerhalb).
- c. Wenn TCP/UDP 1433 und 1434 am Internet freigeschalten werden müssen, sollten diese Freischaltungen genau konfiguriert werden, damit möglichst keine Angriffe auf diesen Ports zugelassen werden.

Zusätzliche Information wie Microsoft SQL/MSDE Server sicher gemacht werden können, finden Sie unter

- [Microsoft SQL/MSDE Server 7.0 Security](#)
- [Microsoft SQL/MSDE Server 2000 Security](#)

[zum Anfang ^](#)

W5 Windows Authentifizierung

W5.1 Beschreibung

Kennwörter, Passwortphrasen und Sicherheitscodes werden fast in jeder Interaktion zwischen Anwendern und Systemen verwendet. Die meisten Arten von Anwenderauthentifizierung und auch Dateischutz beruhen auf Kennwörter, die von den Anwendern eingegeben werden. Da erfolgreiche Anmeldungen meistens nicht aufgezeichnet werden, oder wenn aufgezeichnet kaum Verdacht erregen, eröffnet ein bekannt gewordenes Kennwort die Möglichkeit, Systeme fast unbemerkt auszuspionieren. Ein Angreifer hat kompletten Zugriff zu allen Systemressourcen, die dem User auch zur Verfügung stehen. Dadurch erhöht sich die Wahrscheinlichkeit, dass der Angreifer Zugriff auf andere Systeme und eventuell auch Administratorenrechte erlangen kann. Unabhängig von der Bedrohung sind Accounts mit schlechten oder überhaupt ohne Kennwörter sehr verbreitet und Firmen mit guten Kennwortrichtlinien sind viel zu selten.

Die am meisten verbreiteten Schwachstellen mit Kennwörtern sind:

- Anwenderkonten mit schlechten oder überhaupt ohne Kennwort.
- Unabhängig von der Qualität wird das Kennwort nicht geschützt.
- Das Betriebssystem oder zusätzliche Software generieren administrative Accounts mit schlechten oder überhaupt ohne Kennwort.
- Passwort Hash Algorithmen sind bekannt und oft werden die Hashwerte so gespeichert, dass jeder diese Werte lesen kann. Der beste und angemessenste Schutz dagegen ist eine starke Kennwortrichtlinie. Diese Richtlinie soll genaue Anweisungen enthalten, wie ein starkes Kennwort aussehen muss und wie Kennwörter auf Integrität geprüft werden.

Microsoft Windows speichert oder versendet Kennwörter nicht im Klartext sondern verwendet Hashwerte der Kennwörter für die Authentifizierung. Ein Hashwert ist ein Ergebnis einer mathematischen Funktion (dem Hash Algorithmus) mit einer fixen Länge, die Menge der Daten (Message Digest) ist beliebig. (MSDN Library) Es gibt drei Windows Authentifizierungsalgorithmen: LM (am unsichersten, am kompatibelsten), NTLM und NTLMv2 (am sichersten, am wenigsten kompatibel). Obwohl die meisten Windowsumgebungen keinen Bedarf an LAN Manager (LM) Unterstützung haben, speichert Windows nach wie vor LM Hashwerte der Kennwörter (auch bekannt unter LANMAN Hash) standardmäßig unter Windows NT, Windows 2000 und Windows XP (nicht unter Windows 2003). Da LM eine viel schwächere Verschlüsselungsmethode als die aktuelleren Ansätze (NTLM und NTLMv2) verwendet, können LM Kennwörter in sehr kurzer Zeit geknackt werden. Selbst Kennwörter, die starke Eigenschaften haben, können mit Brute-Force-Attacken mit heutiger Hardware in weniger als einer Woche geknackt werden.

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/Security/h_gly.asp

Die Schwächen des LM Hashwertes beruhen auf folgenden Umständen:

- Kennwörter werden auf 14 Stellen abgeschnitten.
- Kennwörter werden mit Leerzeichen auf 14 Zeichen aufgefüllt.
- Kennwörter werden auf Großbuchstaben umgewandelt.
- Kennwörter werden in 2 Blöcke zu je 7 Zeichen aufgeteilt.

Dieser Hashing Prozess bedeutet, dass ein Angreifer nur zwei 7-stellige Kennwörter knacken muss, bei denen nur Großbuchstaben verwendet werden, um authentifizierten Zugang zum System zu erlangen. Da die Komplexität ein Kennwort zu knacken, geometrisch mit der Länge des Hashwertes wächst, ist ein 7-stelliger Hashwert um mindestens eine Größenordnung einfacher zu knacken als ein 14-stelliger Hashwert. Da die Hashwerte immer 7-stellig sind (inklusive Leerzeichen) und nur Großbuchstaben verwendet werden, ist eine Wörterbuchattacke ebenfalls einfacher. Die LM Hashmethode unterminiert daher komplett eine gute Kennwortrichtlinie.

Zusätzlich zu dem Risiko, dass LM Hashwerte in der SAM gespeichert sind, ist die LAN Manager Authentifizierung oft standardmäßig auf den Clientsystemen eingeschaltet und wird von den Servern akzeptiert. Das führt dazu, dass Windows-Systeme die einen stärkeren Hashalgorithmus verwenden könnten anstelle schwache LM Hashwerte über das Netzwerk verschicken. Das führt dazu, dass die Windows Authentifizierung anfällig für Abhörangriffe durch Sniffer ist und dadurch wird der Aufwand für einen Angreifer ein Kennwort zu knacken verringert.

W5.2 Betroffene Betriebssysteme

Alle Microsoft Windows Betriebssysteme.

W5.3 CVE/CAN Einträge

[CVE-2000-0222](#)

[CAN-1999-0504](#), [CAN-1999-0505](#), [CAN-1999-0506](#)

W5.4 Wie Sie herausfinden, ob Sie betroffen sind

Obwohl es erkennbare Anzeichen für generelle Kennwortschwächen gibt, wie aktive Konten von Anwendern, die die Firma schon verlassen haben oder Dienste, die nicht verwendet werden, ist

der einzige Weg sicher zu sein, dass jedes Kennwort starke Eigenschaften aufweist die Verwendung von Kennwort-Crackprogrammen, die gleichen Werkzeuge, die ein Angreifer verwendet.

Hinweis: Nie ein Kennwort-Crackprogramm verwenden, selbst wenn Sie für das System administrative Rechte haben, ohne ausdrückliche, vorzugsweise schriftliche Genehmigung des Arbeitgebers. Administratoren mit den besten Absichten wurden entlassen, da Sie Kennwort-Crackprogramme ausgeführt haben, ohne Genehmigung das zu tun.

Einige der besten Programme sind verfügbar unter: [LC4 \(l0phtcrack Version 4\)](#) und [John the Ripper](#)

Bezüglich der lokal gespeicherten LAN Manager Hashwerte:

- Wenn Sie standardmäßige Installationen von NT, 2000 oder XP verwenden, sind die Systeme anfällig, da der LAN Manager Hashwert automatisch lokal gespeichert wird.
- Wenn Sie Altsysteme verwenden, die LM Authentifizierung benötigen um mit dem Server zu kommunizieren, sind diese Systeme anfällig, da die LM Hashwerte mit Sniffen im Netzwerk gelesen werden können.

W5.5 Wie Sie sich dagegen schützen können

Die beste und die am besten geeignete Verteidigung gegen Kennwortschwächen ist eine starke Kennwortrichtlinie mit genauen Anleitungen, wie ein Kennwort auszusehen hat und wie die Integrität der Kennwörter überprüft wird.

Stellen Sie sicher, dass die Kennwörter immer starke Eigenschaften aufweisen. Mit genügend Hardware und genug Zeit kann jedes Kennwort mit Brute-Force-Attacken geknackt werden. Aber es gibt einfachere und sehr erfolgreiche Möglichkeiten Kennwörter in Erfahrung zu bringen, ohne größeren Aufwand. Kennwort-Crackprogramme setzen so genannte Wörterbuchattacken ein. Da die Verschlüsselungsmethoden bekannt sind, vergleicht das Crackprogramm einfach die verschlüsselte Form des Kennwortes mit den verschlüsselten Wörtern eines Wörterbuches (in vielen verschiedenen Sprachen), dazugehörigen Namen und Kombinationen aus beiden. Daher ist ein Kennwort, das sich aus bekannten Worten zusammensetzt anfällig für Wörterbuchattacken. Viele Firmen instruieren ihre Anwender, Kennwörter aus Kombinationen von alphanumerischen Zeichen und Sonderzeichen zu verwenden. Die Anwender verwenden sehr oft Wörter (z.B. password) und verändern Buchstaben in Zahlen oder Sonderzeichen (pa\$\$w0rd). Solche Veränderungen schützen nicht gegen Wörterbuchattacken: pa\$\$w0rd wird sehr wahrscheinlich als password geknackt.

Ein gutes Kennwort kann daher nicht ein Wort oder einen Namen als Wurzel verwenden. Eine starke Kennwortrichtlinie sollte die Anwender daher darauf hinweisen, dass eine zufällige Buchstaben-Zahlen-Sonderzeichenkombination verwendet werden soll, die sich zum Beispiel aus einer Phrase oder eines Buchtitels oder eines Liedes bilden lässt. Bei einer Verkettung einer längeren Phrase (jeweils der erste Buchstabe eines Wortes, oder ein Wort durch ein Sonderzeichen ersetzen, alle Selbstlaute weglassen, usw.) können die Anwender Buchstaben-, Zahlen-, Sonderzeichenketten generieren, die eine Wörterbuchattacke kaum mehr entschlüsseln kann. Und wenn die Phrase leicht zu merken

ist, sollte es auch das Kennwort sein.

Nachdem die Anwender genaue Instruktionen erhalten haben, wie ein gutes Kennwort aussehen soll, müssen Prozeduren eingesetzt werden, die garantieren, dass diese Richtlinien eingehalten werden. Die beste Möglichkeit das zu tun ist der Zeitpunkt der Änderung des Kennwortes mittels Passfilt (NT4).

Windows 2000, XP und 2003 verfügen über Werkzeuge um starke Kennwörter durchzusetzen. Um die Einstellung Ihres Systems zu überprüfen, müssen folgende Schritte durchgeführt werden (Start - Programme - Verwaltung - Lokale Sicherheitseinstellungen - Kontorichtlinien auswählen - Kennwortrichtlinien). Die lokalen Kennwortrichtlinien haben folgende Einstellungsmöglichkeiten:

- **Kennwörter müssen den Komplexitätsanforderungen entsprechen.** Es wird festgelegt, ob die Kennwörter den Komplexitätsanforderungen entsprechen müssen. Die Komplexitätsanforderungen werden bei der nächsten Kennwortänderung oder Neuerstellung erzwungen. Wenn diese Richtlinie aktiviert ist, muss das Kennwort folgende Mindestanforderungen entsprechen:

Enthält nicht den Accountnamen, ganz oder Teile davon

Muss mindestens 6 Zeichen lang sein

Muss Zeichen aus drei der folgenden vier Kategorien enthalten:

Großbuchstaben (A - Z)

Kleinbuchstaben (a - z)

Zahlen (0 - 9)

Sonderzeichen (z.B. !, \$, #, %)

- **Kennwortchronik erzwingen (Bereich 0 -24):** Es wird festgelegt, wie viele neuen Kennwörter für den Useraccount generiert werden müssen, bevor ein altes Kennwort wieder verwendet werden darf. Die Einstellungsmöglichkeit liegt zwischen 0 und 24 Kennwörtern. Wenn dies auf 0 eingestellt wird können Kennwörter sofort wieder verwendet werden, wenn dies auf 24 eingestellt wird müssen 24 neue Kennwörter verwendet werden bevor ein altes Kennwort wieder verwendet werden kann. Diese Einstellung ermöglicht Administratoren die Sicherheit zu erhöhen, in dem alte Kennwörter nicht fortwährend wieder verwendet werden können. Um eine Kennwortchronik effektiv zu verwenden, stellen Sie das Minimale Kennwortalter so ein, dass Kennwörter nicht sofort geändert werden können.
- **Maximales Kennwortalter (Bereich: 0-999 Tage):** Es wird festgelegt, wie viele Tage ein Kennwort verwendet werden kann bevor es geändert werden muss. Sie können festlegen, nach wie vielen Tagen (0 bis 999) ein Kennwort abläuft. Wenn diese Einstellung 0 ist, läuft das Kennwort nie ab.
- **Minimales Kennwortalter (Bereich: 0-999 Tage):** Es wird festgelegt, wie viele Tage ein Kennwort verwendet werden muss bevor es geändert werden kann. Es

kann ein Wert zwischen 0 und 999 Tagen eingestellt werden, eine sofortige Änderungsmöglichkeit wird mit der Einstellung 0 erreicht. Das minimale Kennwortalter muss weniger als das maximale Kennwortalter sein. Konfigurieren Sie das minimale Kennwortalter höher als 0 um die Kennwortchronik sinnvoll zu verwenden. Ohne minimales Kennwortalter können die Anwender Kennwörter eingeben, bis sie das favorisierte Kennwort wieder verwenden können. Die standardmäßige Einstellung folgt nicht dieser Empfehlung, damit ein Administrator ein Kennwort für den Anwender einstellen kann und dieser dann beim ersten Anmeldeversuch das Kennwort ändern kann. Wenn das minimale Kennwortalter auf 0 gesetzt ist, braucht der Anwender das Kennwort nie zu ändern. Aus diesem Grund ist die Kennwortchronik standardmäßig auf 1 gestellt.

- **Minimale Kennwortlänge (Bereich: 0-14 Zeichen):** Es wird festgelegt, wie viele Zeichen mindestens ein Kennwort enthalten muss. Der Wert kann zwischen 1 und 14 eingestellt werden oder es kann 0 eingestellt werden, wodurch kein Kennwort notwendig ist. Die Einstellung der minimalen Kennwortlänge soll mit der Kennwortrichtlinie übereinstimmen (andernfalls wird empfohlen, mindestens 8 Zeichen oder mehr einzustellen; die [National Security Agency \(NSA\)](#) empfiehlt 12 Zeichen).
- **Kennwörter für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern:** Es wird festgelegt, ob Windows 2000, 2003 oder XP Professional Kennwörter mit umkehrbarer Verschlüsselung speichert. Diese Richtlinie unterstützt Applikationen, die Anwenderkennwörter für die Authentifizierung benötigen. Kennwörter mit umkehrbarer Verschlüsselung zu speichern entspricht in etwa dem Speichern des Kennwortes in Klartext. Daher ist diese Einstellung nie auf aktiviert zu setzen, außer die Applikationsanforderung überwiegt über dem Schutz des Kennwortes.

Eine Möglichkeit zum automatischen Erstellen von komplexen Kennwörtern besteht in Windows NT, 2000, XP und 2003. Führen Sie den folgenden Befehl aus (vom Command Prompt):

```
Net user username /random
```

Das Ausführen dieses Befehls generiert ein komplexes, immer 8-stelliges Kennwort, das auf der Konsole angezeigt wird. Diese Methode wird üblicherweise für Serviceaccounts verwendet, nicht für Benutzeraccounts.

Die beste Möglichkeit, Kennwörter auf ihre Qualität zu überprüfen ist das Ausführen von Kennwort-Crackprogrammen im Stand-alone Modus als Teil der Routineüberprüfung.

Wichtiger Hinweis: Nie ein Kennwort-Crackprogramm verwenden, selbst wenn Sie für das System administrative Rechte haben, ohne ausdrückliche, vorzugsweise schriftliche Genehmigung des Arbeitgebers. Administratoren mit den besten Absichten wurden entlassen, da sie Kennwort-Crackprogramme ausgeführt haben, ohne Genehmigung dazu zu tun.

Nachdem Sie eine Genehmigung zur Kennwortüberprüfung haben, sollte die Überprüfung regelmäßig auf einem geschützten System durchgeführt werden. Die Anwender, deren Kennwort entschlüsselt wurde, sollten im Vertrauen darüber informiert werden und es

sollte den Anwender erklärt werden, welche Eigenschaften Kennwörter haben sollten. Administratoren und das Management sollten diese Prozeduren gemeinsam durchführen, damit das Management unterstützend eingreifen kann, wenn die Anwender die Benachrichtigung ignorieren.

Andere Möglichkeiten, um sich gegen schwache Kennwörter (oder gar keine) zu schützen ist die Verwendung von alternativen Authentifizierungsmethoden wie Token oder Biometrie.

Starke Kennwörter schützen. Selbst wenn die starken Kennwörter verwendet werden, können Accounts kompromittiert werden, weil die Kennwörter nicht geschützt wurden. Gute Richtlinien sollten inkludieren, dass Kennwörter niemals weitergegeben werden dürfen, nicht aufgeschrieben werden, wo andere Personen sie lesen könnten und Dateien, in denen Kennwörter für automatische Authentifizierung stehen ordnungsgemäß geschützt werden (Kennwörter können besser geschützt werden, wenn diese Praktiken nur wenn absolut notwendig angewendet werden). Ein maximales Kennwortalter sollte erzwungen werden, damit ein Kennwort, welches diesen Regeln durchschlüpft nur für eine kurze Zeit verwendet werden können. Alte Kennwörter sollten nicht wieder verwendbar sein. Stellen Sie sicher, dass den Anwendern durch Hinweise der Ablauf des Kennwortalters rechtzeitig bekannt gegeben wird. Wenn die Anwender mit der Meldung: "Ihr Kennwort ist abgelaufen und sie müssen es jetzt ändern" konfrontiert werden, wird eher ein schlechtes Kennwort ausgewählt.

2. Accounts genau überprüfen.

- Jeder servicebasierende oder administrative Account, der nicht verwendet wird, sollte deaktiviert oder gelöscht werden. Jeder servicebasierende oder administrative Account der verwendet wird sollte mit einem neuen, starken Kennwort versehen werden.
- Überprüfen Sie die Accounts Ihrer Systeme und generieren Sie eine Hauptliste. Vergessen Sie nicht die Kennwörter von Routern, digitalen Druckern, die an das Internet angebunden sind sowie Drucker und Kopierer zu überprüfen und in der Liste aufzunehmen.
- Entwickeln Sie Prozeduren, um autorisierte Accounts zu dieser Liste hinzuzufügen und auch um Accounts zu entfernen, die nicht mehr benötigt werden.
- Überprüfen Sie die Liste regelmäßig um festzustellen, dass keine neuen Accounts hinzugefügt wurden und das nichtverwendete Accounts entfernt wurden.
- Sie sollten fixe Prozeduren für das Entfernen von Accounts haben, wenn Angestellte oder externe Mitarbeiter das Unternehmen verlassen und die Konten nicht mehr benötigt werden.

3. **Eine starke Kennwortrichtlinie für das Unternehmen einhalten.** Zusätzlich zu Betriebssystemen oder Netzwerkkontrollen, gibt es viele umfangreiche Werkzeuge, um eine gute Kennwortrichtlinie zu managen. Viele Musterrichtlinien, Richtlinienentwicklungsleitfaden, Kennwortsicherheitsgrundlagen und Links zu verschiedenen Webseiten mit Sicherheitsrichtlinien können unter [SANS Security Policy Project](#) gefunden werden.

4. **LM Authentifizierung im Netzwerk deaktivieren.** Der beste Ersatz für LAN Manager Authentifizierung ist die NT LAN Manager Version2 (NTLMv2) Authentifizierung. Die NTLMv2 Challenge/Response Methode verwendet starke Verschlüsselung und bessere Authentifizierung und Session-Sicherheitsmechanismen. Der Registrierungsschlüssel, der die Möglichkeit überprüft ist in Windows NT und Windows 2000:

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\LSA
Value: LMCompatibilityLevel
Value Type: REG_DWORD - Number
Valid Range: 0-5
Default: 0

Beschreibung: Dieser Parameter spezifiziert, welche Authentifizierung verwendet wird.

- 0 - Sendet LM Antworten und NTLM Antworten; verwendet nie NTLMv2 Sessionsicherheit
- 1 - Verwendet NTLMv2 Sessionsicherheit wenn ausgehandelt
- 2 - Sendet nur NTLM Authentifizierung
- 3 - Sendet nur NTLMv2 Authentifizierung
- 4 - DC weist LM Authentifizierung ab
- 5 - DC weist LM und NTLM Authentifizierung ab (nur NTLMv2 wird akzeptiert)

In Windows 2000, 2003 und XP können dieselben Funktionalitäten durch die Konfiguration der LAN Manager Einstellungen (Windows 2000) oder Netzwerksicherheit eingestellt werden: LAN Manager Authentifizierungsstufe (Windows XP, Windows 2003) (Start - Programme - Verwaltung - Lokale Sicherheitsrichtlinien - Lokale Richtlinien - Sicherheitsoptionen).

Wenn alle Ihre Systeme das Betriebssystem Windows NT SP4 oder später verwenden, können diese Einstellungen auf 3 auf allen Clients gestellt werden und 5 auf allen Domain Controllern. Damit werden keine LM Hashwerte über das Netzwerk transportiert. Bei Altsystemen (wie Windows 95/98) funktioniert NTLMv2 nicht mit dem standardmäßigen Microsoft Network Client. Um NTLMv2 Funktionalität zu erlangen, muss der Directory Service Client installiert werden. Nach der Installation ist der Registrierungs-Value-Name "LMCompatibility" und die möglichen Einstellungen sind 0 und 3.

Wenn bei Altsysteme NTLMv2 nicht erzwungen werden kann, dann kann eine geringe Verbesserung durch die Verwendung von NTLM (NT Lan Manager Version 1) anstelle des LM Hashwertes erreicht werden, die auf den Domain Controllern erzwungen werden kann (der LMCompatibilityLevel wird auf 4 eingestellt, oder wenn Lokale Sicherheitsrichtlinien verwendet wird: Send NTLMv2 Response only\Refuse LM). Die sicherste Option im Bezug auf Altsysteme ist die Migration auf ein neues Betriebssystem, da die alten Betriebssysteme die Minimum Sicherheitsanforderungen nicht unterstützen.

5. **Verhindern, dass der LM Hashwert gespeichert wird** Ein wesentliches Problem, obwohl der LM Hashwert nicht im Netzwerk versendet wird ist, dass der LM Hashwert nach wie vor in der SAM oder im Active Directory gespeichert wird. Microsoft hat einen Mechanismus verfügbar, wodurch die Kreation eines LM Hashwertes ausgeschaltet wird. Dies ist jedoch nur in Windows 2000, 2003 und XP Systemen möglich. In Windows 2000

(SP2 oder später) ist folgender Registrierungsschlüssel dafür verantwortlich:

Hive: HKEY_LOCAL_MACHINE

Key: System\CurrentControlSet\Control\LSA\NoLMHash

Wenn dieser Schlüssel unter Windows 2000 am Domain Controller generiert wird, werden keine LanMan Hashwerte mehr kreiert und im Active Directory gespeichert.

In Windows XP und 2003 kann die gleiche Funktionalität implementiert werden, in dem die Einstellungen Netzwerksicherheit konfiguriert wird: LAN Manager Hashwert nach nächstem Kennwortwechsel nicht speichern (Start - Programme - Verwaltung - Lokale Sicherheitseinstellungen - Lokale Richtlinien - Sicherheitsoptionen).

Nachdem die Änderungen durchgeführt wurden, müssen die Systeme neu gestartet werden, damit die Änderungen wirksam werden.

Wichtiger Hinweis: Diese Änderungen verhindern nur die neue Generierung von LM Hashwerten. Bereits existierende LM Hashwerte werden erst entfernt, wenn der Anwender das nächste Mal das Kennwort ändert.

6. **Verhindern, dass Kennworthashwerte und die SAM kopiert werden können.** Programme zum Cracken von Kennwörtern, die in diesem Abschnitt beschrieben sind, erlangen Hashwerte durch:
- Kennwörter vom Netzwerk mitlesen (Sniffer). 1. Ein geschwichtes Netzwerk verwenden; 2. Erkennung und Entfernung von Netzwerkkarten im "promiscuous Mode" (können mit Hilfe der meisten kommerziellen Security Assessment Tools, oder bei Freeware Tools wie [ethereal](#)).
 - Kopieren der SAM (gespeichert im Verzeichnis %SystemRoot%\System32\Config\ üblicherweise C:\Winnt\System32\Config\ in Windows NT und 2000 oder C:\Windows\System32\Config\ in Windows XP und 2003). Die Datei ist normalerweise vom Windows Betriebssystem gesperrt und kann nur kopiert werden, wenn das System mit einem anderen Betriebssystem gestartet wird. SAM Dateien können auch durch ein Backup der SAM Datei oder des System State (Windows 2000, 2003, XP) erlangt werden. SAM Dateien sind auch auf der NT4 Repair Disk gespeichert.

Gegenmaßnahmen: Beschränken und überwachen Sie den physischen Zugriff auf Computersysteme (speziell die Domain Controller), Backupmedien und Repair Disks.

Die folgenden Microsoft Artikel dienen als nützliche Referenzen:

- [How to Disable LM Authentication on Windows NT \[Q147706\]](#) beschreibt die notwendigen Änderungen in der Registrierung für Windows 9x und Windows NT/2000 Systeme.
- MS03-034 : Ein Fehler im NetBIOS kann zur Informationsbekanntmachung führen (824105)
- [LMCompatibilityLevel and Its Effects \[Q175641\]](#) erklärt die Interoperabilität der

- o einzelnen Parameter.
- o [How to Enable NTLMv2 Authentication for Windows 95/98/2000/NT \[Q239869\]](#) erklärt, wie Windows 2000 Directory Service Client für Windows 95/98 Systeme eingesetzt werden kann, um die NTLMv2 Kompatibilität zu erreichen.
- o [New Registry Key to Remove LM Hashes from Active Directory and Security Account Manager](#)

[zum Anfang ^](#)

W6 Web Browser

W6.1 Beschreibung

Der Browser ist ein Programm mit dem ein Computeranwender auf Windows Systemen Zugang zum Web erlangt. Der dominierende Web Browser ist der Microsoft Internet Explorer (IE), welcher der standardmäßige Web Browser auf Windows Plattformen ist. Andere Web Browser inkludieren Mozilla, Firefox, Netscape und Opera. Die letzte Version des Internet Explorers ist Version 6, und wird hier beschrieben. Die Sicherheitsschwachstellen sind auch für Mozilla Versionen 1.4 – 1.7.1, Firefox Version 0.9.x, Netscape Version 7.x und Opera Version 7.x gültig.

Die Probleme sind sechsfach:

1. Eine Vielzahl von Sicherheitsschwachstellen über die letzten Jahren im Vergleich zu anderen Browsern – 153 IE Sicherheitsschwachstellen seit April 2001, laut [Security Focus Archive](#).
2. Lange Zeit bevor bekannte Sicherheitsschwachstellen gepatcht werden konnten – Anwender mussten bis zu 6 Monaten auf Patches von Microsoft warten, nachdem Sicherheitsschwachstellen bekannt wurden.
3. IE's Active X und Active Scripting – durch IE Sicherheitsschwachstellen, im speziellen mit der Verwendung von ActiveX, waren in der Vergangenheit die Umgehung von Sicherheitseinstellungen möglich wodurch eine Kompromittierung des Betriebssystems auf Hostsystemen möglich wurde.
4. Eine Vielzahl von nicht gepatchten Sicherheitsschwachstellen - 34, laut <http://umbrella.name/originalvuln/msie/>
5. Spyware/Adware Sicherheitsschwachstellen – Das betrifft alle Browser, aber IE ist anfälliger als andere Browser.
6. Die Integration des IE Browsers in das Betriebssystem, wodurch das Betriebssystem anfälliger für Sicherheitsschwachstellen ist.

Andere Browser haben auch Probleme, aber nicht in dem Ausmaße wie der IE. Ein boshafter Webprogrammierer kann eine Webseite kreieren die Sicherheitsschwachstellen des Internet Explorers ausnutzt, einfach durch das öffnen der Seite mit dem IE. Ein typisches Beispiel dafür ist die [Download.Ject](#) Sicherheitsschwachstelle. Die Schwachstelle war für viele Monate bekannt und nutzt eine Schwachstelle in ActiveX aus. Es wurde am 8. Juni ein Exploit veröffentlicht, der Patch von Microsoft wurde erst im Juli 2004 zur Verfügung gestellt. Durch die Kombination von ActiveX, Scripting die Integration in das Betriebssystem ist der Internet Explorer anfälliger für Attacken als viele andere Browser. Die Konsequenzen daraus können die Offenlegung von Cookies, lokalen Dateien oder Daten, die Ausführung von Programmen, der Download und die Ausführung von beliebigen Code bis zur kompletten Übernahme des Gerätes sein.

W6.2 Betroffene Betriebssysteme

Diese Sicherheitsschwachstellen bestehen auf allen Windows Systeme, die einen der Browser verwenden. Es ist wichtig zu wissen, dass der IE mit einer Vielzahl von Microsoft Programmen installiert wird und daher typischerweise auf allen Windowssystemen vorhanden ist, obwohl die

Anwender den IE gar nicht installieren wollen. Alle anderen Browser werden durch den Anwender installiert und der Anwender selbst entscheidet, ob der Browser von anderen Applikationen verwendet werden darf oder nicht.

W6.3 Browser Sicherheitsschwächen, zur Verfügung gestellt von Secunia

A. Internet Explorer:

2004 - 15 Security Advisories (zum 30. Juli, 2004)

1. [Microsoft Internet Explorer Multiple Vulnerabilities](#)
2. [Internet Explorer Frame Injection Vulnerability](#)
3. [Internet Explorer File Download Error Message Denial of Service Weakness](#)
4. [Internet Explorer Security Zone Bypass and Address Bar Spoofing Vulnerability](#)
5. [Internet Explorer Local Resource Access and Cross-Zone Scripting Vulnerabilities](#)
6. [Microsoft Internet Explorer and Outlook URL Obfuscation Issue](#)
7. [Windows Explorer / Internet Explorer Long Share Name Buffer Overflow](#)
8. [Microsoft Outlook Express MHTML URL Processing Vulnerability](#)
9. [Internet Explorer/Outlook Express Restricted Zone Status Bar Spoofing](#)
10. [Multiple Browser Cookie Path Directory Traversal Vulnerability](#)
11. [Internet Explorer Cross Frame Scripting Restriction Bypass](#)
12. [Internet Explorer File Identification Variant](#)
13. [Internet Explorer Travel Log Arbitrary Script Execution Vulnerability](#)
14. [Internet Explorer File Download Extension Spoofing](#)
15. [Internet Explorer showHelp\(\) Restriction Bypass Vulnerability](#)

B. Mozilla Vulnerabilities

2004 - 7 Secunia Advisories

1. [Mozilla Fails to Restrict Access to "shell:"](#)
2. [Mozilla XPInstall Dialog Box Security Issue](#)
3. [Multiple Browsers Frame Injection Vulnerability](#)
4. [Mozilla Browser Address Bar Spoofing Weakness](#)
5. [Mozilla / NSS S/MIME Implementation Vulnerability](#)
6. [Multiple Browser Cookie Path Directory Traversal Vulnerability](#)
7. [Mozilla Cross-Site Scripting Vulnerability](#)

D. Netscape Vulnerabilities

2004 - 2 Secunia Security Advisories

1. [Mozilla Fails to Restrict Access to "shell:"](#)
2. [Multiple Browsers Frame Injection Vulnerability](#)

E. Opera Vulnerabilities

2004 - 8 Secunia Security Advisories

1. [Opera Browser Address Bar Spoofing Vulnerability](#)
2. [Multiple Browsers Frame Injection Vulnerability](#)
3. [Opera Address Bar Spoofing Security Issue](#)
4. [Opera Browser Favicon Displaying Address Bar Spoofing Vulnerability](#)
5. [Multiple Browsers Telnet URI Handler File Manipulation Vulnerability](#)
6. [Opera Browser Address Bar Spoofing Vulnerability](#)
7. [Multiple Browser Cookie Path Directory Traversal Vulnerability](#)
8. [Opera Browser File Download Extension Spoofing](#)

W6.4 Erkennung und Schutz vor Browser Sicherheitsschwachstellen

Wenn Sie den Internet Explorer auf Ihren Systemen verwenden gibt es zur Zeit keine Möglichkeit festzustellen, ob das System für Sicherheitsprobleme anfällig ist, da eine Vielzahl von Sicherheitsproblemen existieren und es keine Patches dafür gibt. Trotzdem sollte die [Windows Update Site](#) regelmäßig besucht werden um sicherzustellen, dass die verfügbaren Patches installiert werden um gegen die Schwachstellen des IE geschützt zu sein. Anwender die an zusätzlichen Schutz vor Browser Sicherheitsschwachstellen interessiert sind könnten die folgenden Hinweise nützlich sein:

Überlegen Sie alternative Browser, die kein ActiveX verwenden. Die meisten Internetseiten verwenden kein ActiveX. Da die Windows Update Webseite, die ActiveX verwendet, von dieser Maßnahmen betroffen ist, könnte auch das [Automatic Updates](#) Feature verwendet werden. Andere Update Optionen wie [Shavlik's HFNetChkPro™](#) oder [Microsoft Baseline Security Analyzer \(MBSA\)](#) können ebenfalls verwendet werden. Es können auch Online Internet Explorer Analysetools wie [Qualys Browser Check](#) sehr nützlich sein um den Sicherheitsstatus des Systems festzustellen.

Wenn die Option a. nicht durchzuführen ist, da ActiveX im Intranet der Organisation verwendet wird, überlegen Sie den Internet Explorer für das Intranet und einen anderen Browser für das Internet zu verwenden.

Wenn ein alternativer Browser keine Option darstellt, könnte ActiveX ausgeschaltet werden außer für interne ActiveX Applets, die auf den Systemen vorinstalliert werden können. Microsoft stellt einen Weg zur Verfügung, ActiveX nicht im Internet Explorer auszuführen.

Andere Browser verfügen nicht über diese automatisierten Tools wie der Internet Explorer. Bei der Verwendung von Mozilla/Firefox, Netscape oder Opera sollten die relevanten Webseiten (<http://www.mozilla.org>, <http://www.netscape.com>, <http://www.opera.com> oder <http://umbrella.name/index.html>) besucht werden, um Probleme und Patches zu finden.

W6.5 Wie Sie den Internet Explorer sicherer machen können

Konfiguration der Sicherheitseinstellungen im Internet Explorer

1. Internetoptionen unter dem Menüpunkt Extras auswählen.
2. Den Sicherheitstab anklicken und dann Stufe anpassen für die Internetzone auswählen.

Die meisten Fehler werden durch Active Scripting oder ActiveX Steuerelemente ausgenutzt.

3. Unter Scripting "Deaktivieren" für "Einfügeoperation über ein Script zulassen" anklicken, um zu verhindern, dass zwischengespeicherter Text vom Clipboard ausgelesen werden kann.

Hinweis: Active Scripting zu deaktivieren kann dazu führen, dass manche Webseiten nicht richtig funktionieren.

ActiveX Steuerelemente sind nicht so populär aber potentiell gefährlicher, da erweiterter Zugang zum System möglich ist.

4. Deaktivieren auswählen für "Download von signierten ActiveX Steuerelementen".
5. Deaktivieren auswählen für "Download von unsignierten ActiveX Steuerelementen".
6. Deaktivieren auswählen für "ActiveX Steuerelemente initialisieren und ausführen, die nicht sicher sind".

Java Applets haben typischerweise mehr Möglichkeiten als Scripts.

7. Unter Microsoft VM, Java Einstellungen "Hohe Sicherheit" auswählen, um Java Applets keinen erweiterten Zugriff auf das System zu geben (in Sandbox auszuführen).
8. Unter Verschiedenes "Auf Datenquellen über Domaingrenzen hinweg zugreifen" deaktivieren um Crosssite Scripting Attacken zu verhindern.

Stellen Sie sicher, dass keine unsicheren Websites unter Vertrauenswürdige Sites oder Lokales Intranet eingetragen sind, da diese Zonen ein schwächeres Sicherheitsniveau haben.

[zum Anfang ^](#)

W7 File Sharing Applikationen

W7.1 Beschreibung

Peer to Peer File Sharing Programme (P2P) werden immer häufiger verwendet und werden immer beliebter. Diese Applikationen werden zum Herunterladen und Verteilen von vielen unterschiedlichen Dateitypen verwendet (z.B. Musik, Video, Grafiken, Text, Quellcode und proprietäre Informationen, um nur einige zu nennen). P2P Applikationen haben mehrere berechnete Verwendungsbereiche, wie die Verteilung von OpenSource/GPL Binaries, ISO Images von bootbaren Linux Distributionen, Kreationen von unabhängigen Künstlern und auch kommerziell die Verteilung von Filmtrailern oder Spieleanschauen. Andere Male sind die Daten entweder urheberrechtlich geschützt oder von fragwürdigen Quellen. Nachdem Napster rechtliche Erfahrungen sammeln musste, werden die meisten P2P Programme jetzt über ein Netzwerk von Clients betrieben, die Verzeichnisse freigeben, Dateien oder manchmal ganze Festplatten. Die Anwender können über die Client Software Suchkriterien eingeben. Die Client Software kontaktiert beteiligte Systeme um die gesuchte Datei zu finden, dabei werden eine oder mehrere Verbindungen zwischen den beteiligten Systemen geöffnet. Die Clientsysteme sind beim Herunterladen der Daten beteiligt, sie stellen Daten zur Verfügung und einige Systeme funktionieren als Superknoten und übernehmen Koordinationsfunktionen für mehrere User.

Peer to Peer Kommunikation besteht aus Anfragen, Antworten und Dateitransfer. Ein Client kann gleichzeitig mehrere Downloads und Uploads durchführen. Die Suchfunktionen können fast jede Zeichenfolge bearbeiten. Die meisten dieser Programme verwenden Standardports, können aber auch automatisch oder manuell konfiguriert werden um andere Ports zu verwenden. Dadurch soll die Erkennung erschwert und Firewalls und ausgehende Filterlisten überlistet werden. Die Verwendung von HTTP Wrapper wird immer beliebter, da dadurch die Restriktionen umgangen werden können. Durch die Mehrfachverbindungen der Suchfunktionen und das Herunterladen kann signifikanten Datenverkehr erzeugt werden. Dadurch werden lokale Netzwerke und auch Weitverkehrsnetzwerke stark belastet.

Es gibt eine Anzahl von Sicherheitsschwachstellen bei der Verwendung von P2P Software, die in drei Kategorien zusammengefasst werden können. Technische Schwachstellen können für Angriffe ausgenutzt werden. Soziale Schwachstellen sind jene, die dadurch ausgenutzt werden, indem der von Dritten angeforderte binäre Inhalt geändert oder entstellt wird. Die rechtlichen Probleme können aus urheberrechtlichen Gründen oder aus rechtlich fragwürdigen Inhalten entstehen.

Wie oben erwähnt, könnten technische Schwachstellen von entfernten Systemen durch das Herunterladen, Installieren und Ausführen von Programmen und Dateien ausgenutzt werden. Die CVE und CAN Einträge beziehen sich alle auf technische Sicherheitsschwachstellen. Diese können von Denial of Service Attacken bis zu beliebigen Dateizugriff reichen und sollten sehr ernst genommen werden. In der CVE Datenbank werden Verletzungen des Datenschutzes und der Vertraulichkeit, die durch die Verwendung von P2P Applikationen entstehen können nicht

behandelt, beide sind aber wichtige Anliegen. Viele dieser Applikationen inklusive "Spyware" und "Adware" Komponenten können sehr viel Bandbreite verbrauchen, da sie das Surfverhalten an die Hersteller schicken. Eine schlecht konfigurierte P2P Anwendung kann unerlaubten Zugriff auf ihr gesamtes Netzwerk durch die Freigabe von verbundenen Netzwerklaufwerken ermöglichen. Es gibt keine oder nur geringe Möglichkeiten, die Art der Daten die gemeinsam genutzt werden können, einzuschränken. Kompromittierung von vertraulichen Informationen und anderen Daten sowie Veröffentlichung von geistigem Eigentum können die Folge sein.

Soziale Schwachstellen bestehen, wenn ein bössartiger User oder ein bereits infiziertes System Daten erstellt oder so verändert, dass andere User diese als begehrenswert finden. Viren, Trojaner, Würmer und andere bössartigen Programme können daraus resultieren. Die Opfer dieser Attacken sind meist weniger technisch versierte Personen, die Daten durch Doppelklick ausführen, ohne zu merken, dass die Dateierweiterung oder das Icon mit der Art der Daten normalerweise nicht übereinstimmt, oder das ausführbare Programme dadurch aktiviert werden können. Unabhängig von dem Inhalt der Downloads müssen die Anwender aktuelle Antivirenprogramme verwenden um die Downloads zu scannen. Wenn möglich, sollten die Checksummen geprüft werden um sicher zu stellen, dass der Download auch das ist, was der Anwender will und was zur Verfügung gestellt wurde. P2P Mechanismen können auch zur Verteilung von bössartigen Code verwendet werden, wie Viren die sich in P2P Inhalten verstecken und sich selbst in den shared Ordnern von infizierten Clients speichern. P2P kann auch Befehle und Steuerungsverkehr zu betroffene Clients tunneln.

Rechtliche Probleme müssen von Firmen- und Privatanwendern ernst genommen werden. Die Inhalte, die durch P2P Applikationen verfügbar sind inkludieren urheberrechtlich geschützte Musik, Filme und Programmdateien. Organisationen wie [MPAA](#), [RIAA](#) und [BSA](#) suchen aktiv nach Verletzungen des Urheberrechtes, die durch P2P Netzwerke entstehen. Strafandrohungen, gesetzlichen Verfügungen und zivile Strafanträge sind landesweit bei Gericht anhängig. Der Erfolg oder Misserfolg dieser Bestrebungen sowie die moralischen Überlegungen bezüglich des Herunterladens von solchen Dateien sind zweitrangig im Vergleich zu den Kosten, die einem Unternehmen für die Beantwortung und die Verteidigung von solchen Anschuldigungen entstehen. Pornografische Inhalte sind in P2P Netzwerken auch sehr verbreitet. Ob solche Inhalte in Ihrer Gerichtsbarkeit legal sind oder nicht ist irrelevant, wenn das Unternehmen wegen sexueller Belästigung verklagt wird, weil ein Mitarbeiter pornografisches Material heruntergeladen hat.

W7.2 Betroffene Betriebssysteme

Alle Versionen von P2P Programmen die auf Windows Plattformen funktionieren, sowie Versionen unter Linux und UNIX.

W7.3 CVE/CAN Einträge

[CAN-2000-0412](#), [CVE-2001-0368](#), [CAN-2002-0314](#), [CAN-2002-0315](#), [CVE-2002-0967](#), [CAN-2003-0397](#)

W7.4 Wie Sie herausfinden, ob Sie betroffen sind

Herauszufinden, ob P2P Aktivitäten in Ihrem Netzwerk stattfinden, kann eine Herausforderung darstellen. P2P Software kann erkannt werden, indem der Netzwerkverkehr beobachtet und aufgezeichnet wird und nach den standardmäßigen Ports durchsucht wird. Es kann auch nach Applikationsstrings von gängigen P2P Programmen gesucht werden. Bitte beachten Sie, dass am Ende dieses Punktes die Ports für gängige P2P Programme angegeben sind. Es gibt eine Anzahl von Applikationen und Services die dabei hilfreich sein können, P2P Verkehr zu erkennen oder zu verhindern. Manche hostbasierende Intrusion Prevention Software kann die Installation von die Installation und Ausführung von P2P Programme verhindern. Cisco Network Based Application

Recognition (NBAR) und andere netzwerkbasierenden Produkte können verhindern, dass P2P Verkehr ins Netzwerk oder aus dem Netzwerk möglich ist, oder aber P2P Verkehr aufgezeichnet. Den WAN Verbindung mit Applikationen wie NTOP zu monitoren kann auch helfen, P2P Verkehr zu erkennen. Speichermedien können auch nach Dateien durchsucht werden, die oft heruntergeladen werden. Dazu zählen die Dateien *.mp3, *.wma, *.avi, *.mpeg, *.jpg, *.gif, *.zip, *.torrent und *.exe. Durch regelmäßige Überprüfung des Plattenspeichers kann auch plötzlich ansteigenden Speicherverbrauch auf eine Verwendung von P2P Programmen hinweisen. Nessus hat auch ein Plug-In, dass laufende P2P Applikationen erkennt. Für Microsoft Windows Systeme kann SMS verwendet werden, um installierte ausführbare Dateien auf den Clients zu erkennen.

W7.5 Wie Sie sich dagegen schützen können

Firmenrichtlinien:

Ihr Unternehmen sollte eine Richtlinie haben, die das Herunterladen von urheberrechtlich geschützten Daten verbietet.

Ihr Unternehmen sollte eine Richtlinie für den angemessenen Gebrauch der Internetverbindung haben.

Netzwerkplatten und PCs sollten regelmäßig auf nicht erlaubte Daten überprüft werden.

Netzwerkeinschränkungen:

Normalen Anwender sollte es nicht erlaubt sein, Software - im speziellen P2P - zu installieren.

Ein Proxyserver sollte für die Kontrolle des Internetzuganges überlegt werden.

Die Accesslisten für ausgehende Services sollten nur geschäftsrelevante Ports erlauben. Da immer mehr P2P Programme HTTP verwenden, ist diese Regelung jedoch kaum effektiv.

Das Netzwerk sollte auf P2P Aktivitäten überprüft werden und etwaige Verstöße sollten an die zuständigen Stellen weitergeleitet werden.

Unternehmensweite Antivirensoftware soll installiert und täglich aktualisiert werden.

Ports, die standardmäßig von Peer to Peer Software verwendet werden:

Napster	eDonkey	Gnutella	KaZaa
---------	---------	----------	-------

- 552 P2P napster upload request
- 556 P2P Outbound GNUTella client request
- 557 P2P GNUTella client request
- 559 P2P Inbound GNUTella client request
- 561 P2P Napster Client Data
- 562 P2P Napster Client Data
- 563 P2P Napster Client Data
- 564 P2P Napster Client Data
- 565 P2P Napster Server Login
- 1383 P2P Fastrack (kazaa/morpheus) GET request
- 1432 P2P GNUTella GET
- 1699 P2P Fastrack (kazaa/morpheus) traffic
- 2180 P2P BitTorrent announce request
- 2181 P2P BitTorrent transfer

Napster	eDonkey	Gnutella	Kazaa
Tcp 8888	tcp 4661	tcp/udp 6345	tcp 80 (WWW)
Tcp 8875	tcp 4662	tcp/udp 6346	tcp/udp 1214
Tcp 6699	udp 4665	tcp/udp 6347	
		tcp/udp 6348	
		tcp/udp 6349	

[zum Anfang ^](#)

W8 LSASS

W8.1 Beschreibung

Das Windows Local Security Authority Subsystem Service in Windows 2000, Server 2003 und Server 2003 64 Bit, XP und XP 64 Bit Editionen beinhaltet kritische Buffer Overflows, die ausgenutzt, zu kompletter Systemkompromittierung führen. Dieser Overflow wird im Microsoft Security Bulletin MS04-01 genau beschrieben. Der Angriff kann remote und anonym über RPC auf Windows 2000 und XP durchgeführt werden, lokale Rechte sind für Server 2003 oder XP 64 Bit Editionen erforderlich.

Das Windows Local Security Authority Subsystem Service (LSASS) spielt eine wichtige Rolle für System Authentifizierung und Active Directory Funktionalität. Beim Interfaceprozess mit dem Active Directory kann die Logging Funktion der LSASRV.dll mit einem übermäßig langen String überflutet werden. Dieser Fehler kann zur kompletten Systemkompromittierung führen.

Die Schwere dieser Möglichkeit, dass die Schwachstelle remote ausgenutzt werden kann wird durch die LSASS basierenden Würmer SASSER und Korgo demonstriert. Auch bekannt als W32.Sasser (<http://www.cert.org/current/archive/2004/07/12/archive.html#sasser>, <http://www.microsoft.com/security/incident/sasser.msp>) und W32.Korgo (<http://www.cert.org/current/archive/2004/07/12/archive.html#korgo>). Viele dieser zur Zeit verwendeten "bot" Würmer verwenden diese Sicherheitschwachstelle auch zur Infektion und die

Wichtigkeit als Sicherheitsproblem wird oft übersehen.

Der Schwachstelle wurde eine CVE Nummer gegeben, CAN-2003-0533. Es wird empfohlen, dass Netzwerkadministratoren nicht nur die Systeme auf diese Sicherheitsschwachstelle hin patchen, es ist auch wichtig, Accesskontrollen am Netzwerkeingang durchzuführen, damit Windows RPC basierende Missbräuche nicht in das Firmennetzwerk dringen können.

W8.2 Betroffene Betriebssysteme

Windows 2000, Windows XP und Professional, Windows XP 64-Bit Edition, Windows 2003

W8.3 CVE/CAN Einträge

[CVE-1999-0227](#)

[CAN-1999-1234](#), [CAN-2001-1122](#), [CAN-2003-0507](#), [CAN-2003-0533](#), [CAN-2003-0663](#), [CAN-2003-0818](#)

W8.4 Wie Sie herausfinden, ob Sie betroffen sind

Diese Sicherheitsschwachstelle kann entweder über das Netzwerk geprüft werden oder lokal am System selbst. Eine Netzwerküberprüfung sollte dann verwendet werden, wenn Sicherheits- und Netzwerkadministratoren fehleranfällige Maschinen in einem Netzwerk in einem IP Bereich finden müssen. Eine lokale Überprüfung ist für Enduser, die das System auf diesen Fehler überprüfen wollen.

Für netzwerkbasierende Erkennung sind die folgenden drei frei verfügbaren Tools zur Fehlererkennung geeignet:

Nessus, ein netzwerkbasierendes Vulnerability Assessment Tool, hat ein smb_kb835732.nasl Plug-In (id 12209) das überprüft, ob der Patch KB835732 vorhanden ist. Details und Download siehe <http://cgi.nessus.org/plugins/dump.php?id=12209>

DSScan von Foundstone ermöglicht eine Überprüfung des ganzen Netzwerkes und hat die Möglichkeit, Warnmeldungen an die betroffenen Systeme zu senden. Details und Download siehe <http://www.foundstone.com/resources/proddesc/dsscan.htm>

Sasser Worm Scanner von eEye stellt fest, ob das System anfällig für den LSASS Exploit und den Sasser Wurm Virus ist. Details und Download siehe <http://www.eeye.com/html/resources/downloads/audits/index.html>

Für die lokale Überprüfung können Microsoft Tools verwendet werden.

Der Microsoft Baseline Security Analyzer (MBSA) hat die Möglichkeit festzustellen, ob der Computer für diesen Exploit anfällig ist. Details und Download siehe <http://www.microsoft.com/technet/security/tools/mbsahome.msp>

Windows Update scannt den Computer gibt eine Selektion von Updates aus, die für das System notwendig sind. Wenn MS04-011 (KB835732) als ein zu installierender Update gelistet wird, dann ist der Computer angreifbar. Eine Schritt für Schritt Anleitung ist unter <http://windowsupdate.microsoft.com> verfügbar.

W8.5 Wie Sie sich dagegen schützen können

Zusammenfassung:

1. Blockieren der Ports auf der Firewall

2. Die letzten Patches von Microsoft installieren
3. Einschalten der Systems advance TCP/IP filtering

Details:

1. Blockieren der Ports auf der Firewall.

Wenn eine Firewall im Einsatz ist, können die internen Netzwerke durch blockieren der angegebenen Ports gegen Angriffe von außen geschützt werden:

UDP/135, UDP/137, UDP/138, UDP/445
TCP/135, TCP/139, TCP/445, TCP/593

Es wird empfohlen, eine hostbasierende Personal-Firewall zu verwenden und jeden unerwünschten Netzwerkverkehr zu blockieren. Wenn die Internet Connection Firewall (ICF), die bei Windows XP und 2003 inkludiert ist verwendet wird, werden eingehende Ports automatisch gesperrt. Um die Internet Connection Firewall einzuschalten, führen Sie folgende Schritte durch:

Start, und **Systemsteuerung** anklicken

In der Standardansicht, klicken Sie auf **Netzwerkverbindungen**, und dann **Ein Heim- oder ein kleines Firmennetzwerk einrichten**. Die Internet Connection Firewall wird eingeschaltet, wenn Sie eine Konfiguration im Netzwerkassistent auswählen, die angibt, dass der Computer direkt mit dem Internet verbunden ist.

Um die Internet Connection Firewall manuell zu konfigurieren, folgen Sie dieser Anleitung:

Start, und **Systemsteuerung** anklicken

In der Standardansicht, klicken Sie auf **Netzwerkverbindungen**.

Rechte Maustaste auf die Verbindung, auf der Sie die Firewall aktivieren wollen, dann

Eigenschaften

Klicken Sie auf den **Erweitert** Tab

Klicken Sie auf **Diesen Computer und das Netzwerk schützen, indem das Zugreifen auf diesen Computer vom Internet eingeschränkt oder verhindert wird**, und dann **OK**

Hinweis: Wenn Sie einigen Programme oder Dienste durch die Firewall ermöglichen wollen, dann klicken Sie auf **Einstellungen** und den **Erweitert** Tab und dann wählen Sie die Programme, Protokolle und Dienste aus die benötigt werden.

2. Installieren Sie die letzten Patches für LSASS abhängig vom Betriebssystem.

Der LSASS Patch ist auf der folgenden Microsoft Site verfügbar.

<http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx>

3. Schalten Sie TCP/IP Filter ein um eingehenden Verkehr zu blockieren. Zur Konfiguration der

TCP/IP Filter folgen Sie den angegebenen Schritten:

- A) **Start, Systemsteuerung**, rechte Maustaste auf **Netzwerkverbindungen**, und auf **Öffnen** klicken.
- B) Rechte Maustaste auf die Netzwerkverbindung, die Sie konfigurieren wollen und dann **Eigenschaften**
- C) Unter **Eigenschaften von AdapterName** am **Allgemein** Tab, klicken Sie auf **Internetprotokoll (TCP/IP)**, und dann **Eigenschaften**.
- D) In dem **Eigenschaften von Internetprotokoll (TCP/IP)** Fenster auf **Erweitert** klicken.
- E) Auf den **Optionen** Tab klicken.
- F) Auf **TCP/IP-Filterung** klicken, und dann auf **Eigenschaften**.
- G) Klicken Sie in die **TCP/IP-Filterung aktivieren (alle Adapter)** Box.
- H) Unter **TCP/IP-Filterung** gibt es drei Spalten mit den folgenden Bezeichnungen:
 - **TCP-Ports**
 - **UDP-Ports**
 - **IP-Protokolle**

In jeder Spalte müssen Sie eine der folgenden Optionen auswählen:

- A) **Alle zulassen**. Wählen Sie diese Option, wenn Sie jeden TCP und UDP Verkehr erlauben.
- B) **Nur zulassen**. Wählen Sie diese Option, wenn sie nur ausgewählten TCP oder UDP Verkehr erlauben. Klicken Sie auf **Hinzufügen**, und dann geben Sie den entsprechenden Port in dem Fenster **Filter hinzufügen** an. Sie können nicht UDP oder TCP Verkehr blocken, in dem Sie **Nur zulassen** in der **IP-Protokolle** Spalte auswählen und IP Protokolle 6 und 17 angeben.

Hinweis: Wenn Sie TCP/IP-Filterung konfigurieren, erinnern Sie sich daran, welche Ports geblockt werden müssen. Für die LSASS Schwachstelle muss Inbound der Port TCP/445 geblockt werden.

[zum Anfang ^](#)

W9 Mail Client

W9.1 Beschreibung

Microsoft Outlook ist ein persönlicher Informationsmanager und E-Mail Programm für Microsoft Windows. Es ist hauptsächlich eine E-Mail Applikation, obwohl es auch Kalenderfunktionen, Aufgaben- und Kontaktmanagementfunktionen inkludiert. Wenn Outlook zusammen mit einem Exchange Server verwendet wird, können Groupware-Funktionen genutzt werden, z.B. werden Funktionen für mehrere User unterstützt, Meetingkoordination, freigegebene Kalender und Briefkästen für mehrere User.

Outlook Express (OE) ist eine kostenlose, jedoch mit geringerer Funktionalität ausgestattete Version von Outlook, die hauptsächlich Grundfunktionen von E-Mail und Kontaktmanagement bietet. Outlook Express ist mit dem Internet Explorer seit der IE Version 1.0 verbunden, welcher

wieder ein Bestandteil von Windows seit Windows 95 ist. Die aktuelle Version zur Zeit ist Outlook Express, Version 6.0 mit Service Pack 1 und kann kostenlos heruntergeladen werden. Durch die Integration der Produkte Internet Explorer und Outlook Express in andere Produkte wie Office, Backoffice und das Windows Betriebssystem hat es Microsoft erlaubt, gemeinsame Technologien und Programmcode plattformunabhängig zu verwenden. Unglücklicherweise entsteht dadurch ein "Single Point of Failure" wodurch die Auswirkungen, die durch einen Fehler entstehen können, erhöht werden.

Eines der Hauptziele von Microsoft war es, eine E-Mail und Informationsmanagementapplikation zu entwickeln, die intuitiv und leicht verwendbar ist. Leider stehen die eingebauten automatischen Eigenschaften im Konflikt mit den Sicherheitskontrollen (oft vom Enduser missachtet). Das führte zu vermehrten E-Mails mit Viren und Würmern, ebenso mit böartigem Code, die das lokale System kompromittierten und vielen anderen Attacken.

Potenzielle Sicherheitsbedrohungen der E-Mail Client inkludieren:

Infektion des Computers durch Viren und Würmer – böartiger Code, der sich durch Attachments und eingebettetes Scripting im Text verbreitet;

Spam – unaufgefordert gesendete kommerzielle E-Mail;

Web Beacons – Validation der E-Mail Adresse, ausgelöst durch das Öffnen der E-Mail durch den Empfänger.

Die zur Zeit gültigen Versionen von Outlook und Outlook Express können gegen die oben genannten Gefahren schützen, wenn sie richtig konfiguriert werden.

W9.2 Betroffene Betriebssysteme

Alle Versionen von Microsoft Windows haben Outlook Express in Verbindung mit dem Internet Explorers installiert und sind daher potenziell gefährdet.

Um die verwendete Version von OE zu eruieren, starten Sie den Internet Explorer, dann selektieren Sie das Hilfe Menü, und danach Info. Versionen unter 6 sollten sofort mit den verfügbaren Patches und Hotfixes aktualisiert werden.

Outlook ist nur dann auf einem System installiert, wenn das auch gezielt durchgeführt wird, entweder als eigene Applikation oder als Teil der Microsoft Office Suite. Folgende Outlook Versionen sind für Windows verfügbar:

- Outlook 95
- Outlook 97
- Outlook 98
- Outlook 2000, auch als Outlook 9 bekannt
- Outlook XP, auch als Outlook 10 oder Outlook 2002 bekannt
- Outlook 2003, auch als Outlook 11 bekannt

Versionen vor Outlook 2000 werden nicht mehr von Microsoft Corp. Unterstützt und es ist unbedingt anzuraten, diese Versionen so rasch als möglich auf unterstützte Versionen zu aktualisieren (Outlook 2003, 2002 oder 2000).

Alle Versionen von Outlook sollten die letztgültigen produktspezifischen Service Packs installiert

haben.

Derzeitige Versionen der Outlook Service Packs sind:

Outlook 2000 – Service Pack 3

Outlook XP (Outlook 2000) – Service Pack 3

Outlook 2003 hat bisher noch kein Service Pack

Um festzustellen, welche Version von Outlook installiert ist, starten Sie Outlook – und selektieren Sie Hilfe und Info.

Referenzen:

Outlook Express <http://www.microsoft.com/windows/oe/>

Outlook <http://www.microsoft.com/office/outlook/>

Produkt Lifecycle Daten [http://support.microsoft.com/default.aspx?id=fh; \[In\]; lifeprodo](http://support.microsoft.com/default.aspx?id=fh;[In];lifeprodo)

Microsoft Office Downloads <http://office.microsoft.com/OfficeUpdate>

W9.3 CVE/CAN Einträge

[CVE-1999-0967](#), [CVE-2000-0036](#), [CVE-2000-0567](#), [CVE-2000-0621](#), [CVE-2000-0662](#), [CVE-2000-0753](#), [CVE-2000-0788](#), [CVE-2001-0149](#), [CVE-2001-0340](#), [CVE-2001-0538](#), [CVE-2001-0660](#), [CVE-2001-0666](#), [CVE-2001-0726](#), [CVE-2001-1088](#), [CVE-2002-0152](#), [CVE-2002-0685](#), [CVE-2002-1056](#)

[CAN-1999-0004](#), [CAN-1999-0354](#), [CAN-1999-1016](#), [CAN-1999-1033](#), [CAN-1999-1164](#), [CAN-2000-0105](#), [CAN-2000-0216](#), [CAN-2000-0415](#), [CAN-2000-0524](#), [CAN-2000-0653](#), [CAN-2000-0756](#), [CAN-2001-0145](#), [CAN-2001-0945](#), [CAN-2001-0999](#), [CAN-2001-1325](#), [CAN-2002-0285](#), [CAN-2002-0481](#), [CAN-2002-0507](#), [CAN-2002-0637](#), [CAN-2002-1121](#), [CAN-2002-1179](#), [CAN-2002-1255](#), [CAN-2003-0007](#), [CAN-2003-0301](#), [CAN-2004-0121](#), [CAN-2004-0215](#), [CAN-2004-0284](#), [CAN-2004-0380](#), [CAN-2004-0501](#), [CAN-2004-0502](#), [CAN-2004-0503](#), [CAN-2004-0526](#)

W9.4 Wie Sie herausfinden, ob Sie betroffen sind

Alle Systeme, die den Internet Explorer installiert haben, haben auch Outlook Express installiert. Die manuelle Installation der Office Suite kann Outlook enthalten, neben anderen Produkten wie Word, Excel, PowerPoint oder Access.

Ein System hat Schwachstellen, wenn es entweder

- a. nicht auf dem aktuellen Stand ist. Das kann durch MS Update überprüft werden, oder
- b. die Sicherheitseinstellungen nicht sorgfältig durchgeführt wurden.

W9.5 Wie Sie sich dagegen schützen können

Es gibt eine Anzahl von Einstellungen die durchgeführt werden können um das Sicherheitsrisiko für Outlook und Outlook Express zu verringern.

Outlook / Outlook Express sicherer machen

Die standardmäßigen Einstellungen von Outlook und Outlook Express sind ziemlich offen. Es ist wichtig, diese Einstellungen sicherer zu machen und die Software immer aktuell zu halten.

Beispiele dafür sind:

Besuchen Sie regelmäßig die Windows Update Site <http://windowsupdate.microsoft.com>, und installieren Sie die kritischen Updates.

Schalten Sie die Vorschau aus, in dem Sie auf Ansicht > Layout klicken und die Vorschaufenster anzeigen Option ausschalten.

Stellen Sie die Sicherheitszonen-relevanten Einstellungen für eingehende E-Mail sicher ein.

Selektieren Sie Extras > Optionen > Sicherheit und klicken Sie den Knopf für Zone für eingeschränkte Sites (sicherer) und stellen Sie die Einstellungen auf hoch. Klicken Sie Übernehmen und OK um die Einstellungen zu übernehmen.

Schutz vor Attachments mit potenziellem bösertigen Code

Die Versionen von Outlook 2000 (SP3), Outlook 2002 (SP1 und spätere) und Outlook 2003 (alle Versionen) inkludieren einen effektiven Schutz gegen Anhänge (Attachments) die potentiellen bösertigen Code enthalten könnten. Es werden standardmäßig alle Attachments mit den Extensions .exe, .com, .vbs etc automatisch geblockt. Die Verwendung eines Archivierungstools wie WinZip oder eine andere Art Dateien zu senden (FTP, SCP) wird empfohlen wenn eine legitime Notwendigkeit besteht, ausführbare Dateien als Attachments zu versenden.

Eine komplette Liste der Extensions, die von Outlook geblockt werden kann in folgendem Artikel gefunden werden:

<http://www.microsoft.com/office/ork/2003/three/ch12/OutG07.htm>

Um die Liste der geblockten Dateitypen auszuweiten, ist es notwendig in der Registrierung folgende Änderungen vorzunehmen:

Klicken Sie Start, Ausführen, tippen Sie regedit, und dann OK.

Suchen und klicken Sie auf folgenden Registrierungsschlüssel:

Für Outlook 2003:

HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Security

Für Outlook XP/2002:

HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Security

Für Outlook 2000:

HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Outlook\Security

Im Menü unter Bearbeiten, Neu, Zeichenfolge anklicken.

Tippen Sie Level1Add und dann ENTER.

Im Menü unter Bearbeiten klicken Sie auf Ändern.

Tippen Sie <file_name_extensions> und dann OK.

Hinweis: *file_name_extensions* ist eine Liste von Filenamen Extensions für Attachments. Jede Attachment Filenamen Extension wird durch einen Strichpunkt getrennt. Z.B. tippen Sie .zip; .gif wenn .zip und .gif Dateien geblockt und nicht als Attachments angezeigt werden sollen.

Microsoft Technet Artikel KB837388 *How to configure Outlook to block additional attachment file name extensions* beschreibt diesen Prozess detailliert:

<http://support.microsoft.com/?kbid=837388>

Schutz vor SPAM (unaufgefordert gesendete kommerzielle E-Mail)

Outlook 2003 inkludiert einen effektiven Schutz gegen Spam. Um diesen Schutz zu konfigurieren öffnen Sie Outlook – selektieren Sie *Extras – Optionen – Junk E-Mail – Junk E-Mail Optionen*. Der *Optionen* Tab hat 4 Radioknöpfe, durch die der Grad der Anti-Spam Engine kontrolliert werden kann:

- Keine automatische Filterung – Spam wird nicht ausgefiltert;
- Niedrig (Standardeinstellung) – ziemlich wirkvolle Einstellung; verschiebt die meisten Junk E-Mails in den *Junk E-Mail* Folder und hat fast keine "False Positives";
- Hoch – aggressive Spamfilterung. Filtert fast alle Junk Mail (verschiebt es in den *Junk E-Mail* Folder), kann aber auch normale E-Mail als Spam erkennen. Wenn dieser Grad eingestellt ist empfiehlt es sich, regelmäßig den *Junk E-Mail* Folder nach legitimen E-Mails, die versehentlich als Spam gekennzeichnet wurden zu überprüfen;
- Nur sichere Absender und Empfänger – es werden nur Nachrichten von Personen und Domänen auf den Listen "*Sichere Absender*" und "*Sichere Empfänger*" in den Posteingang übermittelt. Diese Einstellung ist die höchste Spam Einstellung, erfordert aber einige Zeit und Anstrengung die "*Sicherer Absender*" Liste und die "*Sicherer Empfänger*" Liste mit allen legitimen Adressen und Domänen zu befüllen, die mit dem User kommunizieren können sollen.

Outlook Express und ältere Outlook Versionen haben keine effektiven Anti-Spam Funktionen, sie haben aber individuell einstellbare gesperrte Absenderlisten. Um das für Outlook Express zu aktivieren starten Sie Outlook Express – selektieren Sie *Extras – Nachrichtenregeln – Liste der blockierten Absender*.

Schutz vor böartigem Code, eingebettet im Text der E-Mail

E-Mail Nachrichten im rich-text Format (HTML, RTF) kann im Text böartigen Code eingebettet haben im Vergleich zu reinen textbasierender E-Mail, die keinen Code eingebettet haben kann. Der einfachste und effektivste Weg sich vor solchen böartigen Code zu schützen ist, E-Mails im Textformat zu lesen. Um das in Outlook 2003 zu konfigurieren starten Sie Outlook – selektieren Sie *Extras – Optionen* und selektieren Sie den *Einstellungen* Tab – dann *E-Mail Optionen* und selektieren Sie *Standardnachricht im Nur-Text-Format lesen*. Klicken Sie zweimal *OK*.

Schutz vor Web Beaconsing

Web Beaconsing ist eine Methode der Verifikation, dass eine E-Mail geöffnet wurde und daher der

Empfänger ein gültiges Ziel für zukünftigen Spam ist. Dabei wird ein kleines Bild (üblicherweise 1x1 Pixel) in der HTML formatierten Nachricht inkludiert. Diese Technik wird häufig von Spammern und Werbungsversendern verwendet. Zusätzlich zu der Bestätigung, dass ein User die E-Mail geöffnet hat können mit Web Beacons gewisse Informationen (IP Adresse, Sprache, Browser Version) über den User und das verwendete System gewonnen werden. Um Web Beacons im Outlook 2003 zu verhindern starten Sie Outlook – *Extras – Optionen* – selektieren Sie den Sicherheit Tab – klicken Sie auf den *Einstellungen für den automatischen Download ändern...* Knopf – und selektieren Sie *Bilder oder anderen externen Inhalt in HTML-Nachrichten nicht automatisch downloaden und Warnhinweis anzeigen, bevor externer Inhalt für das Bearbeiten, Weiterleiten oder Beantworten von Nachrichten abgerufen wird* – Klicken Sie zweimal auf *OK*.

Verhalten der Anwender

Da das menschliche Element oft das schwächste Glied im Sicherheitsprozess darstellt, ist es wichtig, einige „Best Practice“ Empfehlungen für den Umgang mit E-Mail zu befolgen.

Wenn Sie eine Anlage (Attachment) empfangen, sollten Sie immer zuerst eine Virenüberprüfung durchführen. Selbst wenn es von einem vertrauten Absender kommt, ist das wichtig. Mehr Information im Abschnitt „Anti-Virus“.

Nachdem Sie einen Anhang empfangen haben, speichern Sie diesen in einem eigenen Verzeichnis und nicht im Verzeichnis Eigenen Dokumente. Viele Viren verseuchen zuerst die Dateien in dem Verzeichnis, in dem sie gespeichert sind. Selektieren Sie ein anderes Verzeichnis oder sogar eine andere Partition, um empfangene Attachments von den restlichen Dateien zu trennen.

Öffnen Sie keine unerwarteten Anhänge, auch nicht von Freunden. Selbst in DOC oder XML Dateien können Programme eingebettet sein, die das System beschädigen können. Wenn Sie Dokumente mit anderen Microsoftprogrammen wie z.B. Word öffnen müssen, stellen Sie sicher, dass unter Extras > Optionen > Sicherheit die Einstellung für Zone für eingeschränkte Sites auf Hoch gestellt ist. Nur signierte Makros sollen erlaubt werden.

Überprüfen Sie immer die digitalen Signaturen die mit ausführbaren Programmen in Verbindung stehen um sicher zu stellen, dass die Dateienintegrität sicher gestellt ist und es auch von einer vertrauenswürdigen Site kommt.

Anti-Virus

Antivirenprogramme schützen vor den meisten Viren, Würmern, Trojanern und anderem böartigen Programmcode. Es ist absolut notwendig, die Signaturendatenbank immer auf dem letzten Stand zu halten. Mindestens 1 x wöchentlich (am besten täglich und automatisch) soll überprüft werden, ob neue Signaturen verfügbar sind. Nur durch regelmäßige Installation der neuesten Signaturen können Antivirenprogramme gegen die neuesten Angriffe schützen. Die meisten Antivirenprogramme haben einen Automatismus für diese Updates. Es ist auch klug, regelmäßig alle Dateien zu scannen und auf Viren zu überprüfen, egal um welche Dateientypen es sich dabei handelt.

Moderne Antivirenprogramme haben die Möglichkeit, alle eingehenden und ausgehenden E-Mails auf Viren zu überprüfen um sicherzustellen, dass böartige Scripts oder Programme blockiert werden, bevor sie Schaden anrichten können.

Es ist empfohlen, ein aktuelles Virenprogramm zu installieren, bevor Sie E-Mail oder andere Internet Dienste verwenden, da sich die meisten Viren über E-Mail in Form von Anhängen

verbreiten und bösartige Scripts schon durch das Lesen oder die Vorschau ausgeführt werden können.

Referenz:

Microsoft Antivirus Referenz <http://www.microsoft.com/security/protect/antivirus.asp>

Outlook und Outlook Express aktualisieren

Outlook Express wurde im Laufe der Zeit einige Male aktualisiert, um bessere Funktionalität, Stabilität und Sicherheit zu ermöglichen. Die aktuellste Version ist kostenlos unter <http://www.microsoft.com/windows/oe/> verfügbar.

Um sicher zu stellen, dass Outlook und andere Microsoft Programme aktuell sind, besuchen Sie die [Office Product Updates](#) Seite. Diese Site erkennt kritische und empfohlene Updates, die durchgeführt werden sollten.

Für detaillierte Information über Sicherheitsmerkmale in Office 2003 lesen Sie das [Office 2003 Security white paper](#).

Hinweis: Es sollte immer der zuständige Systemadministrator kontaktiert werden, bevor Änderungen durchgeführt werden. Administratoren finden detaillierte technische Informationen über Outlook E-Mail Sicherheitsupdates im [Office Resource Kit](#).

Deinstallation von Outlook und Outlook Express

Wenn ein anderes E-Mailprogramm verwendet wird, kann Outlook oder Outlook Express bedenkenlos deinstalliert werden.

Outlook auf allen Windows Versionen

Outlook kann deinstalliert werden in dem Sie Start > Einstellungen > Systemsteuerungen > Software und dann Outlook auswählen und deinstallieren anklicken.

Outlook Express auf Windows 98/ME

Outlook Express kann deinstalliert werden, in dem Sie Start > Einstellungen > Systemsteuerungen > Programme hinzufügen/entfernen anklicken. Wenn das Programm hinzufügen/entfernen Fenster erscheint, klicken Sie auf den Windows Setup Knopf und suchen Sie Microsoft Outlook Express und entfernen Sie die Markierung in der Box.

Klicken Sie auf Übernehmen und OK um die Einstellungen zu übernehmen und Outlook Express zu entfernen.

Outlook Express auf Windows 2000/XP oder aktualisierte Versionen des Internet Explorers

Das Entfernen von Outlook Express in Windows 2000/XP oder bei der Verwendung des aktuellen Internet Explorers ist komplexer. Die folgenden Anleitungen haben genaue Beschreibungen:

Windows 2000 mit Microsoft Outlook Express Version 5.x/6.0

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q263837>

Windows 98/Me und aktualisierte Microsoft Outlook Express Version 5.x/6.0

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q256219>

Hinweis: Microsoft Outlook Express könnte unbemerkt installiert werden, wenn Sie ein

Service Pack oder ein Betriebssystemupdate installieren.

[zum Anfang ^](#)

W10 Instant Messaging

W10.1 Beschreibung

Die Instant Messaging Technology hat sich in den letzten Jahren von einer einfachen Add-On Applikation, die es den Usern ermöglicht, schnell mit Familienmitgliedern oder Freunden in Kontakt zu treten hin zu einer Windows Betriebssystem Kernfunktion entwickelt. Sie wird oft für Geschäftskommunikation, operationalem Support und für enge Zusammenarbeit verwendet. Obwohl Produkte von Drittfirmen noch immer einen großen Marktanteil der verwendeten Instant Messaging (IM) Applikationen halten, ist der Trend nach integrierter Instant Messaging Funktionalität deutlich zu sehen. Dadurch kann es aber in Unternehmen zu einer Sicherheitsbedrohung kommen, und das obwohl Richtlinien für den angemessenen Gebrauch oder ein operatives Sicherheitsrahmenwerk vorhanden sind und die Verwendung dieser Funktionalität untersagt ist. Die Erkennung von Schwachstellen in diesen Applikationen stellt ebenfalls ein Sicherheitsrisiko dar, wenn die Organisation nicht über technische Maßnahmen, Sicherheitspersonal und geeignete Maßnahmen verfügt, die das Risiko verringern können.

Die bei meisten verbreiteten IM Applikation auf Windows Systemen sind Yahoo! Messenger (YM), AOL Messenger (AIM), MSN Messenger (MSN) und Windows Messenger (WM), der jetzt komplett in Windows XP Professional und Home Edition integriert ist. Die Möglichkeiten die diese Programme auf den Desktop bringt sind vielfältig und reichen von remote webbasierender E-Mail, Voice-Chat, Videokommunikation, Senden und Empfangen von Dateien bis über einfache textbasierenden Chat.

Es gibt einen Trend, zu "Multi Network" Messaging Programmen, die dem User mit einem zentralen Interface Zugang zu unterschiedlichen Netzwerken und Protokollen ermöglichen, wie Trillian und der vor kurzen entstandenen AOL, Yahoo! Und MSN Chat Allianz. Dadurch können alle drei Clients unabhängig vom Arbeitsplatz miteinander kommunizieren.

Es gibt immer mehr remote ausnutzbare Sicherheitsschwachstellen in diesen Programmen oder zugehörigen Abhängigkeiten und die Integrität und die Sicherheit der Netzwerke steigt direkt proportional mit der raschen Integration und dem Einsatz von Windows Systemen. Die Angriffsszenarien für Instant Messaging Schwachstellen sind sehr unterschiedlich und reichen von remote Buffer Overflow Attacken (RPC basierend, Paketfehlbildung), URI/böswillige Link basierende Attacken zu File Transfer Schwachstellen und ActiveX Exploits.

Sicherheitsschwachstellen in diesen Programmen sind typischerweise in folgenden Kategorien zu unterteilen:

- **Veraltete ActiveX Steuerelemente** – z.B. MSN Messenger "ResDLL" Buffer Overflow CAN-2002-0155, Yahoo! Voice Chat ActiveX Control Buffer Overflow Vulnerability (<http://www.securityfocus.com/bid/7561>), Yahoo! Webcam ActiveX Control Buffer Overrun Vulnerability (<http://www.securityfocus.com/bid/8634>).
- **URI Implementationsprobleme** – z.B. Yahoo! Messenger bösertige Script Ausführung CAN-2002-0032, Yahoo! Messenger URI Handler Buffer Overflow CAN-2002-0031.
- **Verschiedene Buffer Overflows, wie die durch File Transfer.** – z.B. MSN Messenger File Validation Failure CAN-2004-0122, Yahoo! Messenger "Imvironment" und "Message" Feld Buffer Overflows bzw. CAN-2002-0320 and CAN-2002-0320, AOL Instant Messenger TLV 0x2711 Packet Parsing Buffer Overflow CAN-2002-0005, VU#912659, Yahoo!

Messenger YAuto.DLL Open Buffer Overflow Vulnerability (<http://www.securityfocus.com/bid/9145>), AOL Instant Messenger Getfile Screenname Buffer Overrun Vulnerability (<http://www.securityfocus.com/bid/8825>)

- **RPC basierende Kommunikation** – z.B. MSN Messenger Buffer Overflow von einer RPC basierenden Meldung CAN-2003-0717

Diese Applikationen bringen nicht nur neue netzwerkbasierende Sicherheitsrisiken mit sich, sie stellen auch ein Risiko für das geistige Eigentum dar, speziell der Verlust der Vertraulichkeit, und der Produktionszeitverlust der Mitarbeiter. Obwohl die Verringerung der remote ausnutzbaren Sicherheitsschwächen von höchster Wichtigkeit ist, sind auch die Richtlinien für akzeptierten Verwendung und Eingangs- und Ausgangsfilterung des Netzwerkes von hoher Bedeutung. Damit kann sichergestellt werden, dass die Fehler, die durch Instant Messaging im Netzwerk entstehen können, verhindert werden.

W10.2 Betroffenen Betriebssysteme:

Windows 98, Windows ME, Windows 2000 und Professional, Windows XP und Windows 2003 können Microsoft Instant Messenger installiert haben. Alle Versionen von Windows XP haben den Instant Messenger im Betriebssystem integriert.

W10.3 CVE/CAN Einträge:

CVE-2002-0005[NOMINATE], CVE-2002-0032, CVE-2002-0155[NOMINATE], CVE-2002-0785
CAN-2002-0031[NOMINATE], CAN-2002-0228, CAN-2002-0320, CAN-2002-0362[NOMINATE],
CAN-2003-0717[NOMINATE], CAN-2004-0043, CAN-2002-1486[NOMINATE]

W10.4 : Wie Sie herausfinden, ob Sie betroffen sind

Um herauszufinden, welche Version von Microsoft Instant Messenger installiert ist, starten Sie die Applikation, und wählen Sie Info vom Help Menü aus. Versionen unter 6.2 sollten mit alle verfügbaren Sicherheitshotfixes aktualisiert werden.

W10.5 Wie Sie sich dagegen schützen können

(a) Stellen Sie sicher, dass die installierte Messenger Software wie Yahoo, MSN, AOL, Trillian etc immer up-to-date ist und alle Patches installiert sind.

(b) Stellen Sie sicher, dass die Windows Betriebssysteme mit MS 03-043 gepatcht sind, wodurch die Sicherheitsschwachstelle im Messenger Service behoben wird.

(c) Konfigurieren Sie Intrusion Prevention/Detection Systeme die einen Alarm auslösen, wenn File Transfer über Messaging Programme stattfindet.

(d) Wenn es die entsprechende Sicherheitsrichtlinie ermöglicht, sollten die folgenden Ports auf der Firewall geblockt werden. Beachten Sie dass dadurch kein kompletter Schutz erreicht werden kann, da einige Applikationen diese Firewallregeln umgehen können.

1863/tcp: Microsoft .NET Messenger, MSN Messenger

5050/tcp: Yahoo Messenger

6891/tcp: MSN Messenger File Transfers

5190-5193/tcp: AOL Instant Messenger

(e) Blockieren Sie den Zugang zu Webseiten die Links zu URLs enthalten wie "aim:" oder "ymsgr:". Das kann vor Ausnutzung eines Fehlers im URI Handlers schützen. Eine andere Möglichkeit ist die entsprechende Registrierungsschlüssel in "HKEY_CLASSES_ROOT" zu entfernen.

(f) Sperren Sie den Zugang zu Webseiten, die ActiveX Steuerelemente enthalten, die mit den Messenger Problemen in Verbindung stehen. Dadurch kann verhindert werden, dass die Fehler im ActiveX in Verbindung zu Messenger Programmen ausgenutzt werden.

[zum Anfang ^](#)

Top Schwachstellen von UNIX Systemen (U)

U1 BIND Domain Name System

U1.1 Beschreibung

Berkeley Internet Name Domain (BIND) ist die weltweit am meisten verwendete Implementierung der Domain Name Services (DNS). DNS ist ein wesentliches System, das die Auflösung von Hostnamen (z.B. www.sans.org) zu entsprechenden registrierten IP Adressen ermöglicht. Dass BIND nahezu überall verfügbar und ein grundlegender Dienst ist, hat diesen Dienst zu einem häufigen Ziel von Angriffen. Denial of Service (DoS)-Angriffe, die üblicherweise zu einem kompletten Verlust der Namensdienste für Websites führen, plagen schon seit langem BIND. Weitere Angriffsmöglichkeiten für unter anderem Buffer Overflows und Cache Poisoning wurden entdeckt. Obwohl das Entwicklerteam von BIND in der Vergangenheit rasch auf Schwachstellen reagiert oder diese behoben hat, sind noch immer eine extrem große Anzahl von veralteten oder verwundbaren Servern aktiv.

Eine Reihe von Faktoren tragen zu diesem Zustand bei, allen voran Administratoren, die nichts von sicherheitsbedingten Upgrades wissen, Systeme mit unnötigerweise aktiviertem BIND daemon („named“) und schlechte Konfigurationsdateien. Jeder dieser Faktoren kann zu Denial of Service, Buffer Overflows oder DNS Cache poisoning führen. Unter den aktuellsten Schwachstellen von BIND war eine Denial of Service-Möglichkeit, beschrieben in [CERT Advisory CA-2002-15](#). In diesem Fall könnte ein Angreifer bestimmte DNS-Pakete senden, die eine interne Überprüfung der Konsistenz erzwingen. Diese Überprüfung ist eine Schwachstelle und führt dazu, dass der BIND daemon sich selbst abschaltet. Eine weitere Schwachstelle ist ein Buffer Overflow, beschrieben in [CERT Advisory CA-2002-19](#). Hier kann ein Angreifer verwundbare Implementierungen der DNS Resolver Bibliotheken ausnützen. Durch Senden von bösartigen DNS-Antworten könnte ein Angreifer diese Schwachstelle ausnützen und beliebigen Code ausführen oder sogar Denial of Service verursachen.

Ein weiteres Risiko von verwundbaren BIND-Servern ist die Möglichkeit, diese zu kompromittieren und sie als Lager für unerwünschte Inhalte beziehungsweise als Ausgangspunkt für weitere bestimmungswidrige Aktivitäten zu verwenden.

U1.2 Betroffene Betriebssysteme

Nahezu alle UNIX- und Linux-Systeme sind mit einer Version von BIND ausgestattet. Die Installation von BIND kann bei Server-Installationen beabsichtigt sein, oder unbeabsichtigt bei allgemeinen bzw. Standard-Installationen. Auch für Windows gibt es binäre Versionen von BIND.

U1.3 CVE/CAN Einträge

[CVE-1999-0009](#), [CVE-1999-0024](#), [CVE-1999-0184](#), [CVE-1999-0833](#), [CVE-1999-0837](#), [CVE-1999-0835](#), [CVE-1999-0848](#), [CVE-1999-0849](#), [CVE-1999-0851](#), [CVE-2000-0887](#),

[CVE-2000-0888](#), [CVE-2001-0010](#), [CVE-2001-0011](#), [CVE-2001-0012](#), [CVE-2001-0013](#)

[CAN-2002-0029](#), [CAN-2002-0400](#), [CAN-2002-0651](#), [CAN-2002-0684](#), [CAN-2002-1219](#),
[CAN-2002-1220](#), [CAN-2002-1221](#), [CAN-2003-0914](#)

U1.4 Wie Sie herausfinden, ob Sie betroffen sind

Jeder DNS Server, der eine Version von BIND verwendet, die mit dem Betriebssystem gebündelt kommt, sollte mit den aktuellen Patches des entsprechenden Herstellers versehen werden. Wenn die verwendete Version aus dem Source-Code des [Internet Software Consortium \(ISC\)](#) kompiliert wurde, sollte sichergestellt werden, dass es sich dabei um die aktuellste Version handelt. Veraltete oder ungepatchte Versionen von BIND sind höchstwahrscheinlich verwundbar.

In den meisten Implementierungen zeigt der Befehl „named -v“ die installierte BIND Version als X.Y.Z, wobei X die Hauptversion, Y die Unterversion und Z der Patchlevel ist. Derzeit sind die Versionen 4, 8 und 9 die Hauptversionen. Wird ein selbst kompilierter BIND Server verwendet, sollte man die Version 4 vermeiden und stattdessen die Version 9 verwenden. Sie können die neuesten Quelltexte, Version 9.3.0rc2, von [ISC](#) beziehen.

Ein proaktiver Ansatz, die Sicherheit von BIND zu erhalten, ist, angepasste Berichte über Warnungen und Schwachstellen zu abonnieren, wie zum Beispiel bei [SANS](#), oder indem man zum Beispiel bei den bei [OSVDB](#) veröffentlichten Empfehlungen am Laufenden bleibt. Zusätzlich zu den Sicherheitsbenachrichtigungen kann ein aktualisierter Scanner von Schwachstellen sehr wirksam bei der Diagnose von Schwachstellen innerhalb von DNS Systemen sein.

U1.5 Wie Sie sich dagegen schützen können

- **Allgemeiner Schutz vor BIND Schwachstellen:**
 1. Deaktivieren Sie den BIND Dienst (genannt „named“) auf allen Systemen, die nicht bestimmt und berechtigt sind, als DNS Server zu laufen.
 2. Spielen Sie alle Patches des Herstellers ein oder steigen Sie auf die neueste Version der DNS-Server um. Für detaillierte Informationen über das Härten einer BIND Installation, lesen Sie bitte in die Artikel über das Sichern von Name Services, die in der [UNIX Security Checklist](#) des CERT zitiert werden.
 3. Um automatisierte Angriffe oder Scans eines Systems zu erschweren, verstecken Sie die Versions- Information im Banner in BIND, indem Sie die aktuelle Version von BIND mit einer falschen Versionsnummer im „file options“ Feld der Datei „named.conf“ ersetzen.
 4. Erlauben Sie Zone Transfers nur zu Secondary DNS Servern in vertrauenswürdigen Domänen. Deaktivieren Sie Zone Transfers zu über- oder untergeordneten Domänen, indem Sie stattdessen delegieren oder weiterleiten.
 5. Gefängnis: Um zu verhindern, dass ein kompromittierter BIND Dienst das gesamte System öffnet, schränken Sie BIND so ein, dass er als nicht-privilegiertes User in einem `chroot()` Verzeichnis läuft. Für BIND 9, schauen Sie bitte in <http://www.losurs.org/docs/howto/Chroot-BIND.html>.
 6. Deaktivieren Sie Rekursion und Glue-Fetching um sich gegen DNS Cache Poisoning zu verteidigen.
- **Schutz gegen frisch entdeckte Schwachstellen von BIND:**
 1. Die Denial of Service Schwachstelle von ISC BIND 9:
<http://www.cert.org/advisories/CA-2002-15.html>
 2. Verschiedene Denial of Service Schwachstellen von ISC BIND 8:
<http://www.isc.org/products/BIND/bind-security.html>
 3. Cache Poisoning durch negative Antworten:

<http://www.kb.cert.org/vuls/id/734644>

Es gibt viele ausgezeichnete Anleitungen zum Härten von BIND. Eine hervorragende Anleitung zum Härten von BIND auf Solaris Systemen sowie weitere Referenzen auf BIND Dokumentation können in [Running the BIND9 DNS Server Securely](#) und in den Archive von Arbeiten über die Sicherheit von BIND bei [Afentis](#) gefunden werden. Man kann weitere Dokumentation, die allgemeine BIND Security-Praktiken behandelt bei http://www.linuxsecurity.com/resource_files/server_security/securing_an_internet_name_server.pdf finden. Administratoren können sich auch nach Alternativen zu BIND wie zum Beispiel DJBDNS zu finden bei <http://cr.yip.to/djbdns.html> umschauen.

[zum Anfang ^](#)

U2 Webserver

U2.1 Beschreibung

HTTP-Datenverkehr ist die mit Abstand häufigste Verwendung des öffentlichen Internets. Unix Webserver wie Apache und der Sun Java System Web Server (früher: iPlanet) liefern den Großteil dieses Verkehrs und verdienen daher besonderes Augenmerk in Sachen Sicherheit. Das inkludiert Schwachstellen der Server selbst ebenso wie von Erweiterungsmodulen, Standard-/Beispiel-/Test-CGI-Skripts, PHP Bugs und diversen anderen Angriffsmöglichkeiten.

Während viele dieser Möglichkeiten existieren, ist die am weitesten verbreitete Ursache von beeinträchtigten Unix Webservern das Ergebnis von schlecht konfigurierten oder schlecht gewarteten Systemen. Diese Beeinträchtigungen reichen von Denial of Service über Web Site Defacement bis zum kompletten Root-Zugang für den Angreifer.

Verschiedene Hersteller und Open-Source-Projekte stellen Best-Practice Konfigurationen und fortlaufende Security-Updates für ihre Produkte zur Verfügung, und es ist dabei wesentlich, dass jeder Administrator von Webservern ein wachsames Auge darauf hat. Dabei ist es wichtig zu realisieren, dass die meisten Webserver durch bereits bekannte, öffentlich verfügbare Attacken, die Schwachstellen ausnutzen, für die es schon lange Patches oder Workarounds gibt, beeinträchtigt werden.

U2.2 Betroffene Betriebssysteme

Auf allen UNIX-Systemen können HTTP-Server laufen. Viele Linux und UNIX Varianten haben den Apache bereits als Standard installiert und aktiviert. Weiters können sowohl Apache als auch iPlanet/Java System auf einem Rechner mit einem anderen Betriebssystem wie zum Beispiel Windows laufen, und man kann davon ausgehen, dass auch diese Versionen von vielen dieser Probleme betroffen sind.

U2.3 CVE/CAN Einträge

Wie bereits erwähnt, können sowohl Apache als auch iPlanet/Java System auf mehreren Plattformen laufen. Anwender dieser Server sollten die entsprechenden „CVE/CAN-Einträge“ dieser Liste sowie die Windows Liste unter Punkt W1.3 durchgehen um sicherzustellen, dass alle möglichen Schwachstellen berücksichtigt werden.

Apache

[CVE-1999-0021](#), [CVE-1999-0066](#), [CVE-1999-0067](#), [CVE-1999-0070](#), [CVE-1999-0146](#),
[CVE-1999-0172](#), [CVE-1999-0174](#), [CVE-1999-0237](#), [CVE-1999-0260](#), [CVE-1999-0262](#),
[CVE-1999-0264](#), [CVE-1999-0266](#), [CVE-1999-0509](#), [CVE-2000-0010](#), [CVE-2000-0208](#),

[CVE-2000-0287](#), [CVE-2000-0941](#), [CVE-2002-0061](#), [CVE-2002-0082](#), [CVE-2002-0392](#)

[CAN-2000-0832](#), [CAN-2002-0513](#), [CAN-2002-0655](#), [CAN-2002-0656](#), [CAN-2002-0657](#),
[CAN-2002-0682](#), [CAN-2003-0132](#), [CAN-2003-0189](#), [CAN-2003-0192](#), [CAN-2003-0254](#),
[CAN-2004-0488](#), [CAN-2004-0492](#)

iPlanet/Sun Java System Web Server
[CVE-2000-1077](#), [CVE-2002-0845](#)

[CAN-2001-0419](#), [CAN-2001-0746](#), [CAN-2001-0747](#), [CAN-2002-0686](#), [CAN-2002-1315](#),
[CAN-2002-1316](#)

OpenSSL
[CAN-2003-0543](#), [CAN-2003-0544](#), [CAN-2003-0545](#)

PHP
[CVE-2002-0081](#)

[CAN-2003-0097](#), [CAN-2004-0594](#)

Andere
[CAN-2004-0529](#), [CAN-2004-0734](#)

U2.4 Wie Sie herausfinden, ob Sie betroffen sind

Von allen ungepatchten oder Standardwebservern sollte angenommen werden, dass sie Schwachstellen haben. Der beste Weg um bei Sicherheitsfragen für ein bestimmtes Produkt auf dem neuesten Stand zu bleiben, ist, die Sicherheitsinformationsseiten der jeweiligen Hersteller zu lesen. Beispiele für solche Seiten sind unter anderem:

Apache HTTP Server [Main Page & Security Report](#) (Enthält Links zu [ApacheWeek](#))

[Sun Web, Portal, & Directory Servers Download Center & BigAdmin Portal](#)

PHP [Home Page](#) and [Downloads](#)

[OpenSSL](#)

Jede aufgezählte Schwachstelle sollte *so rasch wie möglich* behoben werden. Das Zeitfenster zwischen der Ankündigung einer Schwachstelle und der öffentlichen Verfügbarkeit eines Angriffswerkzeugs, und weiter noch der Freisetzung eines Wurms, der diese Schwachstelle ausnützt, wird immer kleiner.

Um den Prozess der Suche nach Schwachstellen zu erleichtern, kann man sich beliebiger Schwachstellenscanner bedienen. Zu diesen gehören zum Beispiel [Nessus](#) und [SARA](#) (beide Open-Source) oder die [Gratis-Werkzeuge](#) oder [kommerziellen Scanner](#) von eEye. Diese Scans sollten netzwerkweit laufen um es Administratoren zu ermöglichen, das Risiko ausgehend von bekannten und unbekanntem Webservern abzuschätzen.

U2.5 Wie Sie sich dagegen schützen können

1. Stellen Sie sicher, dass alle Webserver den aktuellsten Patch-Level verwenden. In „Wie Sie herausfinden, ob Sie betroffen sind“ finden Sie links zu den entsprechenden Seiten der Hersteller.
2. Deaktivieren Sie alle nicht benötigten Funktionen des Servers. Besonders wichtig ist dabei CGI Zugriff, php-Unterstützung, mod_ssl und mod_proxy (Apache). Deaktivieren Sie diese als Standard und aktivieren Sie sie nur, wenn sie wirklich benötigt werden!
 - Wenn PHP, CGI, SSI oder andere Scripting Sprachen benötigt werden, überlegen Sie die Verwendung von suEXEC. suEXEC erlaubt, unter Apache Skripts mit einer anderen Userid als der Apache Userid zu verwenden.
 - **WARNUNG:** Es ist wichtig, dass suEXEC zur Gänze verstanden wird. Wenn es ungenau verwendet wird, dann können so neue Sicherheitslücken entstehen.
 1. Für Apache 1.3.x siehe <http://httpd.apache.org/docs/suexec.html>
 2. Für Apache 2.0.x siehe <http://httpd.apache.org/docs-2.0/suexec.html>
3. Schützen Sie den Inhalt von cgi-bin und anderen Skript-Verzeichnissen. Alle Beispiels- und Standardskripts sollten entfernt werden.
4. Schützen von PHP:

Dies ist ein weites Gebiet für sich allein. Was folgt, liefert ein paar gute Ausgangspunkte um sicherzustellen, dass Ihre PHP-Installation sicher ist.

 - Deaktivieren Sie Parameter, die PHP veranlassen, Informationen im HTTP Header preiszugeben.
 - Stellen Sie sicher, dass PHP im sicheren Modus (safe mode) läuft.

Detaillierte Informationen finden Sie auf:

<http://www.securityfocus.com/printable/infocus/1706>

5. Zusätzliche Module können beim Absichern von Apache helfen. Das mod_security (www.modsecurity.org) Modul kann beim Schutz vor Cross Site Scripting (XSS) und SQL Injection helfen. Detaillierte Implementierungsanweisungen können auf deren Website gefunden werden.
6. Skripts nach Schwachstellen inklusive XSS und SQL Injection zu durchsuchen ist ebenfalls wichtig. Es gibt ein paar Open-Source-Werkzeuge, die dabei unterstützen. Nikto (zu finden auf <http://www.cirt.net/code/nikto.shtml>) ist eines der vollständigeren CGI Scanning Werkzeuge.
7. Man sollte auch überlegen, HTTP-Server in einer chroot-Umgebung zu betreiben. Wenn ein HTTP-Server in einer chroot-Umgebung gestartet ist, kann er auf keinen Teil der Verzeichnisstruktur des Betriebssystems außerhalb des chroot-Verzeichnisbaums zugreifen. Das kann oft helfen, Angriffe zu verhindern. Zum Beispiel könnte bei einer Attacke eine Shell aufgerufen werden, und da /bin/sh sehr wahrscheinlich nicht (und das sollte der Fall sein) innerhalb der chroot-Umgebung läuft, wäre diese Attacke nutzlos. **WARNUNG:** Chrooting kann sich nachteilig auf CGI, PHP, Datenbanken und andere Module oder Kommunikation, die benötigen kann, dass aus der Umgebung des Webserver auf externe Bibliotheken oder Programme zugegriffen wird, auswirken. Da es zahlreiche Methoden für chroot gibt, sollte die Dokumentation der Software gelesen werden. Weitere Informationen können Sie bei den folgenden Links finden.
 - <http://www.w3.org/Security/Faq/wwwsf3.html#SVR-Q5>
 - <http://www.modsecurity.org/documentation/apache-internal-chroot.html>
 - http://www.sun.com/software/whitepapers/webserver/wp_ws_security.pdf
8. Lassen Sie Webserver nicht als root laufen. Eine eigene UserID und Gruppe mit minimalen rechten sollte für diesen Zweck angelegt werden, und keine anderen Prozesse sollten mit dieser Userid oder Gruppe laufen (z.B. starten Sie Apache als User "apache" statt als User "nobody").
9. Reduzieren Sie die veröffentlichten Serverinformationen.

Obwohl dieser Vorschlag dazu tendiert auf Widerspruch von Leuten stößt, die der Meinung sind, dass "Security by Obscurity" keine akzeptable Methode zur Risikominimierung ist, und eine Anzahl von Angriffsversuchen im öffentlichen Internet durch stures Ausprobieren stattfindet (erkennbar an der Tatsache, dass in vielen Apache Logs IIS-Angriffsversuche zu finden sind), gibt es dennoch einige Exploits, die aufgrund von Header-Informationen aktiv werden.

- Um die Standard-Apache HTTP-Antworten zu modifizieren.
 1. Für Apache 1.3.x siehe <http://httpd.apache.org/docs/mod/core.html#servertokens>
<http://httpd.apache.org/docs/mod/core.html#serversignature>.
 2. Für Apache 2.0.x siehe <http://httpd.apache.org/docs-2.0/en/mod/core.html#servertokens>.
 - Stellen Sie sicher, dass mod_info nicht aus dem Internet sichtbar ist.
 - Directory indexing sollte deaktiviert sein.
10. Effizientes und gründliches Logging ist wesentlich um effektiv potentielle Sicherheitsprobleme oder merkwürdiges Verhalten des Webservers zu entdecken. Es ist empfehlenswert, regelmäßig Logs zu rotieren und alte Logs zu archivieren. Das sorgt für leichter handhabbare Logfilegrößen und macht es einfacher sie zu durchforsten, wenn notwendig.

Verschiedene Informationen bezüglich Logformate und –rotation finden Sie hier:

- Für Apache 1.3.x siehe: <http://httpd.apache.org/docs/logs.html>
- Für Apache 2.0.x siehe: <http://httpd.apache.org/docs-2.0/logs.html>

In einigen Szenarios mag der Inhalt dieser Logs nicht ausreichend sein. Besonders, wenn PHP, CGI oder andere Skript-Sprachen verwendet werden, ist es eine gute Idee, GET und POST-Daten mitzuloggen. Das kann wichtige Daten und Beweise im Falle eines Sicherheitsproblems liefern. Die Aufzeichnung von GET und POST-Daten kann mit dem mod_security (f. Apache) implementiert werden.

- <http://www.modsecurity.org>
- <http://www.securityfocus.com/infocus/1706>

[zum Anfang ^](#)

U3 Authentisierung

U3.1 Beschreibung

Passwörter, Passphrasen und/oder Sicherheitscode werden in beinahe jeder Interaktion zwischen Anwendern und Informationssystemen verwendet. Die meisten Arten der Authentifizierung von Benutzern sowie des Schutzes von Dateien und Daten hängt stark von Passwörtern ab, die von Anwendern oder Herstellern gewählt wurden. Weiters, da ordnungsgemäß durchgeführte Anmeldungen oft nicht aufgezeichnet werden beziehungsweise normalerweise unverdächtig sind, ist ein kompromittiertes Passwort eine Gelegenheit, Systeme nahezu unentdeckt zu erkunden. Ein Angreifer im Besitz eines gültigen User Passworts hätte kompletten Zugang zu allen Ressourcen, die dem jeweiligen Benutzer zur Verfügung stehen und hätte es wesentlich leichter, auf andere Accounts oder Maschinen in der Nähe zuzugreifen oder sogar root auf diesem System zu werden. Trotz dieser Bedrohung sind Accounts von Benutzern und Administratoren mit schwachen oder nicht existenten Passwörtern noch immer sehr weit verbreitet. Weiters sind Organisationen mit gut entwickelten und durchgesetzten Passwort-Richtlinien noch immer sehr selten.

Die häufigsten Schwachstellen von Passwörtern sind: (a) Benutzerkonten ohne oder nur mit schwachen Passwörtern; (b) Benutzerkonten mit weithin bekannten oder offen angezeigten Passwörtern; (c) Benutzerkonten mit Administratorenrechten, die vom Betriebssystem oder Software erzeugt wurden und keine oder allgemein bekannte, schwache Passwörter haben; und (d) schwache oder bekannte Algorithmen zum Hashen von Passwörtern und/oder Passwort-Hashes die schwach abgesichert für jeden sichtbar abgespeichert werden.

Die beste Verteidigung gegen all diese Schwachstellen ist eine gut entwickelte Passwortrichtlinie, die Folgendes enthält: genaue Anleitungen für Benutzer zur Erzeugung von starken Passwörtern; explizite Regeln für Benutzer um sicherzustellen, dass ihre Passwörter sicher bleiben und regelmäßig geändert werden; Definition eines Prozess für die IT-Mitarbeiter um schwache/unsichere/allgemein bekannte BZW. Standardpasswörter sofort zu ersetzen und um inaktive Accounts zu sperren bzw. nicht benutzte Accounts zu löschen; und Definition eines proaktiven und regelmäßig durchgeführten Prozesses zum Überprüfen aller Passwörter auf Ihre Stärke und Komplexität; Löschen von nicht benötigten Standard Benutzer- und Administratorkonten; und regelmäßige Überprüfung der Zugriffs-/Anmeldelogs. Ein allgemeiner Unix Configuration Guide ist auf http://www.cert.org/tech_tips/unix_configuration_guidelines.html verfügbar.

U3.2 Betroffene Betriebssysteme

Jedes Betriebssystem beziehungsweise jede Anwendung auf einer beliebigen Plattform wo sich ein Anwender durch Userid und Passwort anmelden.

U3.3 CVE/CAN Einträge

[CVE-1999-0502](#), [CVE-2001-0259](#), [CVE-2001-0553](#), [CVE-2001-0978](#), [CVE-2001-1017](#), [CVE-2001-1147](#), [CVE-2001-1175](#)

[CAN-1999-0501](#), [CAN-1999-1029](#), [CAN-2004-0243](#), [CAN-2004-0653](#)

U3.4 Wie Sie herausfinden, ob Sie betroffen sind

1. Suche nach allgemeinen Benutzerkonten

- Gibt es allgemein bekannte Benutzeraccounts die von mehreren Personen oder von externen Mitarbeitern gemeinsam benutzt werden und/oder frei sichtbare Passwörter, auf Zetteln auf dem Schreibtisch oder am Monitor, so sind das offensichtliche Wege in Ihr Netzwerk für jeden, der physischen Zugang zu diesen Systemen hat.

2. Suche nach schwache Passwörtern oder schwachen Passwort-Strategien

- Wenn man neue Benutzerkonten mit dem selben Initialpasswort oder einem leicht erratbaren Initialpasswort versieht (sogar wenn dieses nach dem ersten Login geändert werden muss), so bietet auch das einem Angreifer eine zeitlich begrenzte Möglichkeit, Zugriff auf das System zu erlangen.
- Finden Sie heraus, ob Passworthashes in `/etc/password` oder in `/etc/shadow` auf den lokalen Systemen gespeichert werden. Die Datei `/etc/password` muss von allen Benutzern Ihres Netzwerks gelesen werden können um die Anmeldung des Benutzers durchzuführen. Wenn allerdings diese Datei auch die Passworthashes enthält, kann jeder Benutzer mit Zugang zu diesem System diese Haschwerte lesen und versuchen, sie mit einem Passwortcracker zu knacken. Die Datei `/etc/shadow` wurde so angelegt, dass sie nur von

root lesbar ist und sollte, wo verfügbar, dazu verwendet werden, Hashwerte zu speichern. Werden Ihre lokalen Accounts nicht durch /etc/shadow geschützt, dann ist das Risiko für diese Passwörter sehr hoch. Die meisten neuen Betriebssysteme verwenden standardgemäß /etc/shadow um Passworthashes zu speichern, sofern das nicht bei der Installation geändert wurde. Bei manchen Installationen ist es auch möglich, dass Sie den MD5-Algorithmus zum Hashen Ihrer Passwörter verwenden können, was sicherer ist als der ältere crypt-Algorithmus.

3. NIS-Umgebungen

NIS ist eine Sammlung von Diensten, die als Datenbank dienen um Ortsinformationen, genannt Maps, für andere Netzwerkdienste, wie zum Beispiel Network File System (NFS), zur Verfügung zu stellen. Aufgrund ihrer Konstruktion enthalten NIS Konfigurationsdateien NIS Passworthashes, wodurch die Hashwerte von allen Anwendern gelesen werden können und die Passwörter einem gewissen Risiko unterliegen. Das kann bei manchen Implementierungen von LDAP als Netzwerkanmeldedienst der Fall sein. Neuere Implementierungen von NIS wie NIS+ oder LDAP sind im Allgemeinen strenger beim Schutz von Passworthashes, sofern diese nicht bei der Installation geändert wurden. Allerdings können diese neueren Implementierungen schwieriger einzurichten und zu konfigurieren sein, was vor deren Verwendung abschrecken könnte.

4. Allgemeine Überlegungen

Sogar wenn Passworthashes durch /etc/shadow oder andere Implementierungen geschützt sind, können Passwörter noch immer auf andere Methoden erraten werden. Es gibt andere weit verbreitete Arten von Passwortschwächen, inklusive der Existenz von nicht mehr benutzten Accounts von Benutzern, die das Unternehmen verlassen haben. Üblicherweise vernachlässigen Organisationen das Schließen und Entfernen von alten Benutzerkonten solange es keine Prozeduren oder besonders gewissenhafte Administratoren gibt.

Standardinstallationen von Betriebssystemen oder Netzwerkanwendungen (durchgeführt entweder vom Hersteller oder durch einen Administrator) können eine große Zahl von nicht benötigten und nicht benutzten Diensten mit sich bringen. In vielen Fällen führt die Ungewissheit darüber, was ein Betriebssystem oder eine Anwendung benötigt, dazu dass Hersteller oder Administratoren alles installieren für den Fall, dass es später einmal benötigt wird. Das erleichtert den Installationsprozess wesentlich, bringt aber auch eine Vielzahl von nicht benötigten Diensten und Accounts mit Standard-, schwachen oder bekannten Passwörtern mit sich.

Weiters sind Passwörter, die im Klartext über das Netzwerk gesendet werden, wie zum Beispiel bei Telnet, ftp oder http, dem Risiko ausgesetzt, unauthorisiert mitgesniffelt zu werden. Die Verwendung von verschlüsselten Verbindungen wie zum Beispiel mit OpenSSH oder SSL können verwendet werden um Passwörter vor allen, die die Verbindung ausspionieren wollen, zu schützen.

U3.5 Wie Sie sich dagegen schützen können

Die beste und geeignetste Verteidigung gegen Schwächen von Passwörtern sind strenge Vorschriften mit detaillierten Anweisungen, die zu einem vernünftigen Umgang mit Passwörtern führen und auch regelmäßige proaktive Überprüfungen der Passwörter durch die Systemadministratoren mit voller Unterstützung durch das Unternehmen enthält. Die folgenden

Schritte sollten als Richtlinie für ein gute Passwortvorschriften verwendet werden:

1. **Stellen Sie sicher, dass die alle Passwörter stark sind.** Mit genug Hardware und genügend Zeit kann jedes Passwort mit Brute Force geknackt werden. Von Angreifern verwendete Passwortcracker benutzen Wörterbuch-Attacken. Da die üblichen Passwortverschlüsselungsverfahren weit reichend bekannt sind, vergleichen Knackprogramme einfach die verschlüsselte Form des Zielpasswortes mit der verschlüsselten Form aller Wörter eines Wörterbuchs (in einigen Sprachen) und mit der verschlüsselten Form von Eigennamen sowie Permutationen von beiden. Daher sind Passwörter, die in irgendeiner Weise einem Wort (oder Wörtern in beinahe jeder bekannten Sprache) ähnlich sind, sehr anfällig für eine Wörterbuch-Attacke. Viele Unternehmen weisen ihre Anwender an, Passwörter durch Kombinieren von alphanumerischen Zeichen oder Sonderzeichen zu erzeugen, und die Anwender halten sich meistens daran, indem sie ein Wort (z.B.: Passwort) nehmen und Buchstaben durch Ziffern oder Sonderzeichen ersetzen (z.B.: Pa\$\$w0rt). Solche Permutationen können nicht gegen Wörterbuch-Attacken schützen: Pa\$\$w0rt wird genauso wahrscheinlich geknackt wie Passwort.

Ein gutes Passwort darf daher kein Wort und keinen Namen als Ursprung haben. Strenge Passwortvorschriften sollten Benutzer anweisen Passwörter aus etwas Zufälligerem, wie einem Satz, oder einem längerem Titel eines Buchs oder eines Liedes, zu erzeugen. Durch Verknüpfen eines längeren Satzes in eine Kette (das heißt: man nimmt den ersten Buchstaben jedes Wortes des Satzes (vorzugsweise mit Klein- und Großschreibung), oder man ersetzt ein Wort durch ein Sonderzeichen im ursprünglichen Satz und/oder ersetzt alle Vokale im zusammengefügteten Satz durch Sonderzeichen, usw.) können Anwender ausreichend lange Passwörter erzeugen, die alphanumerische Zeichen und Sonderzeichen so kombinieren, dass es schwer wird mit Wörterbuchattacken erfolgreich zu sein. Wenn der ursprüngliche Satz leicht zu merken war, dann sollte es das Passwort auch sein.

Sobald die Benutzer geeignete Anweisungen zur Erzeugung guter Passwörter erhalten haben, sollten detaillierte Verfahren vorhanden sein um sicher zu stellen, dass diese Anleitungen auch befolgt werden. Am besten macht man das indem man das Passwort bei der Passwortänderung überprüft. Die meisten UNIX/Linux-Varianten können Npasswd als Frontend verwenden um eingegebene Passwörter mit den Passwortvorschriften zu vergleichen. Systeme mit PAM können so erweitert werden, dass sie cracklib (Bibliotheken, enthalten in Crack) verwenden um Passwörter bei deren Erzeugung zu überprüfen. Die meisten neuen Systeme mit PAM können auch so konfiguriert werden, dass sie schlecht Passwörter, die nicht bestimmte Voraussetzungen erfüllen ablehnen.

Ist es nicht möglich, Passwörter bei ihrer Eingabe mit Tools wie Npasswd oder Bibliotheken, die PAM verwenden, und Wörterbuchbibliotheken zu untersuchen, dann sollten Knackprogramme vom Systembetreuer auf einen nicht vernetzten Rechner als Teil einer proaktiven Prozedur laufen. Werkzeuge, die auch von potentiellen Angreifern verwendet werden, sind generell die beste Wahl. Auf einem UNIX/Linux-System wären das unter anderem Crack und John the Ripper.

Bitte beachten Sie: Verwenden Sie nie einen Passwortscanner, sogar auf Systemen auf welchen Sie root-ähnliche Rechte haben, ohne explizite und vorzugsweise schriftliche Erlaubnis Ihres Arbeitgebers. Administratoren mit den wohlwollendsten aller Absichten wurden schon entlassen, weil sie Passwortknacker verwendet haben ohne dafür autorisiert zu sein. Diese Genehmigung sollte ein schriftliches Dokument sein, das Teil der strengen

Passwortvorschriften des Unternehmens ist und regelmäßige Überprüfungen der Passwörter erlaubt/anordnet.

Sobald Sie die Genehmigung, Passwortknacker zu verwenden, erhalten haben, sollten Sie dies regelmäßig auf einem physisch geschützten und gesicherten System durchführen. Die Werkzeuge auf der Maschine sollten niemandem außer den autorisierten Systembetreuern zugänglich sein. Anwender, deren Passwörter geknackt wurden sollten vertraulich benachrichtigt werden und Anleitungen erhalten, wie sie bessere Passwörter wählen können. Sowohl Administratoren als auch das Management sollten gemeinsam diese Benachrichtigungsprozeduren als Teil der Passwortvorschriften des Unternehmens entwickeln, sodass das Management beraten oder unterstützen kann falls Anwender nicht auf diese Benachrichtigungen reagieren.

Andere Möglichkeiten um sich vor nichtexistenten oder schwachen Passwörtern zu schützen bzw. um Prozeduren der Passwortvorschriften zu erhalten sind (a) Verwenden einer alternativen Art der Anmeldung wie Passwörter erzeugende Token oder biometrische Verfahren. Diese sind effektiv, wenn Sie Probleme mit schwachen Passwörtern haben und können als weitere Art der Anmeldung verwendet werden. Dabei sollte beachtet werden, dass einige Passwörter erzeugende Token Prozeduren benötigen, die sicherstellen, dass sie nicht von nicht berechtigten Personen verwendet werden können, und dass sie im Falle eines Diebstahls rasch vom System abgelehnt werden. Die Biometrie ist noch nicht ganz ausgereift, und abhängig vom Anmeldeverfahren (z.B.: Fingerabdrücke oder Gesichtserkennung) ist die Technik noch nicht perfekt und es kann durchaus zu Fehlern kommen. (b) Es gibt einige Werkzeuge von Drittherstellern (frei und kommerziell), die Ihnen helfen gute Passwortvorschriften zu verwalten.

2. **Schützen Sie starke Passwörter.** Wenn Sie Passworthashes in /etc/passwd speichern, aktualisieren Sie Ihr System, dass es /etc/shadow verwendet. Wenn Ihr System NIS oder LDAP so verwendet, dass Hashwerte nicht geschützt werden können, so kann jeder (sogar nicht angemeldete Benutzer) Ihre Passworthashes lesen und versuchen, sie zu knacken. Sie sollten sich nach sicheren Alternativen zu der NIS und LDAP-Version, die Sie verwenden, umschaun. Bis diese unsicheren Anwendungen gesichert oder ersetzt werden können, sollten Sie die Berechtigungen und Passwörter dieser Anwendungen regelmäßig und proaktiv sichern und überprüfen. Prüfen Sie auch, ob Sie den MD5-Algorithmus statt crypt zum Hashen Ihrer Passwörter verwenden können.

Sogar wenn die Passwörter an sich stark sind, so können doch Accounts kompromittiert werden, wenn die Anwender nicht ihre Passwörter schützen. Gute Passwortvorschriften sollten detaillierte Prozeduren für Benutzer enthalten, die erfordern, dass Benutzern nie ihr Passwort jemandem anderen mitteilen, ihre Passwörter nicht aufschreiben wo jemand anderer sie lesen könnte, und Dateien die Passwörter für automatisierte Anmeldungen enthalten geeignet gesichert werden. Weiters sollten die Benutzer, sollte Ihr Passwort gestohlen oder jemandem anderen bekannt sein, sofort den Systembetreuer benachrichtigen. Das Ablaufende der Gültigkeit von Passwörtern sollte eingehalten werden damit Passwörter, die den Regelungen entgegen nur für kurze Zeit angreifbar sind und alte Passwörter nicht wiederverwendet werden können. Administratoren sollen sicherstellen, dass die Anwender vor dem bevorstehenden Ablaufende der Gültigkeit ihres Passworts gewarnt werden und noch ausreichend Gelegenheit haben, ihr Passwort zu ändern bevor es abläuft. Wenn die Benutzer die Nachricht „Ihr Passwort ist abgelaufen und muss jetzt geändert werden“ erhalten, dann tendieren sie dazu, schlechte Passwörter zu wählen.

3. **Kontrollieren Sie Accounts genau.**

Die folgenden Maßnahmen garantieren eine bessere Kontrollen von Accounts:

- Alle Service-basierten oder administrativen Konten, die nicht verwendet werden, sollten deaktiviert oder wenn möglich, zur Gänze entfernt werden.
- Alle Service-basierten oder administrativen Konten die verwendet werden, sollten neue und starke Passwörter erhalten sobald der Dienst oder Account eingerichtet bzw. aktiviert wird.
- Versehen Sie neu erzeugte Benutzerkonten mit zufällig erzeugten Initialpasswörtern und zwingen Sie die Benutzer dazu, diese bei der ersten Anmeldung zu ändern.
- Überprüfen Sie regelmäßig und proaktiv die Accounts auf Ihrem System, und verwalten Sie eine Liste aller dieser Accounts mit einer Beschreibung des Dienstes, der dieses Konto benötigt und der beabsichtigten Verwendung.
- Überprüfen Sie regelmäßig, ob wirklich alle verwendeten Accounts noch benötigt werden.
- Entwickeln Sie zwingende Prozeduren um Accounts auf diese Liste zu setzen bzw. von ihr zu entfernen.
- Sie brauchen strikte Prozeduren für die Entfernung von Accounts, wenn Angestellte oder externe Mitarbeiter das Unternehmen verlassen oder wenn die Konten nicht länger benötigt werden.
- Setzen Sie sich mit Ihrer Personal Abteilung in Verbindung um über Abgänge informiert zu werden.
- Überprüfen Sie die oben genannte Liste regelmäßig um sicherzustellen dass keine neuen Account hinzugefügt wurden bzw. nicht benötigte Accounts gelöscht wurden.

Vergessen Sie weiters nicht, die Accounts und Passwörter auf Systemen wie Routern, Switches und digitalen Druckern und Kopierern mit Anschluss ans Internet zu überprüfen. Wenn diese eine schwache Passwortverwaltung haben und Benutzer dort dasselbe Passwort wie auf Unix-Systemen verwenden, dann kann das böswilligen Benutzern Tür und Tor öffnen.

Sie können eine Liste mit Standardpasswörtern für diverse Produkte hier finden:

<http://www.cirt.net/cgi-bin/passwd.pl>

4. **Verschlüsselte Logins**

Die Verwendung der besten Passwörter kann sinnlos sein, wenn die Passwörter im Klartext über das Netz gesendet werden. Wenn das passiert, kann jeder mit Zugriff auf den Netzwerkverkehr die Passwörter lesen während sie übertragen werden. Beispiele für Programme und Protokolle, die Passwörter im Klartext übertragen sind Telnet, ftp, http und die Berkeley r-Dienste.

Um dies zu verhindern, sollten verschlüsselnde Programme und Protokolle verwendet werden. So werden Passwörter nicht im Klartext übertragen, was es wesentlich schwieriger macht, Passwörter mit traditionellem Sniffen zu entdecken.

Es gibt einige Alternativen zur Verwendung der oben erwähnten Programme. OpenSSH kann

Telnet, FTP und die Berkeley r-Dienste ersetzen, und SSL kann verwendet werden um Verschlüsselung für http zur Verfügung zu stellen.

5. Superuser Accounts

Der root-Account ist der privilegierteste Account auf einem Unix-System. Es gibt keinerlei Sicherheitseinschränkungen für ihn, was heißt dass man alles damit auf einem System machen kann. Daher ist das DER Account, auf den böswillige User Zugriff haben wollen.

Verbieten Sie root-Anmeldungen von außen. Anwender sollten den su Befehl verwenden um root-Zugang zu erhalten. Su ändert die effektive uid des Accounts zu der eines anderen Accounts, in diesem Fall, des root-Accounts

Wenn Anwender nur wenige mächtigere Befehle benötigen, verwenden Sie sudo. Sudo (superuser do) erlaubt es Systemverwaltern, bestimmten Benutzern oder Gruppen die Möglichkeit, bestimmte (oder alle) Befehle als root zu verwenden, wobei alle Befehle und Befehlsargumente aufgezeichnet werden. In diesem Fall muss der Benutzer auch nicht das root-Passwort eingeben.

Die Benutzung des root-Accounts sollte auf die Installation des Systems und von Applikationen, bestimmte Konfigurationen und Notfälle eingeschränkt werden.

Schränken Sie den Personenkreis mit Zugang zum root-Passwort ein. Es sollte nur den Systemverwaltern bekannt sein.

Weitere Informationen zu Sudo finden Sie auf <http://www.courtesan.com/sudo/>, Informationen zu Su erhalten Sie durch die Eingabe von man su bei der Eingabeaufforderung.

6. Allgemeine Accounts

Allgemeine Accounts werden oft in der Entwicklung verwendet um einer Anwendung zu erlauben mit anderen Anwendungen oder Datenbanken zu kommunizieren. Zugriff des Herstellers ist eine weitere Situation, in der oft allgemeine Accounts verwendet werden. Bei der Verwaltung dieser Accounts ist große Sorgfalt notwendig um die Nachvollziehbarkeit von Zugriffen und Änderungen aufrechtzuerhalten.

Allgemeines

Zuerst, verwenden Sie allgemeine Accounts nur als letzten Ausweg. Wenn ein Benutzer oft oder über längere Zeit Zugang benötigt, sollte er einen eigenen Account erhalten.

Wenn ein allgemeiner Account benötigt wird (mehrere Mitarbeiter der Hersteller benötigen Zugang, Anwendungen benötigen authentisierten Zugriff, ...), sollte ein befugter Mitarbeiter für alle mit diesem Account durchgeführten Tätigkeiten verantwortlich gemacht werden.

Anwendungs-Accounts

Verwenden Sie keine hardcodierte Passwörter in Anwendungen. Stellen Sie geeigneten Schutz von Account und Passwort-Information sicher (verschlüsselte Datei, Lese-Zugriff, ...)

Herstellerzugang

- Beschaffen Sie sich eine unterschriebene Erklärung, in der der Hersteller die volle Verantwortung für alles, was mit diesem Account passiert, übernimmt.
- Bestimmen Sie einen Verantwortlichen für die Verwaltung der Passwörter der Hersteller-Accounts
- Legen Sie Support-Accounts in Kuverts ab und lassen Sie die Hersteller anrufen um Zugriff auf das System zu erhalten.
- Verwenden Sie Zwei-Faktor-Authentisierung wo möglich
- Lassen Sie den Verantwortlichen für Hersteller-Passwörter die Passwörter der Support-Accounts nach jeder Verwendung ändern. Das ist nicht notwendig, wenn Sie Zwei-Faktor-Authentisierung verwenden.
- Überprüfen Sie, ob die Kuverts mit Passwörtern unbeschädigt sind.
- Führen Sie regelmäßige Audits durch

7. Protokoll

Die Aufbewahrung von Protokollen über Benutzeraktivitäten ist ein wesentlicher Teil der Absicherung von Systemen. Die Aufzeichnung aller Anmeldeversuche unabhängig von deren Erfolg hilft Ihnen, festzustellen, was auf Ihren Systemen passiert. Weiters ist die genaue Aufzeichnung von su und sudo Aktivitäten wichtig, um Ihnen zu zeigen, wer versucht hat Tätigkeiten mit Berechtigungen, die sich von seinen unterscheiden, durchzuführen.

Häufige Überprüfungen der Protokolle kann Sie auf die Spur von potentiell Missbrauch von Berechtigungen oder anderen ungewöhnlichen Aktivitäten auf dem System führen.

Weiterführende Informationen über alle Facetten des Logging finden Sie auf <http://www.loganalysis.org/>

[zum Anfang ^](#)

U4 Versionskontroll Systeme

U4.1 Beschreibung

Versionskontroll Systeme stellen Werkzeuge zur Verwaltung unterschiedlicher Versionen von Dokumenten oder Quellcode zur Verfügung. Weiters ermöglichen sie, dass mehrere Benutzer an denselben Dateien arbeiten können. Solche Systeme sind wesentlich um Softwareentwicklungsprojekte oder Firmendokumente zu verwalten, so hat man nicht nur einen zentrale Speicherlösung, sondern kann auch auf verschiedene Versionen zugreifen. Das Concurrent Versions System (CVS) ist das bekannteste System zur Kontrolle der Quellcodeerstellung, das heute im Linux/Unix-Umfeld verwendet wird. Viele Open-Source-Projekte erlauben „anonymen“ Zugang zu deren CVS-Repositories. Ein CVS-Repository kann für den Fernzugriff über das „pserver“-Protokoll, das Port 2401/TCP verwendet konfiguriert werden. Ein so konfigurierter Server enthält die folgenden Schwachstellen:

- A) Ein Heap-basierter Buffer Overflow, der durch speziell geschnitzte „Einträge“ ausgelöst wird. Ein Angreifer kann diesen Buffer Overflow verwenden um beliebigen Code auf dem CVS-Server zu verwenden. Exploit Code für CVS-Server auf Linux, FreeBSD und Solaris wurde in den Security Mailing Listen veröffentlicht. Wichtig ist, dass jedes Repository, das für „anonymen Zugang“ konfiguriert wurde, potentiell verwundbar ist.
- B) Schwachstellen in der Implementation von anderen Befehlen und Funktionen können durch einen angemeldeten Angreifer verwendet werden um ein Denial of Service auf dem CVS Server zu verursachen oder um beliebigen Code auf dem CVS-Server auszuführen. Einige

dieser Probleme können auch von "anonymen" Usern ausgenutzt werden.

Subversion ist ein weiteres Versionskontroll System für Linux, das immer weiter verbreitet ist. Das Projekt wurde mit dem Ziel, ein besseres System als CVS zu entwickeln. Über das "svn"-Protokoll kann man auf ein Subversion Repository zugreifen, denn dieses Repository "svnserve" verwendet. Der svn-Server läuft standardmäßig auf Port 3690/TCP. Dieser Server hat folgende Schwachstellen:

- Ein Heap-basierter Overflow, der von einem nicht angemeldeten Angreifer verwendet werden kann um beliebigen Code auszuführen.
- Ein Stack-basierter Overflow, der durch einen speziell bearbeiteten "get-dated-rev" svn-Befehl ausgelöst werden kann. Wenn der Server für anonymen Zugang konfiguriert ist, kann ein nicht authentisierter Angreifer durch so einen Exploit beliebigen Code auf dem Server ausführen kann. Im Internet sind bereits mehrere Exploits für diese Schwachstelle verfügbar.

Wenn ein Angreifer Zugang erhält, kann er nicht nur Quelltextdateien mit Hintertüren oder Fehlern versehen, die, wenn die Software verteilt wird, eine große Zahl von kompromittierten Systemen erzeugen, das könnte auch nützlich sein um einen tatsächlichen Angestellten in kriminelle Aktivitäten durch "Identity Spoofing" zu verwickeln.

U4.2 Betroffene Betriebssysteme

Linux, FreeBSD, AIX, HP-UX, Solaris und SGI und potentiell alle, die CVS oder Subversion verwenden können.

U4.3 CVE/CAN Einträge

[CAN-2004-0396](#), [CAN-2004-0397](#), [CAN-2004-0413](#), [CAN-2004-0414](#), [CAN-2004-0416](#), [CAN-2004-0417](#), [CAN-2004-0418](#)

U4.4 Wie Sie herausfinden, ob Sie betroffen sind

Wenn Ihr CVS Server für Fernzugriff über das „pserver“-Protokoll konfiguriert ist und Sie eine der folgenden Versionen der CVS-Software verwenden, ist Ihr CVS-Server angreifbar:

- CVS stable release Version 1.11.16 und älter
- CVS feature release Version 1.12.8 und älter

Sie können die CVS Version durch den Befehl „cvs ver“ herausfinden

Wenn Ihr Subversion Server für Fernzugriff über das „svn“-Protokoll konfiguriert ist und Sie eine Version älter als 1.0.5 verwenden, ist Ihr Server angreifbar.

U4.5 Wie Sie sich dagegen schützen können

Für CVS Server:

- Stellen Sie sicher, dass Ihre CVS-Software auf den aktuellsten Stand gebracht wurde. Der Quellcode für die neueste Software kann von <https://www.cvshome.org/> heruntergeladen werden.
- Konfigurieren Sie den CVS-Server um das SSH-Protokoll statt dem pserver-Protokoll für Fernzugriffe zu verwenden. Zusätzlich sollten Sie den CVS-Server in einer „chroot“-Umgebung laufen lassen. Eine detaillierte Anleitung finden Sie bei <http://www.netsys.com/library/papers/chrooted-ssh-cvs-server.txt>.

- Wenn auf das CVS Repository von innerhalb des Firmen-/Unternehmensnetzwerks zugegriffen wird, sperren Sie den Port 2401/tcp am Netzwerk-Perimeter.
- Stellen Sie sicher, dass die veröffentlichten Exploits bei Ihrem CVS-Server nutzlos sind. Die veröffentlichten Exploits finden Sie bei:
http://www.k-otik.com/exploits/05212004.CVS_Linux.c.php
http://www.k-otik.com/exploits/05212004.CVS_Solaris.c.php
- Versuchen Sie, den CVS-Server für anonymen read-only Zugriff auf einem Stand-Alone-System zu installieren, wie zum Beispiel in einer DMZ.

Für Subversion Server:

- Stellen Sie sicher, dass Ihr Subversion Server auf den aktuellsten Stand gebracht wurde. Die aktuellste Version kann von <http://subversion.tigris.org> heruntergeladen werden.
- Konfigurieren Sie den Zugriff auf Subversion Repositories auf webDAV statt dem „svn“ Protokoll.
- Wenn auf das Subversion Repository von innerhalb des Firmen-/Unternehmensnetzwerks zugegriffen wird, sperren Sie den Port 3690/tcp am Netzwerk-Perimeter.
- Stellen Sie sicher, dass die veröffentlichten Exploits bei Ihrem CVS-Server nutzlos sind. Die veröffentlichten Exploits finden Sie bei:
http://www.metasploit.com/projects/Framework/modules/exploits/svnserve_date.pm
<http://www.k-otik.com/exploits/06112004.subexp.c.php>
- Versuchen Sie, den Subversion Server für anonymen read-only Zugriff auf einem Stand-Alone-System zu installieren, wie zum Beispiel in einer DMZ.

U4.6 Referenzen

CERT Advisory

<http://www.kb.cert.org/vuls/id/192038>

SecurityFocus BIDs

<http://www.securityfocus.com/bid/10384>

<http://www.securityfocus.com/bid/10499>

<http://www.securityfocus.com/bid/10386>

<http://www.securityfocus.com/bid/10519>

CVS Homepage

<http://www.cvshome.org>

Subversion Homepage

<http://subversion.tigris.org>

Security List Postings

<http://www.securityfocus.com/archive/1/363775/2004-05-17/2004-05-23/0>

<http://www.securityfocus.com/archive/1/365541/2004-06-07/2004-06-13/0>

<http://www.securityfocus.com/archive/1/363781/2004-05-17/2004-05-23/0>

<http://archives.neohapsis.com/archives/bugtraq/2004-06/0180.html>

[zum Anfang ^](#)

U5.1 Beschreibung

Email ist einer der am weitesten verbreiteten Anwendungen im Internet, da SMTP eines der ältesten Protokolle ist. Mail Transport Agents (MTAs) sind die Server, die für die Übertragung von E-Mail vom Sender zum beabsichtigten Empfänger zuständig sind, üblicherweise über SMTP, damit SSL auf unsicheren Ports verschlüsselt werden kann, mit TLS wenn beide Seiten es unterstützen. Sendmail ist der am weitesten verbreitete Unix-basierte MTA. Allerdings über die Jahre haben die Menge an Sicherheitsproblemen und die Komplexität der Konfiguration dieser Software zu einigen populären Alternativen wie zum Beispiel Qmail, Courier-MTA, Postfix und Exim geführt

Es ist wenig überraschend, wenn man den weitverbreiteten Gebrauch von Email bedenkt, dass dieses System dauernd von Viren, Würmern und menschlichen Angreifern attackiert wird. Während sehr viele dieser Attacken auf die am häufigsten verwendeten Emailclients abzielen, werden MTAs auch recht häufig angegriffen. Die meisten der aktuellen Schwachstellen dieser Server fallen in eine der folgenden Kategorien:

- Angriffe auf ungepatchte Systeme inklusive Buffer Overflows, Heap Overflows, etc.
- Missbrauch von offenen Relays, das bevorzugte Werkzeug von Spammern
- Ausnutzung von anderen, nicht-Relay Fehlkonfigurationen wie zum Beispiel Datenbanken mit Benutzerkonten, für Spam oder Social Engineering (oder sogar für Angriffe auf Emailclients)

Man kann sicher sein, dass, wenn ein verwundbarer MTA im Netzwerk läuft, dieser fast sofort gefunden und missbraucht wird. Glücklicherweise kann man das Risiko des eigenen Email-Systems durch ein paar einfache Schritte während der Installation und danach regelmäßiger Wartung drastisch reduzieren. Die MTAs, die sich genau an die RFCs halten, sind am besten geeignet, da sich Spam Software oft nicht daran hält.

U5.2 Betroffene Betriebssysteme

Beinahe alle Varianten und Distributionen von Unix werden mit einem der oben genannten MTAs ausgeliefert. Obwohl die Hersteller in den letzten Jahren die Sicherheit der Standardinstallationen stark verbessert haben, sollte man davon ausgehen, dass jedes System mit einem MTA der nicht gepatcht bzw. gewartet ist oder mit Standardkonfiguration läuft, angreifbar ist.

U5.3 CVE/CAN Einträge

Sendmail

[CVE-1999-0047](#), [CVE-1999-0095](#), [CVE-1999-0096](#), [CVE-1999-0129](#), [CVE-1999-0131](#),
[CVE-1999-0203](#), [CVE-1999-0204](#), [CVE-1999-0206](#), [CVE-1999-1109](#), [CVE-2000-0319](#),
[CVE-2001-0653](#), [CVE-2001-1349](#), [CVE-2002-0906](#)

[CAN-1999-0098](#), [CAN-1999-0163](#), [CAN-2001-0713](#), [CAN-2001-0714](#), [CAN-2001-0715](#),
[CAN-2002-1165](#), [CAN-2002-1278](#), [CAN-2002-1337](#), [CAN-2003-0161](#), [CAN-2003-0285](#),
[CAN-2003-0694](#)

Qmail

[CVE-2000-0990](#), [CAN-2003-0654](#)

Courier-MTA

[CVE-2002-0914](#), [CVE-2002-1311](#), [CVE-2003-0040](#), [CVE-2004-0224](#), [CVE-2004-0777](#)

Exim

[CVE-2001-0889](#)

[CAN-2003-0743](#), [CAN-2004-0399](#), [CAN-2004-0400](#)

Postfix

[CAN-2003-0468](#)

U5.4 Wie Sie herausfinden, ob Sie betroffen sind

Überprüfen Sie den Patch Level

Um festzustellen, ob Ihr System verwundbar ist, ist der erste Schritt, den Patch Level Ihres MTA festzustellen sowie herauszufinden ob für diese Version Schwachstellen bekannt. Mit Hilfe von CVE (<http://cve.mitre.org/>) können Sie Schwachstellen Ihres MTAs identifizieren.

Sendmail

Sendmail hatte in der Vergangenheit eine große Anzahl von Schwachstellen. Diese Schwachstellen entstanden oft durch die Komplexität von Sendmail. Diese machten Sendmail zu einem der am meisten missbrauchten Dienst im Internet.

Jede veraltete oder nicht gepatchte Version der Software ist sehr wahrscheinlich angreifbar.

Um die Version von Sendmail herauszufinden können Sie den folgenden Befehl verwenden:
echo \\$\$Z | sendmail -bt -d

Vertrauen Sie nicht unbedingt der Versionsbezeichnung, die der Server ausgibt, denn die wird nur aus einer Textdatei auf dem System ausgelesen, die möglicherweise nicht richtig aktualisiert wurde.

Um herauszufinden, ob die Version, die Sie verwenden, aktuell ist, finden Sie auf <http://www.sendmail.org/current-release.html> die aktuelle Version von Sendmail.

Exim

Exim ist weiterer populärer MTA. Auch Exim hatte einige Schwachstellen in der Vergangenheit.

Um die Version von Exim herauszufinden, verwenden Sie den folgenden Befehl:
exim -bV

Um herauszufinden, ob die Version, die Sie verwenden, aktuell ist, finden Sie auf <http://www.exim.org/version.html> die aktuelle Version von Exim.

Qmail

Qmail ist ein sicherer MTA, der wenige Schwachstellen in der Vergangenheit hatte. Qmail ist auch einer der populärsten MTAs nach Sendmail.

Es gibt keinen einfachen, zuverlässigen Weg, die Version von Qmail herauszufinden, außer die Version in den Man-Pages durch GNU:

```
grep -A1 version /var/qmail/man/man7/qmail.7
```

Qmail hat zahlreiche Erweiterungen, die von Anwendern beigesteuert wurden, was das Auffinden von Schwachstellen erschwert.

Sie können die für Qmail empfohlenen Patches bei <http://www.qmail.org/top.html#patches> finden, ein Paket (namens netqmail), das Qmail und die empfohlenen Patches enthält, finden Sie hier: <http://www.qmail.org/netqmail/>

Courier-MTA

Courier-MTA ist ein striktes RFC Mail Server System, das Maildir+, maildrop, MySQL, Postgresql und LDAP als Ablage für Alias und Benutzerkonten unterstützt.

Um die Version herauszufinden, verwenden Sie den Befehl "showmodules".

Sicherheitsinformationen und die aktuelle Version finden Sie bei <http://www.courier-mta.org>.

Postfix

Wie Qmail ist Postfix ein sicherer MTA und hatte sogar noch weniger Schwachstellen in der Vergangenheit. Neuere Versionen haben erweiterte Fähigkeiten im Bereich von Zugriffskontrolle, Content Inspection und Rate Limiting, deshalb kann Upgrading eine gute Idee sein, auch wenn die verwendete Version nicht verwundbar sein sollte.

Die Version von Postfix liefert der folgende Befehl:

```
postconf -d mail_version
```

Um herauszufinden, ob die von Ihnen verwendete Version aktuell ist, schauen Sie nach der aktuellen Version unter <ftp://ftp.porcupine.org/mirrors/postfix-release/index.html>

- **Überprüfen Sie Ihren Relay Status**

Was ist ein offenes Relay

Weiterleiten von Mail ist eine grundlegende Funktion von MTAs, aber fehlerhafte Konfigurationen können Ihren MTA in ein offenes Relay verwandeln. Das passiert, wenn ein MTA eine Mail weiterleitet, von der weder Sender noch Empfänger lokale User sind. Mit anderen Worten, der Sender und der Empfänger sind nicht Teil der Domain und der MTA hat eigentlich mit der Transaktion nichts zu tun. Unter normalen Umständen hätte die Email keinen Grund, diesen MTA zu passieren.

Überprüfen Sie, ob Ihr MTA ein offenes Relay ist

Die Kontrolle, ob Ihr MTA ein offenes Relay ist, ist eine der wichtigsten Tätigkeiten nach der Kontrolle des Patch-Levels. So kann man herausfinden, ob jemand durch Ihren MTA unerwünschte Werbemails (SPAM) senden kann. Die folgenden Werkzeuge unterstützen Sie bei dieser Kontrolle:

<http://www.abuse.net/relay.html>

<http://www.cymru.com/Documents/auditing-with-expect.html>

Was ist eine Realtime Blackhole Liste?

Eine Realtime Blackhole Liste (RBL) ist eine Liste von IP-Adressen von Servern deren Besitzer sich weigern, die Ausbreitung von Spam im Internet zu stoppen. Diese Listen werden von Mail Administratoren verwendet um Verbindungen zu ihren Servern von diesen bekannten Spammern abzulehnen.

Ist Ihr Server auf einer RBL

Wenn Sie Ihren Mailserver in einer dieser Listen finden, dann ist er sehr wahrscheinlich ein offenes Relay, außer Sie haben erst kurzfristig die Konfiguration geändert. Es könnte auch sein, dass einer der Ihrer "echten" Anwender Ihren Server missbraucht hat und SPAM oder

“Newsletter” verschickt hat. Das kann Sie auch auf eine RBL befördern. Sie können in den folgenden Sites nach der IP-Adresse Ihres Servers suchen um herauszufinden, ob diese Adresse auf einer der Listen ist:

<http://www.mail-abuse.com/support/lookup.html>

<http://www.ordb.org/>

Bedenken Sie dabei, dass es viele RBLs gibt und diese Suchseiten nur die bekanntesten berücksichtigen.

- **Prüfen Sie Ihren Mailserver**

Ein Audit Ihres Mailservers ermöglicht Ihnen, Schwachstellen zu finden, die von böswilligen Personen verwendet werden können um nicht autorisierte Aktionen auf/mit Ihrem Mailserver durchzuführen.

Nessus

Nessus ist ein freier und mächtiger Schwachstellenscanner, der ein spezieller Plugin für SMTP-Server enthält. Das ermöglicht Ihnen, MTA Schwachstellen auf schnelle und effiziente Weise zu finden

Sie können Nessus mit Plugins auf folgender Site finden: <http://www.nessus.org>

SARA

Sara steht für “Security Auditor's Research Assistant”. Es ist ein Werkzeug für Sicherheitsanalysen, das die SANS Top 20 Schwachstellen in der Liste mit den zu untersuchenden Schwachstellen enthält.

SARA ist verfügbar auf <http://www-arc.com/sara/>

U5.5 Wie Sie sich dagegen schützen können

Die folgenden Schritte sollten unternommen werden um Ihren Mailserver zu schützen. Sie sind in zwei Teile unterteilt: Allgemeine Empfehlungen, die unabhängig vom Mailserver sind, und Spezifische Empfehlungen, die sich an Sendmail, Qmail und Postfix orientieren:

2. Allgemeine Empfehlungen

- Entscheiden Sie, ob Sie einen MTA benötigen und ob dieser öffentlich verfügbar sein muss.
- Deaktivieren Sie den Mailserver auf allen Systemen, die nicht speziell für den Betrieb eines Mailservers entwickelt und genehmigt wurden. Es sollten Prozeduren installiert werden, die eine erneute Aktivierung verhindern. Verwenden Sie Firewallregeln um das durchzusetzen.
- Installieren Sie alle Patches der Hersteller oder steigen Sie auf die neueste version Ihres Mailservers um.
- Verwenden Sie einen getrennten internen MTA um internen Mailverkehr zu behandeln.
- Reduzieren Sie die Rechte mit welchen der MTA läuft, oder betreiben Sie ihn in einem Chroot-Gefängnis, wenn möglich
- Lesen Sie die gesamte Mailserver Dokumentation und abonnieren Sie die entsprechenden Mailing Listen, sofern verfügbar.

Schützen Sie sich gegen Mail Relaying

Um zu verhindern, dass Ihr Mailserver von Spammern missbraucht wird, muss er so konfiguriert werden, dass er keine Mails von nicht vertrauenswürdigen Netzen und Domains weiterleitet:

Sendmail

Wenn Sie Sendmail im Daemon-Mode verwenden müssen, stellen Sie sicher, dass Ihre Konfiguration so gestaltet ist, dass sie Mails richtig weiterleitet und das nur für Systeme Ihres Einflussbereichs. Unterstützung bei der richtigen Konfiguration Ihres Servers finden Sie bei <http://www.sendmail.org/tips/relaying.html> und http://www.sendmail.org/m4/anti_spam.html. Beginnend mit Sendmail 8.9.0 ist das offene Relay standardmäßig deaktiviert. Allerdings haben einige Hersteller von Betriebssystemen dies in deren Standardkonfigurationen wieder aktiviert. Wenn Sie die Version von Sendmail, die mit Ihrem Betriebssystem geliefert wurde, verwenden, legen Sie besonderes Augenmerk darauf, dass Ihr Server nicht für Relaying verwendet wird.

Qmail

Qmail bietet eine gute Dokumentation über selektives Relaying und Hilfe um Relaying in Ihrem System zu deaktivieren. Für Details: <http://www.lifewithqmail.org/lwq.html#relaying>

Courier-MTA

Da Courier-MTA von Haus aus nur geschlossene Relay zulässt, bietet es Hilfe, Relaying für bestimmte Netze und IP-Adressen zu aktivieren. Zusätzlich wird SMTP Authentisierung verwendet um Relaying zur Verfügung zu stellen.

[Http://www.courier-mta.org](http://www.courier-mta.org) – FAQ Sektion.

Exim

Exim hat auch detaillierte Anleitungen, wie man Relaying verhindert:

<http://www.exim.org/howto/relay.html>

Postfix

Für Postfix gibt es einige Schritte, die helfen, Den Zugriff und die Weiterleitung zu beschränken und zu kontrollieren. Nur für Rechner und Netze, die im 'mynetworks' Parameter aufgezählt sind, wird die Weiterleitung erlaubt. Details auf http://www.postfix.org/SMTPLD_ACCESS_README.html

3.Andere anwendungsspezifische Details

A)Weitere Information, wie man Sendmail sicherer konfigurieren und betreiben kann, findet man bei:

<http://www.sendmail.org/secure-install.html>

http://www.sendmail.org/m4/security_notes.html

<http://www.sendmail.org/~gshapiro/security.pdf>

B)Um zu verhindern, dass ein kompromittierter Postfix Ihr gesamtes System entblößt, schränken Sie ihn so ein, dass er als nicht-privilegierter Benutzer in einer Chroot-Umgebung läuft.

Details zur Postfixkonfiguration finden Sie auf:

<http://www.linuxjournal.com/article.php?sid=4241>

C)Der folgende Link ist ein Beispiel, wie Sie Ihren MTA konfigurieren können, Blackholes zu verwenden:

<http://www.ordb.org/faq/#usage>

D) Courier-MTA hat die Unterstützung von RBLs bereits eingebaut und stellt eine anfängliche RBL in der Konfigurationsdatei von esmtpd zur Verfügung.

E) Postfix bietet einige Möglichkeiten, Spam einzuschränken. Informationen darüber finden Sie bei:

<http://www.securitysage.com/antispam/intro.html>

[zum Anfang ^](#)

U6 Simple Network Management Protocol (SNMP)

U6.1 Beschreibung

Das Simple Network Management Protocol (SNMP) wird verwendet, um beinahe alle Arten moderner TCP/IP-fähiger Geräte zu beobachten und zu konfigurieren. Da SNMP ziemlich allgegenwärtig ist in seiner Verbreitung auf Netzwerk Systemen, wird es meistens als Mittel eingesetzt, Geräte wie Drucker, Router, Switches und Access Points zu konfigurieren und zu verwalten, bzw. Daten für Netzwerküberwachungssysteme zu liefern.

Simple Network Management Kommunikation besteht aus verschiedenen Arten von Nachrichten, die zwischen SNMP Management Stationen und Netzwerkgeräten, die Agent-Software verwenden, ausgetauscht werden. Die Art, wie diese Nachrichten behandelt werden und die Authentifizierungsmechanismus hinter der Verarbeitung der Nachrichten haben wesentliche ausnützbare Schwachstellen.

Die Schwachstellen der Methode, mit der SNMP Version 1 Traps verarbeitet und erzeugt, ist im CERT Advisory [CA-2002-03](#) detailliert beschrieben. Es gibt eine Menge von Schwachstellen in der Art, wie Trap- und Requestnachrichten von Management Stationen und Agenten verarbeitet und decodiert werden.

Diese Schwachstellen sind nicht auf bestimmte Implementierungen von SNMP beschränkt, sondern betreffen eine Vielzahl von SNMP Implementierungen verschiedener Hersteller. Die Ergebnisse dieser Schwachstellen, wenn sie von Angreifern ausgenutzt werden liegen irgendwo im Bereich zwischen Denial of Service und ungewollter Konfiguration und Verwaltung Ihrer SNMP-fähigen Geräte.

Der eingebaute Authentifizierungsmechanismus in älteren SNMP-Systemen ist eine weitere wesentliche Schwachstelle. Die Versionen 1 und 2 von SNMP verwenden unverschlüsselte „Community Strings“ als einzigen Authentifizierungsmechanismus. Das Fehlen von Verschlüsselung ist schlimm genug, aber der Standard-Community String, der von der überwältigten Mehrheit der Hersteller verwendet wird, ist „public“, ein paar vermeintlich clevere Hersteller von Netzwerk Equipment haben den String auf „private“ für sensiblere Informationen geändert. Angreifer können diese SNMP-Schwachstelle verwenden um Geräte aus der Ferne umzukonfigurieren oder auszuschalten. Gesniffter SNMP-Verkehr kann sehr viel über den Aufbau Ihres Netzwerks und die angeschlossenen Geräte enthüllen. Eindringlinge verwenden diese Informationen um sich Ziele auszusuchen und Angriffe zu planen.

Die meisten Hersteller aktivieren SNMP Version 1 als Standard, und viele bieten keine Produkte an, die die Sicherheitsmodelle von SNMP Version 3 verwenden können, die so konfiguriert werden können, dass sie verbesserte Authentifizierungsmechanismen verwenden. Es gibt jedoch frei verfügbaren Ersatz, der SNMPv3 bietet, unter der GPL oder BSD Lizenz.

SNMP ist nicht auf UNIX beschränkt; es wird viel mit Windows verwendet, mit Netzwerkgeräten, Wireless Access Points und Bridges, mit Druckern und Embedded Devices. Aber der Großteil der SNMP-bezogenen Angriffe, die bis jetzt gesehen wurden, waren auf UNIX Systemen mit schlechten SNMP Konfigurationen. Da SNMP-Verkehr im Klartext übertragen wird, muss man, wenn der Verkehr mitgehört werden könnte, den Einsatz von SNMP sorgfältig bedenken.

Um mehr über die Schwachstellen von SNMP zu erfahren, hat das CERT CC ein umfassendes [SNMP FAQ](#) erarbeitet.

U6.2 Betroffene Betriebssysteme

Beinahe alle UNIX und Linux Systeme werden mit installiertem und oft standardmäßig aktiviertem SNMP ausgeliefert. Die meisten anderen SNMP-fähigen Netzwerkgeräte und Betriebssysteme sind ebenso anfällig.

U6.3 CVE/CAN Einträge

CVE-1999-0294	CVE-1999-0472	CVE-1999-0815	CVE-1999-1335	CVE-2000-0221
CVE-2000-0379	CVE-2000-0515	CVE-2000-1058	CVE-2001-0236	CVE-2001-0487
CVE-2001-0514	CVE-2001-0564	CVE-2001-0888	CVE-2002-0017	CVE-2002-0069
CVE-2002-0302	CAN-1999-0186	CAN-1999-0254	CAN-1999-0499	CAN-1999-0516
CAN-1999-0517	CAN-1999-0615	CAN-1999-0792	CAN-1999-1042	CAN-1999-1126
CAN-1999-1245	CAN-1999-1460	CAN-1999-1513	CAN-2000-0147	CAN-2000-0885
CAN-2000-0955	CAN-2000-1157	CAN-2000-1192	CAN-2001-0046	CAN-2001-0352
CAN-2001-0380	CAN-2001-0470	CAN-2001-0552	CAN-2001-0566	CAN-2001-0711
CAN-2001-0840	CAN-2001-1210	CAN-2001-1220	CAN-2001-1221	CAN-2001-1262
CAN-2002-0012	CAN-2002-0013	CAN-2002-0053	CAN-2002-0109	CAN-2002-0305
CAN-2002-0478	CAN-2002-0540	CAN-2002-0812	CAN-2002-1048	CAN-2002-1170
CAN-2002-1408	CAN-2002-1426	CAN-2002-1448	CAN-2002-1555	CAN-2003-0137
CAN-2003-0935	CAN-2003-1002	CAN-2004-0311	CAN-2004-0312	CAN-2004-0576
CAN-2004-0616	CAN-2004-0635	CAN-2004-0714		

U6.4 Wie Sie herausfinden, ob Sie betroffen sind

Sie können überprüfen, ob SNMP auf ans Netzwerk angeschlossenen Geräten läuft, in dem Sie einen Scanner benutzen oder die Systeme manuell überprüfen:

- SNMPing – Sie können das freie SNMPing Scanprogramm vom SANS Institute erhalten: <http://www.sans.org/alerts/snmp/>.
- SNScan - Foundstone hat ein anderes leicht verwendbares SNMP Scanprogramm namens SNScan erzeugt, das von http://www.foundstone.com/knowledge/free_tools.html bezogen werden kann.
- Nessus – Ein Open-Source Schwachstellenscanner, der auf folgendem Link gefunden werden kann: <http://www.nessus.org>

Wenn Sie keines der oben genannten Werkzeuge verwenden können, sollten Sie manuell überprüfen ob SNMP auf Ihren Systemen läuft. Schlagen Sie in der Dokumentation Ihres Betriebssystems nach, wie Sie dessen SNMP Implementierung identifizieren können. Der grundlegende daemon kann üblicherweise identifiziert werden, in dem man die Prozessliste nach

„snmp“ durchsucht oder nach Services schaut, die auf den Ports 161 oder 162 laufen. (Das Werkzeug Isop ist hilfreich bei der Zuordnung von Ports zu Prozessen)

Eine laufende SNMP Instanz ist wahrscheinlich ausreichend Hinweis darauf, dass Sie für Fehler in der Behandlung von Traps und Requests anfällig sind. Für weitere Informationen lesen Sie bitte CERT Advisory [CA-2002-03](#).

Wenn SNMP läuft und eine dieser weiteren Situationen zutrifft, haben Sie eine Schwachstelle bedingt durch Standard oder leicht erratbare Community Strings:

1. Leere oder Standard SNMP Community Namen.
2. Erratbare SNMP Community Namen.
3. Versteckte SNMP Community Strings.

Bitte lesen Sie <http://www.sans.org/resources/idfaq/snmp.php> für Informationen, wie man diese Bedingungen überprüfen kann.

U6.5 Wie Sie sich dagegen schützen können

Schwachstellen in der Behandlung von Traps und Requests:

1. Wenn Sie SNMP nicht unbedingt benötigen, deaktivieren Sie es.
2. Wo immer möglich, verwenden Sie ein SNMPv3 Benutzer basiertes Sicherheitsmodell mit Authentifizierung der Nachrichten und, wenn möglich, Verschlüsselung der Daten.
3. Wenn Sie SNMPv1 oder v2 verwenden müssen, stellen Sie sicher, dass sie die aktuellsten Patches Ihres Herstellers verwenden. Ein guter Ausgangspunkt um herstellerepezifische Informationen zu erhalten ist Appendix A des CERT Advisory [CA-2002-03](#).
4. Filtern Sie SNMP (Port 161 TCP/UDP und 162 TCP/UDP) an den Eingangspunkten Ihres Netzwerks, außer es ist unbedingt notwendig, dass Sie externe Geräte abfragen oder verwalten.
5. Verwenden Sie Host-basierte Zugriffskontrollen auf Ihren SNMP Agentensystemen. Auch wenn diese Fähigkeit durch das Betriebssystem des SNMP Agenten eingeschränkt sein mag, so kann es möglich sein zu definieren, von welchen Systemen Ihre Agenten Anfragen entgegennehmen. Auf den meisten UNIX Systemen kann dies durch die Konfiguration von TCP-Wrapper oder Xinetd erreicht werden. Eine Agenten-basierte Packet-Filter-Firewall auf dem Host kann auch verwendet werden um unerwünschte SNMP Anfrage zu blockieren.

Schwachstellen durch Standard- oder erratbare Community Strings:

1. Wenn Sie SNMP nicht unbedingt benötigen, deaktivieren Sie es.
2. Wo immer möglich, verwenden Sie ein SNMPv3 Benutzer basiertes Sicherheitsmodell mit Authentifizierung der Nachrichten und, wenn möglich, Verschlüsselung der Daten.
3. Wenn Sie SNMPv1 oder v2 verwenden müssen, verwenden Sie dieselben Vorschriften für Community Namen wie für Passwörter. Stellen Sie sicher, dass sie schwer zu erraten oder Knacken sind, und dass sie periodisch gewechselt werden.
4. Überprüfen und bestätigen Sie Community Namen mittels snmpwalk. Weitere Informationen können unter <http://www.zend.com/manual/function.snmpwalk.php> gefunden werden. Eine gute Anleitung für dieses Programm kann unter <http://www.sans.org/resources/idfaq/snmp.php> gefunden werden.
5. Filtern Sie SNMP (Port 161 TCP/UDP und 162 TCP/UDP) an den Eingangspunkten Ihres

Netzwerks, außer es ist unbedingt notwendig, dass Sie externe Geräte abfragen oder verwalten. Wenn möglich, konfigurieren Sie die Filter so, dass sie nur SNMP Verkehr zwischen vertrauten Netzen erlauben.

6. Wo möglich, machen Sie die MIBs read-only. Weitere Informationen können unter http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315 gefunden werden.

[zum Anfang ^](#)

U7 Open Secure Sockets Layer (SSL)

U7.1 Beschreibung

Die Open Source [OpenSSL](#) Bibliothek stellt Kryptographie für Anwendungen, die über Netzwerk kommunizieren, zur Verfügung. OpenSSL ist eine sehr weit verbreitete Implementierung der SSL/TLS-Protokolle und wird von einer großen Zahl von Herstellern verwendet. Das bekannteste Beispiel einer Anwendung, die diese Bibliotheken verwendet ist der Apache Webserver (um sichere http-Verbindungen zu unterstützen). Manche der gebräuchlichen POP3, IMAP, SMTP und LDAP-Server haben auch ihre OpenSSL-basierten Gegenstücke.

Da die OpenSSL Bibliotheken in eine Zahl von Anwendungen integriert ist, kann jede Schwachstelle in den Bibliotheken über diese Anwendungen ausgenutzt werden. Zum Beispiel gibt es mehrere öffentlich verfügbare Exploits, die Apache-Server, die mit bestimmten Versionen dieser Bibliotheken kompiliert wurden, kompromittieren können. Allerdings könnten dieselben Exploits leicht modifiziert werden um zum Beispiel Sendmail, OpenLDAP, CUPS oder andere OpenSSL-fähige Programme zu missbrauchen.

In den OpenSSL-Bibliotheken wurden zahlreiche Schwachstellen gefunden, von welchen die 5 schwerwiegendsten in [CAN-2002-0655](#), [CAN-2002-0656](#), [CAN-2002-0557](#), [CAN-2002-0659](#) und [CAN-2003-0545](#) aufgezählt sind. Diese Schwachstellen können von außerhalb verwendet werden um beliebigen Code mit den Rechten der Anwendungen, die OpenSSL-Bibliotheken verwenden, auszuführen. In manchen Fällen, wie zum Beispiel Sendmail, kann das zu „root“-Rechten führen.

U7.2 Betroffene Betriebssysteme

Alle Unix und Linux Systeme, die OpenSSL 0.9.7c oder älter bzw. OpenSSL 0.9.6l oder älter verwenden. Das kann Pakete von Linux-Distributionen wie Apache, CUPS, Curl, OpenLDAP, Stunnel, Sendmail und andere OpenSSL-basierte Anwendungen betreffen.

U7.3 CVE/CAN Einträge

[CVE-1999-0428](#), [CVE-2001-1141](#)

[CAN-2000-0535](#), [CAN-2002-0557](#), [CAN-2002-0655](#), [CAN-2002-0656](#), [CAN-2002-0659](#), [CAN-2003-0078](#), [CAN-2003-0131](#), [CAN-2003-0147](#), [CAN-2003-0543](#), [CAN-2003-0544](#), [CAN-2003-0545](#), [CAN-2003-0851](#), [CAN-2004-0079](#), [CAN-2004-0081](#), [CAN-2004-0112](#), [CAN-2004-0607](#)

U7.4 Wie Sie herausfinden, ob Sie betroffen sind

Überprüfen Sie die Ausgabe des Befehls ‚openssl version‘. Wenn die Version nicht 0.9.7d oder 0.9.6m ist, sind Sie angreifbar.

U7.5 Wie Sie sich dagegen schützen können

1. Wechseln Sie auf die neueste Version von [OpenSSL](#). Wenn OpenSSL auf dem System bereits vorinstalliert war, installieren Sie die neuesten Patches vom Hersteller Ihres Betriebssystems. Beachten Sie, dass es in manchen Fällen notwendig sein kann, Anwendungen neu zu kompilieren oder zu linkern um die neuen Bibliotheken zu aktivieren.
2. Wenn in Ihrer Umgebung möglich, überlegen Sie sich, ob Sie nicht ipfilter/netfilter oder andere Firewalls verwenden können um den Zugriff auf Ihre OpenSSL-basierten Dienste einzuschränken. Beachten Sie, dass eine der häufigsten Anwendungen von OpenSSL die Absicherung von http-Verkehr über das öffentliche Internet für e-Commerce ist, wo eine Beschränkung der Hosts wahrscheinlich nicht durchführbar ist.

[zum Anfang](#) ^

U8 Fehlkonfiguration der Enterprise Dienste NIS/NFS

U8.1 Beschreibung

Das Network File System (NFS) und das Network Information Service (NIS) sind zwei wichtige in UNIX Netzwerken/auf UNIX Servern oft installierte Dienste. NFS ist ein ursprünglich von Sun Microsystems entwickelter Dienst um Dateisysteme/Verzeichnisse und Dateien zwischen UNIX Systemen eines Netzwerks zu teilen („exportieren“). NIS ist auch eine Sammlung von Diensten, die als Datenbank dienen um Informationen über den Aufenthaltsort, genannt Maps, anderen Diensten wie z.B. NFS zur Verfügung zu stellen. Die häufigsten Anwendungen dieser Maps sind die passwd und group Dateien, die verwendet werden, um die Benutzerverwaltung zu zentralisieren. Die hosts-Datei ist ein weiteres Ziel für NIS.

Die Sicherheitsprobleme mit beiden Diensten, verkörpert durch über die Jahre laufend entdeckte Probleme (Buffer Overflows, DoS und schwache Authentifizierung), machen diese zu einem häufigen Ziel von Angriffen.

Neben den nicht gepatchten Diensten, die noch immer weit verbreitet sind, liegen die größeren Risiken in falsch konfigurierten NIS und NFS, die es lokalen und nicht lokalen Benutzern leicht ermöglichen, Sicherheitsprobleme auszunützen.

Die lockere Authentifizierung durch NIS während der Abfrage von NIS Maps erlaubt es Benutzern, Anwendungen wie ypcat oder getent zu verwenden, die Werte aus einer NIS Datenbank oder aus einer Map oder die Passwortdatei liefern. Dieselbe Art von Problem tritt mit NFS auf, das implizit der UID (User ID) und den GIDs (Group ID) die der NFS Client dem Server präsentiert, vertraut. Abhängig von der Konfiguration des Servers erlaubt sie allen Anwendern, entfernte Dateisysteme zu mounten und zu erforschen.

U8.2 Betroffene Betriebssysteme

Beinahe alle UNIX und Linux Systeme werden mit einer installierten und oft auch aktivierten Version von NFS und NIS ausgeliefert. Im Fall von NFS, obwohl es oft standardmäßig aktiviert ist, ist die exports-Datei üblicherweise leer (diese Datei legt fest, welche Verzeichnisse verteilt werden und auf welche Art das passiert).

U8.3 CVE/CAN Einträge

NFS

[CVE-1999-0002](#), [CVE-1999-0166](#), [CVE-1999-0167](#), [CVE-1999-0170](#), [CVE-1999-0211](#),

CVE-1999-0832, CVE-1999-1021, CVE-2000-0344, CVE-2002-0830

CAN-1999-0165, CAN-1999-0169, CAN-2000-0800, CAN-2002-0830, CAN-2002-1228, CAN-2003-0252, CAN-2003-0379, CAN-2003-0576, CAN-2003-0680, CAN-2003-0683, CAN-2003-0976, CAN-2004-0154

NIS

CVE-1999-0008, CVE-1999-0208, CVE-1999-0245, CVE-2000-1040

CAN-1999-0795, CAN-2002-1232, CAN-2003-0176, CAN-2003-0251

U8.4 Wie Sie herausfinden, ob Sie betroffen sind

Die folgenden Schritte beziehen sich auf Schwachstellen von NIS/NFS:

1. Überprüfen Sie, ob sie auf dem aktuellsten Stand der vom Hersteller Ihres Systems veröffentlichten Patches sind. In den meisten Versionen zeigen die Befehle „rpc.mountd –version“ für NFS und „ypserv –version“ für NIS die Versionen an. Alle nicht gepatchten oder veralteten Versionen sind sehr wahrscheinlich angreifbar.
2. Für Schwachstellen der Programme wäre ein vollständigerer Ansatz die Verwendung eines aktualisierten Schwachstellen Scanners um Ihr System regelmäßig nach Fehlern zu durchsuchen.

Die folgenden Schritte beziehen sich auf die Konfiguration von NIS:

1. Vergewissern Sie sich, dass das root Passwort nicht in einer NIS Map verwaltet wird.
2. Überprüfen Sie, ob die Benutzerpassworte den Sicherheitsanweisungen entsprechen. Ein Passwortcracker kann dafür verwendet werden.
3. Wenn möglich, verwenden Sie Blowfish oder MD5 statt DES zum Hashen von Passwörtern.

Bitte beachten Sie: Verwenden Sie nie einen Passwortscanner, sogar auf Systemen auf welchen Sie root-ähnliche Rechte haben, ohne explizite und vorzugsweise schriftliche Erlaubnis Ihres Arbeitgebers. Administratoren mit den wohlwollensten aller Absichten wurden schon entlassen, weil sie Passwortknacker verwendet haben ohne dafür autorisiert zu sein.

Die folgenden Schritte beziehen sich auf die Konfiguration von NFS:

1. Überprüfen Sie, ob die Hosts, Netgroups und Berechtigungen in der Datei /etc/exports noch aktuell sind.
2. Führen Sie den Befehl „showmount -e SERVER_IP“ aus um zu sehen, was exportiert wird. Überprüfen Sie, ob Ihre Mounts von Ihren Sicherheitsvorschriften gedeckt sind.

U8.5 Wie Sie sich dagegen schützen können

Die folgenden Schritte beziehen sich auf die Konfiguration von NIS:

1. Auf jedem Client können Sie die erlaubten NIS Server explizit auflisten, wodurch andere Systeme daran gehindert werden, sich als NIS Server auszugeben.
2. Wenn Sie die DBM Dateien erzeugen, aktivieren Sie YP_SECURE um sicherzustellen, dass

- der Server nur auf Anfragen von Clients von privilegierten Ports antwortet. Das kann durch den Schalter „s“ des Befehls makedbm erreicht werden.
3. Inkludieren Sie die Hosts und Netzwerke, denen Sie vertrauen, in /var/yp/securenets, das von den Prozessen ypserv und ypxfrd verwendet wird, und denken Sie daran den daemon neu zu starten, damit die Änderungen wirksam werden.
 4. Vergewissern Sie sich, dass auf Ihren NFS Clients der Eintrag +: *:0:0::: in Ihrer password Map ist.
 5. Denken Sie über die Verwendung von NIS über ein sicheres Protokoll wie SSH nach. Ein guter Anfangspunkt ist <http://www.math.ualberta.ca/imaging/snfs/>.

Beachten Sie: Das Lightweight Directory Access Protocol (LDAP) ersetzt NIS in einigen Konfigurationen, und alle Linux Distributionen unterstützen LDAP als Quelle für einige Elemente von Name-Services wie passwd, group und hosts. Ein gutes Buch über die Verwaltung von LDAP ist dabei hilfreich. Weiters unterstützt LDAP von sich aus SSL-Verschlüsselung und Replikation.

Die folgenden Schritte beziehen sich auf die Konfiguration von NFS:

1. Verwenden Sie numerische IP-Adressen oder Voll qualifizierte Domain Namen statt Aliases (aus der hosts-Datei oder aus einer NIS hosts map), wenn Sie Clients in der Datei /etc/exports erlauben.
2. Verwenden Sie /etc/exports um den Zugriff auf das NFS Dateisystem einzuschränken, indem Sie Parameter hinzufügen:
 - o Verhindern Sie, dass normale Benutzer ein NFS Dateisystem mounten können, indem Sie den secure Parameter nach der IP-Adresse oder dem Domainnamen Ihres NFS-Clients anhängen (z.B.: /home 10.20.1.25(secure)).
 - o Exportieren Sie das NFS Dateisystem mit passenden Berechtigungen. Das kann durch Hinzufügen der passenden Berechtigung (ro für Nur-Lese- oder rw für Lese- und Schreibzugriff) nach der IP-Adresse oder dem Domainnamen Ihres NFS-Clients in /etc/exports file (z.B.: /home 10.20.1.25(ro)).
 - o Wenn möglich, verwenden Sie den Parameter root_squash nach der IP-Adresse oder dem Domainnamen Ihres NFS-Clients. Ist dieser Parameter aktiv, so wird die superuser ID root auf dem NFS-Client durch die User ID nobody und die Gruppen ID nogroup (das kann durch die Verwendung der Parameter „anonuid“ und „anongid“ an Ihre Bedürfnisse angepasst werden) auf dem NFS-Server ersetzt. So kann der root-Benutzer auf dem Client auf keine Dateien zugreifen oder sie ändern, für die nur root auf dem Server die Berechtigung hat, was ihn daran hindert superuser Privilegien auf dem Server zu erlangen (z.B.: /home 10.20.1.25(root_squash)).
 - o Wenn Sie ein Verzeichnis mit anonymous-ähnlichen Rechten exportieren wollen, verwenden Sie den „all_squash“ Parameter, der jede User ID und Gruppen ID in die anonuid und anongid IDs umwandelt.
 - o Eine komplette Sammlung der Parameter kann in der Man-Page von /etc/exports gefunden werden. <http://www.netadmintools.com/html/5exports.man.html>
3. Ein Programm NFSBug kann verwendet werden um die Konfiguration zu testen. Diese Tests inkludieren Auffinden von weltweit exportierten Dateisystemen, bestimmen ob die Export-Einschränkungen funktionieren, bestimmen ob Dateisysteme durch den Port-Mapper gemountet werden können, Versuche, Filehandles zu erraten und Ausnutzen verschiedener Lücken um auf das Dateisystem zuzugreifen. <http://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/nfsbug/>
- 4.
5. Auf Solaris aktivieren Sie Port Monitoring indem Sie die Zeile „set nfssrv:nfs_portmon = 1“ an die Datei /etc/system anhängen. Ein Linux-System verweigert standardmäßig die

Zusammenarbeit mit NFS-Clients, die einen nicht-privilegierten Port (über 1024) verwenden.

Allgemeine Überlegungen bezogen auf NIS und NFS:

1. Überarbeiten Sie Ihre Firewall Policies und vergewissern Sie sich, dass Sie alle nicht benötigten Ports wie auch Port 111/TCP/UDP (Portmap) und Port 2049/TCP/UDP (Rpc.nfsd) blockieren. Weiters erlauben Sie den Zugriff auf NIS und NFS Server nur von autorisierten Clients aus. Als weitere Maßnahme kann der Zugriff auch durch tcp_wrapper zu finden auf <http://sunsite.cnlab-switch.ch/ftp/software/security/security-porcupine.org/> eingeschränkt werden.
In Ihrer Datei /etc/hosts.allow sollten Sie den Dienst und die IP-Adressen, die auf diesen Dienst zugreifen dürfen, angeben (z.B.: portmap: 10.20.0.0/16 um dem Netz 10.20.0.0/16 den Zugriff auf den portmap Dienst zu erlauben). Weiters sollten Sie in der Datei /etc/hosts.deny alle Dienste und IP-Adressen, die NICHT auf Dienste zugreifen dürfen, angeben (z.B.: portmap: ALL, was allen nicht in /etc/hosts.allow inkludierten IP-Adressen den Zugriff verwehrt). Es ist wichtig, den Zugriff auf den Dienst Portmap zu beschränken, denn durch diesen Dienst arbeitet NFS.
2. Überlegen Sie sich, NFS über ein sicheres Protokoll wie SSH zu verwenden. Ein guter Ausgangspunkt ist <http://www.math.ualberta.ca/imaging/snfs/>.
3. Installieren Sie alle Patches des Herstellers oder aktualisieren Sie Ihre NIS und NFS daemons auf die neueste Version. Für weitere Informationen über das Härten Ihrer UNIX Installation, lesen Sie bitte CERTs [UNIX Security Checklist](#).
4. Deaktivieren Sie die NFS und NIS daemons auf allen Systemen, die nicht als NFS und/oder NIS Server vorgesehen und genehmigt wurden. Um zu verhindern, dass diese Änderung rückgängig gemacht wird, ist es vernünftig, diese Dienste aus dem Dateisystem zu entfernen.

[zum Anfang ^](#)

U9 Datenbanken

U9.1 Beschreibung

Datenbanken sind die zentralen Elemente von Electronic Business, Finanz-, Bank- und Enterprise Ressourcenplanungs- (ERP) –Systemen und enthalten kritische Informationen über Partner, Kunden und Angestellte. Trotz der Wichtigkeit von Integrität und Vertraulichkeit wurde Datenbank Management Systemen (DBMS) nicht dieselbe Aufmerksamkeit bezüglich Sicherheit wie Betriebssystemen und Netzwerken geschenkt. Datenbank Management Systeme sind Sammlungen von Programmen für die Speicherung, Bearbeitung und Extraktion von Daten einer Datenbank.

Die Integrität und Vertraulichkeit von Daten kann durch einige Faktoren, wie Komplexität der Implementation, unsicherem Gebrauch von Passwörtern, Fehlkonfigurationen, schlecht geschriebenen Anwendungen, hartkodierten Passwörtern und nicht erkannten Hintertürchen zum System, kompromittiert werden. Die meisten Unternehmen und Regierungsorganisationen verwenden Datenbanken für Personalinformationen wie Gehaltsverrechnung oder Gesundheitsdaten für die gesetzliche Pflichten zur Geheimhaltung und Vertraulichkeit bestehen. Datenbanken speichern sensible Finanzdaten aus der Vergangenheit und über die Zukunft, wie Geschäftsaufzeichnungen, Finanztransaktionen und Buchhaltungsdaten. Datenbanken enthalten oft auch Kundendaten wie Bankverbindungen, Kreditkartennummern und vertrauliche Daten von Geschäftspartnern.

Datenbanken sind extrem komplexe Anwendungen und sind sehr oft nur schwer richtig und sicher zu konfigurieren. Datenbankanwendungen wie MySQL, PostgreSQL und Oracle enthalten viele der folgenden Merkmale: Benutzerkonten und Passwörter, Auditing Systeme, Berechtigungsmodelle und spezifische Berechtigungen für die Steuerung von Datenbankobjekten, eingebaute Befehle, einzigartige Skript- und Programmiersprachen, Netzwerkprotokolle, Patches und Service Packs und mächtige Verwaltungs- und entwicklungswerkzeuge. Viele Administratoren verwalten Datenbanken nur auf Teilzeitbasis und erfassen oft nicht die Komplexität dieser Anwendungen. Als Ergebnis werden oft schwerwiegende Sicherheitsprobleme und Konfigurationsfehler nicht überprüft und bleiben daher unentdeckt. Die klassische Sicherheitsgemeinde hat den Bereich der Datenbanken fast zur Gänze ignoriert; viele Datenbankadministratoren zählen üblicherweise Sicherheit nicht zu ihren Aufgaben. Die meisten Datenbanken haben zahlreiche Eigenschaften und Fähigkeiten, die missbraucht oder zur Beeinträchtigung von Vertraulichkeit, Verfügbarkeit und Integrität von Daten verwendet werden können.

Alle modernen relationalen Datenbanksysteme sind "Port-adressierbar", was bedeutet, dass jeder mit weithin verfügbaren Abfragewerkzeugen versuchen kann, sich direkt zur Datenbank zu verbinden und dabei die Sicherheitsmechanismen des Betriebssystems umgeht. Zum Beispiel kann auf Oracle über den Port 1521/TCP, auf MySQL über den Port 3306/TCP und auf PostgreSQL über den Port 5432/TCP zugegriffen werden. Die meisten Datenbankanwendungen haben auch bekannte Standardbenutzerkonten und –Passwörter, die unterschiedliche Level von Zugriffen auf Datenbankressourcen und Tabellen bieten. Heute sind die meisten Datenbanken eng mit einer Frontend-Anwendung verbunden, wobei davon die meisten Webbasiert sind. Wenn eine Anwendung schlecht geschrieben oder konfiguriert ist, kann das dem Angreifer ermöglichen, eine SQL Injection-Attacke oder andere Schwachstellen von Datenbanken zu verwenden.

CERT CC hat ein Advisory, [CA-2003-05](#) über mehrere Oracle Schwachstellen, durch die die zugrunde liegende Datenbank kompromittiert werden könnte, veröffentlicht. Von einiger Zeit hat auch das US-CERT ein Advisory über SQL-Injection Schwachstellen in der Oracle E-Business Suite ([TA04-160A](#)), die zur Kompromittierung der Datenbankanwendung und der Integrität der Daten führen kann, veröffentlicht.

Ähnlich hat auch MySQL ein paar Schwachstellen. Eine kurze Beschreibung einiger häufiger Attacken auf MySQL kann in einem aktuellen Paper von Next Generation Software, <http://www.nextgenss.com/papers/HackproofingMySQL.pdf>, gefunden werden.

U9.2 Betroffene Betriebssysteme

Beinahe alle Linux-Systeme werden mit einer Version von Open-Source-DBMS wie MySQL oder PostgreSQL oder kommerziellen DBMS-Lösungen wie Oracle geliefert. Einige UNIX-Flavors wie Solaris, AIX oder HP-UX unterstützen Oracle, DB2 und andere große kommerzielle Datenbanken genau so wie die meisten Open-Source-DBMS.

U9.3 CVE/CAN Einträge

Oracle:

CVE-2002-0567, CVE-2002-0571

CAN-1999-0652, CAN-1999-1256, CAN-2002-0858, CAN-2002-1264, CAN-2003-0095, CAN-2003-0096, CAN-2003-0222, CAN-2003-0634, CAN-2003-0727, CAN-2003-0894

MySQL:

CVE-1999-1188, CVE-2000-0045, CVE-2000-0148, CVE-2000-0981, CVE-2001-0407

CAN-1999-0652, CAN-2001-1274, CAN-2001-1275, CAN-2002-0229, CAN-2002-0969, CAN-2002-1373, CAN-2002-1374, CAN-2002-1375, CAN-2002-1376, CAN-2003-0073, CAN-2003-0150, CAN-2003-0515, CAN-2003-0780, CAN-2004-0381, CAN-2004-0388, CAN-2004-0627, CAN-2004-0628

PostgreSQL:

CVE-2002-0802

CAN-1999-0862, CAN-2000-1199, CAN-2001-1379, CAN-2002-0972, CAN-2002-1397, CAN-2002-1398, CAN-2002-1399, CAN-2002-1400, CAN-2002-1401, CAN-2002-1402, CAN-2003-0040, CAN-2003-0500, CAN-2003-0515, CAN-2003-0901, CAN-2004-0366, CAN-2004-0547

U9.4 Wie Sie herausfinden, ob Sie betroffen sind

Stellen Sie sicher, dass alle DBMS, die mit einem Betriebssystem geliefert werden die aktuellste Version verwenden. Ungepatchte oder veraltete Versionen von Datenbanken sind wahrscheinlich verwundbar.

Standardinstallationen von DBMS haben wahrscheinlich Schwachstellen, die von Angreifern ausgenutzt werden können.

Führen Sie einen Scan nach Schwachstellen auf den Systemen durch um herauszufinden, ob die DBMS-Software verwundbar ist:

- [MySQL Network Scanner](#): erlaubt das Scannen des gesamten Netzwerks nach MySQL-Servern mit dem Standard-Passwort (leer) und könnte auch "illegale" Server aufstöbern.
- Der Open-Source Netzwerk-Schwachstellen-Scanner Nessus (<http://www.nessus.org>) hat auch Tests für übliche Löcher in Datenbanken unter Unix.
- Kommerzielle Schwachstellenscanner wie Foundstone, Qualys oder eEye Retina können auch verwendet werden um Schwachstellen in Datenbanken zu finden
- Zusätzlich gibt es auch spezielle Datenbankscanner wie AppSecInc oder ISS Database Scanner.

U9.5 Wie Sie sich dagegen schützen können

Als erstes ist es wichtig, sicherzustellen, dass die Datenbankanwendungen auf den aktuellsten verfügbaren Patchlevel gepatcht werden. Suchen Sie auf den entsprechenden Herstellerseiten

nach Patchinformationen:

- Oracle (<http://otn.oracle.com/software/index.html>)
- MySQL (<http://www.mysql.com/products/mysql/>)
- PostgreSQL (<ftp://ftp.postgresql.org/pub>)

Als nächstes stellen Sie sicher, dass das DBMS und die Anwendungen angesichert wurden:

- Verwendung der geringstmöglichen Rechte.
- Entfernen/Ändern Sie Standardpasswörter auf den privilegierten und System-Konten der Datenbank bevor Sie das System mit dem Netzwerk verbinden.
- Verwenden Sie, wo möglich, stored procedures.
- Entfernen/deaktivieren Sie nicht benötigte stored procedures.
- Definieren Sie Limits für alle Felder.
- Validieren Sie alle Daten auf dem Server (Länge, Format, Typ).

Es gibt einige nützliche Ressourcen, die bei der Absicherung von DBMS hilfreich sind:

- Oracle (<http://otn.oracle.com/deploy/security/index.html>)
- MySQL (<http://dev.mysql.com/doc/mysql/en/Security.html>)
- PostgreSQL (<http://www.postgresql.org/docs/7/interactive/security.htm>)

Bleiben Sie am aktuellen Stand mit den Informationen über Schwachstellen, die von den Herstellern veröffentlicht wurden:

- Oracle Security Alerts (<http://otn.oracle.com/deploy/security/alerts.htm>)
- MySQL (<http://lists.mysql.com/>)
- PostgreSQL (<http://www.postgresql.org/lists.html>)

Das SANS Institute hat eine umfassende Sicherheitscheckliste für Oracle veröffentlicht, die nützlich für eine Prüfung einer Oracle Datenbank Installation ist:
<http://www.sans.org/score/oraclechecklist.php>

Das [Center for Internet Security](#) hat auch ein [Oracle Database Benchmark Tool](#) entwickelt, das hilfreich ist um die Sicherheit der Datenbank zu bewerten:
http://www.cisecurity.org/bench_oracle.html

[SANS Security Oracle Step-by-Step](#) liefert nützliche und praktische Tipps zum Härten von Oracle.

Schlussendlich kann zusätzliche Information über die Sicherheit von Datenbanken hier gefunden werden:

- [SANS Reading Room on Database Security](#)
- <http://www.petefinnigan.com/orasec.htm>

[zum Anfang ^](#)

U10.1 Beschreibung

Die zentrale Komponente eines Betriebssystems ist der Kernel. Der Kernel ist für eine Reihe von Low-Level-Interaktionen zwischen dem Betriebssystem und Hardware, Speicher, Scheduling, Interprozesskommunikation Dateisystemen und anderen Komponenten verantwortlich. Da der Kernel privilegierten Zugang zu allen Aspekten des Systems hat, kann ein kompromittierter Kernel verheerend sein. Die Risiken von Kernel Schwachstellen inkludieren Denial of Service, Ausführen von beliebigen Code mit System-Privilegien, uneingeschränkter Zugriff auf die Dateisysteme oder root-Zugang. Viele Schwachstellen können von außerhalb des Systems ausgenutzt werden und sind besonders gefährlich, wenn das über einen im Internet veröffentlichten Dienst passiert. In einigen Fällen kann der Kernel durch ein verformtes ICMP-Paket in einer Schleife hängen bleiben, dadurch alle CPU Ressourcen verbrauchen und so die Maschine nutzlos machen, also ein Denial of Service verursachen.

Richtiges Tuning des Kernels kann nicht nur Ihr System vor Angriffen schützen, sondern es steigert auch die Leistung des Systems.

U10.2 Betroffene Betriebssysteme

Nahezu alle Unix-Varianten einschließlich Solaris und HP-UX, Linux Distributionen, BSD Versionen und Windows Versionen haben Kernel-Schwachstellen gehabt, entweder im Kernel selbst oder durch Fehler in Anwendungen, die entsprechend den Kernel betreffen

U10.3 CVE/CAN Einträge

[CVE-1999-0295](#), [CVE-1999-0367](#), [CVE-1999-0482](#), [CVE-1999-0727](#), [CVE-1999-0804](#),
[CVE-1999-1214](#), [CVE-1999-1339](#), [CVE-1999-1341](#), [CVE-2000-0274](#), [CVE-2000-0375](#),
[CVE-2000-0456](#), [CVE-2000-0506](#), [CVE-2000-0867](#), [CVE-2001-0062](#), [CVE-2001-0268](#),
[CVE-2001-0316](#), [CVE-2001-0317](#), [CVE-2001-0859](#), [CVE-2001-0993](#), [CVE-2001-1166](#),
[CVE-2002-0046](#), [CVE-2002-0766](#), [CVE-2002-0831](#)

[CAN-1999-1166](#), [CAN-2000-0227](#), [CAN-2001-0907](#), [CAN-2001-0914](#), [CAN-2001-1133](#),
[CAN-2001-1181](#), [CAN-2002-0279](#), [CAN-2002-0973](#), [CAN-2003-0127](#), [CAN-2003-0247](#),
[CAN-2003-0248](#), [CAN-2003-0418](#), [CAN-2003-0465](#), [CAN-2003-0955](#), [CAN-2003-0984](#),
[CAN-2004-0003](#), [CAN-2004-0010](#), [CAN-2004-0177](#), [CAN-2004-0482](#), [CAN-2004-0495](#),
[CAN-2004-0496](#), [CAN-2004-0497](#), [CAN-2004-0554](#), [CAN-2004-0602](#)

U10.4 Wie Sie herausfinden, ob Sie betroffen sind

Es gibt einige Wege um herauszufinden, ob der Kernel angreifbar ist:

- Wenn der Hersteller dies anbietet, registrieren Sie sich für Mails über Sicherheitsupdates, wenn Sie die Software registrieren.
- Die meisten der Sicherheitsmailinglisten veröffentlichen Kernel-Schwachstellen sobald diese bekannt sind.
- Das Nachverfolgen der Version der auf einem System verwendeten Kernel sollte Teil der Standardprozeduren sein.
- Software zur Sicherheitsbewertung kann verwendet werden um die Version des auf einem

System verwendeten Kernel herauszufinden. Nessus hat eine Reihe von Plugins um Systeme auf Kernelschwachstellen zu überprüfen *Achtung*: viele dieser Plugins können Denial of Service-Bedingungen hervorrufen und Sie sollten Ihre Systeme vorsichtig scannen, um unvorhergesehene Ausfälle zu vermeiden.

U10.5 Wie Sie sich dagegen schützen können

Es gibt zwei Klassen von Parametern, die in Kernen konfiguriert werden können um Angriffe zu vereiteln. Eine Klasse wird benutzt um die Systemressourcen zu tunen um Denial of Service Angriffen und Buffer Overflows einzuschränken. Die zweite Klasse verwendet man um die Netzwerkeinstellungen gegen Angriffe aus dem Netzwerk zu härten. Diese Befehle und Parameter sind Plattform-spezifisch. Um zu verstehen, wie man den Kernel richtig einstellt, sollte Plattform-spezifische Dokumentation zu Rate gezogen werden.

Es ist empfehlenswert, dass alle Modifikationen gründlich vor der Implementierung in einer Produktionsumgebung getestet werden, und dass Backups gemacht und griffbereit gehalten werden, falls Probleme auftauchen.

Es gibt einige nützliche Ressourcen um Ihnen beim Straffen des Systems durch richtiges Tunen des Kernels zu helfen.

[Solaris Tunable Parameters Reference Manual \(Solaris 8\)](#)
[Solaris Tunable Parameters Reference Manual \(Solaris 9\)](#)
[Solaris Operating Environment Network Settings for Security](#)
[Solaris Kernel Tuning for Security](#) oder <http://www.securityfocus.com/infocus/1385>

[Linux Kernel Hardening](#)
[The Linux Kernel Archives](#)
[Linux Kernel Hardening](#)

[AIX Kernel Tuning](#)

[HP-UX Kernel Tuning and Performance Guide](#)

<http://docs.hp.com/hpux/pdf/5185-6559.pdf>
<http://docs.hp.com/hpux/pdf/TKP-90203.pdf>
<http://docs.hp.com/cgi-bin/otsearch/hpsearch>
<http://docs.hp.com/>

FreeBSD Handbook (enthält Informationen über das Tuning von Kernels):
http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/index.html

OpenBSD:
<http://www.openbsd.org/faq/index.html>
<http://www.openbsd.org/docum.html> (für weitere Informationen)

[NetBSD Tuning, Kernel Tuning](#)

[zum Anfang ^](#)

Appendix A Common Vulnerable Ports

In diesem Abschnitt führen wir die Ports an die üblicherweise untersucht und angegriffen werden. Diese Ports zu blockieren ist die Mindestanforderung für die Absicherung des zu schützenden Bereiches und stellt keine umfassende Spezifikationsliste für Firewalls dar. Ein weitaus besserer Ansatz ist es, alle nicht benötigten Ports zu blockieren, das heißt den gesamten Verkehr zu blockieren und anschließend jene Protokolle von Außen zu erlauben, die für Ihr Unternehmen notwendig sind. Sogar wenn Sie der Meinung sind, dass diese Ports blockiert werden, sollten Sie sie dennoch aktiv beobachten um Einbruchversuche zu entdecken. Eine Warnung ist an dieser Stelle angebracht: das Blockieren einiger der Ports in der folgenden Liste kann benötigte Dienste verhindern. Bitte bedenken Sie die möglichen Auswirkungen dieser Empfehlungen bevor Sie sie implementieren.

Hinweis: Es ist auch wichtig aufzuzeigen, dass im Allgemeinen die Meinung herrscht, dass standardmäßig alles zu blockieren ist was nicht explizit erlaubt wurde. Das ist eine viel effektivere Vorgehensweise als nur bestimmte Ports zu sperren. Dieser Ansatz ist außerdem leichter auf Routern und Firewalls zu warten, da deren Konfigurationen und Kontrolllisten dazu tendieren, kürzer und logischer zu sein.

Bedenken Sie, dass das Blockieren dieser Ports kein Ersatz für umfassende Sicherheitsvorschriften und –planung ist. Sogar wenn diese Ports blockiert werden, kann ein Angreifer, der über andere Wege in Ihr Netzwerk gelangt (z.B.: Modem, Trojaner als E-mail-Attachment, Angriff eines Users von innen oder eine kompromittierte Maschine), diese Ports ausnützen, wenn sie nicht auf allen Systemen in Ihrer Organisation ordentlich gesichert sind.

Name	Port	Protokoll	Beschreibung
Small services	<20	tcp/udp	small services
FTP	21	tcp	file transfer
SSH	22	tcp	Anmeldedienst
TELNET	23	tcp	Anmeldedienst
SMTP	25	tcp	Mail
TIME	37	tcp/udp	Zeitsynchronisation
WINS	42	tcp/udp	WINS Replication
DNS	53	udp	Name Server
DNS Zone transfers	53	tcp	Name Server
DHCP Server	67	tcp/udp	host configuration
DHCP Client	68	tcp/udp	host configuration
TFTP	69	udp	Diverses
GOPHER	70	tcp	alter WWW-ähnlicher Dienst
FINGER	79	tcp	Diverses
http	80	tcp	Web
alternate HTTP port	81	tcp	Web
alternate HTTP port	88	tcp	web (manchmal Kerberos)

LINUXCONF	98	tcp	host configuration
POP2	109	tcp	Mail
POP3	110	tcp	Mail
PORTMAP/RPCBIND	111	tcp/udp	RPC portmapper
NNTP	119	tcp	Network News Dienst
NTP	123	udp	Zeitsynchronization
NetBIOS	135	tcp/udp	DCE-RPC endpoint mapper
NetBIOS	137	udp	NetBIOS name service
NetBIOS	138	udp	NetBIOS datagram service
NetBIOS/SAMBA	139	tcp	file sharing & login service
IMAP	143	tcp	Mail
SNMP	161	tcp/udp	Netzwerkmanagement
SNMP	162	tcp/udp	Netzwerkmanagemen
XDMCP	177	udp	X display manager protocol
BGP	179	tcp	Diverses
FW1-secureremote	256	tcp	CheckPoint FireWall-1
FW1-secureremote	264	tcp	CheckPoint FireWall-1
LDAP	389	tcp/udp	Verzeichnisdienst
HTTPS	443	tcp	Web
Windows 2000 NetBIOS	445	tcp/udp	SMB over IP (Microsoft-DS)
ISAKMP	500	udp	IPSEC Internet Key Exchange
REXEC	512	tcp	} die drei
RLOGIN	513	tcp	} Berkeley r-Dienste
RSHELL	514	tcp	} (für remote login)
RWHO	513	udp	Diverses
SYSLOG	514	udp	Diverses
LPD	515	tcp	remote printing
TALK	517	udp	Diverses
RIP	520	udp	routing protocol
UUCP	540	tcp/udp	file transfer
HTTP RPC-EPMAP	593	tcp	HTTP DCE-RPC endpoint mapper
IPP	631	tcp	remote printing
LDAP over SSL	636	tcp	LDAP over SSL
Sun Mgmt Console	898	tcp	remote administration
SAMBA-SWAT	901	tcp	remote administration
Windows RPC programs	1025	tcp/udp	} oft allociert
Windows RPC programs	Bis		} vom DCE-RPC portmapper
Windows RPC programs	1039	tcp/udp	} auf Windows hosts
SOCKS	1080	tcp	Diverses
LotusNotes	1352	tcp	Datenbank/Groupware
MS-SQL-S	1433	tcp	Datenbank
MS-SQL-M	1434	udp	Datenbank

CITRIX	1494	tcp	remote graphical display
WINS replication	1512	tcp/udp	WINS replication
ORACLE	1521	tcp	Datenbank
NFS	2049	tcp/udp	NFS file sharing
COMPAQDIAG	2301	tcp	Compaq remote administration
COMPAQDIAG	2381	tcp	Compaq remote administration
CVS	2401	tcp	collaborative file sharing
SQUID	3128	tcp	web cache/proxy
Global catalog LDAP	3268	tcp	Global catalog LDAP
Global catalog LDAP SSL	3269	tcp	Global catalog LDAP SSL
MYSQL	3306	tcp	Datenbank
Microsoft Term. Svc.	3389	tcp	remote graphical display
LOCKD	4045	tcp/udp	NFS file sharing
Sun Mgmt Console	5987	tcp	remote administration
PCANYWHERE	5631	tcp	remote administration
PCANYWHERE	5632	tcp/udp	remote administration
VNC	5800	tcp	remote administration
VNC	5900	tcp	remote administration
X11	6000-6255	tcp	X Windows server
FONT-SERVICE	7100	tcp	X Windows font service
alternate HTTP port	8000	tcp	Web
alternate HTTP port	8001	tcp	Web
alternate HTTP port	8002	tcp	Web
alternate HTTP port	8080	tcp	Web
alternate HTTP port	8081	tcp	Web
alternate HTTP port	8888	tcp	Web
Unix RPC programs	32770	tcp/udp	} oft allociert
Unix RPC programs	Bis		} vom RPC portmapper
Unix RPC programs	32899	tcp/udp	} auf Solaris hosts
COMPAQDIAG	49400	tcp	Compaq remote administration
COMPAQDIAG	49401	tcp	Compaq remote administration
PCANYWHERE	65301	tcp	remote administration

ICMP: blockieren Sie eingehende echo request (ping und Windows traceroute), ausgehende echo replies, time exceeded, und destination unreachable Nachrichten außer "packet too big" Nachrichten (Typ 3, Code 4). (In diesem Punkt wird angenommen, dass Sie bereit sind manche der legitimierten Anwendungen von ICMP echo request aufzugeben um manche bekannten bösartigen Anwendungen zu verhindern.)

Zusätzlich zu diesen Ports, blockieren Sie gespoofte Adressen: Pakete, die von außerhalb Ihres Unternehmens kommen mit einer Source-Adresse von innerhalb Ihres Netzwerks, privaten Adresse (RFC 1918) und von der IANA reservierten Adressen (für Details, lesen Sie bitte <http://www.iana.org/assignments/ipv4-address-space>). Außerdem wird empfohlen, dass Sie Pakete an Broadcast- und

Multicast-Adressen blockieren. Blockieren von source route-Paketen oder allen Paketen mit gesetzten IP Optionen ist auch von Vorteil.

Sie sollten auch Ausgangsfilter auf den Border-Routern setzen um gespoofte Pakete von innerhalb Ihres Netzes zu blockieren. Erlauben Sie nur, dass Pakete, mit denen von Ihnen zugewiesenen Adressen Ihr Netzwerk verlassen können.


Anerkennung von Warenzeichen: SANS Institute anerkennt die Wichtigkeit von geistigem Eigentum, Warenzeichen, Urheberrecht, Dienstleistungsmerkmale und Patenten und ist bemüht, diese Standards in diesem Dokument anzuerkennen. Die folgenden Produkte, Systeme oder Applikationen sind als Markennamen anerkannt. Wenn Sie der Meinung sind, dass wir Markenprodukte übersehen haben, schicken Sie bitte Ihre Kommentare und Beobachtungen per E-Mail an top20@sans.org, und wir stellen sicher, dass dieses Dokument entsprechend korrigiert wird.

Microsoft, Windows, Windows Server 2003, Microsoft SQL Server, Microsoft Outlook sind Warenzeichen oder eingetragene Warenzeichen der Microsoft Corporation in den U.S.A und/oder anderen Ländern.

Sendmail, ist ein Warenzeichen oder eingetragenes Warenzeichen der Sendmail, Inc. in den U.S.A und/oder anderen Ländern.

SSH ist ein Warenzeichen oder eingetragenes Warenzeichen der SSH Communication Security in den U.S.A und/oder anderen Ländern.

CERT Coordination Center ist ein Warenzeichen oder eingetragenes Warenzeichen des Carnegie Mellon; Software Engineering Institute in den U.S.A und/oder anderen Ländern.

UNIX Warenzeichen oder eingetragene Warenzeichen  der The Open Group in den U.S.A und/oder anderen Ländern.

[zum Anfang ^](#)

Appendix B

Die Spezialisten, die mitgeholfen haben, die Liste der Top 20 Schwachstellen 2003 zu schreiben

Adair Collins, US Department of Energy
Alan Paller, SANS Institute
Alex Lucas, United Kingdom National Infrastructure Security Co-ordination Center
Alexander Kotkov, CCH Legal Information Services
Anton Chuvakin, Ph.D., netForensics
BJ Bellamy, Kentucky Auditor of Public Accounts
Bradley Peterson, US Department of Energy
Cathy Booth, United Kingdom National Infrastructure Security Co-ordination Center - Incident Response CESG
Chris Benjes, National Security Agency
Christopher Misra, University of Massachusetts Amherst
Dave Dobrotka, Ernst & Young
Dominic Beecher, United Kingdom National Infrastructure Security Co-ordination

Ed Fisher, CableJiggler Consulting, LLC
Edward Skoudis, International Network Services
Edward W. Ray, MMICMAN LLC
Erik Kamerling, Pragmeta Networks/SANS Institute - Editor
Gerhard Eschelbeck, Qualys
Jeff Campione, Editor 2002
Jeff Ito, Indus Corporation
Jeni Li, Arizona State University
Kevin Thacker, United Kingdom National Infrastructure Security Co-ordination
Koon Yaw Tan, Infocomm Development Authority of Singapore (IDA)
Pedro Paulo Ferreira Bueno, MetroRED Telecom, Brazil
Pete Beck, United Kingdom National Infrastructure Security Co-ordination
Richard (Rick) Wanner, InfoSec Centre of Expertise (COE) CGI Information Systems
& Management Consultants Inc.
Roland M Lascola, U.S. Dept. of Energy - Office of Independent Oversight and
Performance Assurance
Ross Patel, Afentis Security
Russell Morrison, AXYS Environmental Consulting Ltd.
Scott A. Lawler, CISSP, Veridian Information Solutions
Stephen Northcutt, SANS Institute
Valdis Kletnieks, Virginia Tech
William Eckroade, U.S. Dept. of Energy

**Dank an die folgenden Personen für ihre hervorragende Arbeit beim editieren,
formatieren und produzieren dieser 2003 Liste**

Audrey (Dalas) Bines, SANS Institute
Brian Corcoran, SANS Institute
Cara L. Mueller, SANS Institute

**Das Top 20 Team möchte sich auch bei den folgenden SANS Absolventen bedanken, die
ihre Zeit geopfert haben, um die Top 20 Liste zu überprüfen und zu kommentieren**

Paul Graham, CIT at the University at Buffalo (UB)
Jerry Berkman, UC Berkeley
Neil W Rickert, Northern Illinois University
Travis Hildebrand, US Department of Veteran Affairs
Christoph Gruber, WAVE Solutions
Mark Worthington, Affiliated Computer Services (ACS), Riverside Public Library
Matthew Nehawandian, CISSP

**Die Spezialisten, die mitgeholfen haben, die Liste der Top 20 Schwachstellen 2002 zu
schreiben**

Jeff Campione, Federal Reserve Board - Editor
Eric Cole, Editor, 2001 Edition
Ryan C. Barnett, Department of the Treasury/ATF
Chris Benjes, National Security Agency
Matt Bishop, University of California, Davis
Chris Brenton, SANS Institute
Pedro Paulo Ferreira Bueno, Open Communications Security, Brazil
Anton Chuvakin, Ph.D., netForensics

Rob Clyde, Symantec
Dr. Fred Cohen, Sandia National Laboratories
Gerhard Eschelbeck, Qualys
Dan Ingevaldson, Internet Security Systems
Erik Kamerling, Pragmeta Networks
Gary Kessler, Gary Kessler Associates
Valdis Kletnieks, Virginia Tech CIRT
Alexander Kotkov - CCH Legal Information Services
Jamie Lau, Internet Security Systems
Scott Lawler, Veridias Information Solutions
Jeni Li, Arizona State University
Nick Main, Cerberus IT, Australia
Jose Marquez, Alutiq Security and Technology
Christopher Misra, University of Massachusetts
Stephen Northcutt, SANS Institute
Craig Ozancin, Symantec
Alan Paller, SANS Institute
Ross Patel, Afentis, UK
Marcus Ranum, ranum.com
Ed Ray - MMICMAN LLC
Chris Rouland, Internet Security Systems
Bruce Schneier, Counterpane Internet Security Inc.
Greg Shipley, Neohapsis
Ed Skoudis, Predictive Systems
Gene Spafford, Purdue University CERIAS
Koon Yaw Tan, Infocomm Development Authority of Singapore
Mike Torregrossa, University of Arizona
Viriya Upatising, Loxley Information Services, Thailand
Rick Wanner, CGI Information Systems and Management Consultants

Personen, die mitgeholfen haben, die einzelnen CVE Einträge zu priorisieren und die Tests für die Top 20 Scanner 2002 definiert haben. Details zu diesem Ablauf finden Sie unter www.sans.org/top20/testing.pdf

Charles Ajani, Standard Chartered Bank, London, UK
Steven Anderson, Computer Sciences Corporation, North Kingstown RI
John Benninghoff, RBC Dain Rauscher, Minneapolis MN
Layne Bro, BEA Systems, Denver CO
Thomas Buehlmann, Phoenix AZ
Ed Chan, NASA Ames Research Center, San Jose CA
Andrew Clarke, Computer Solutions, White Plains NY
Brian Coogan, ManageSoft, Melbourne Australia
Paul Docherty, Portcullis Computer Security Limited, UK
Arian Evans, U.S. Central Credit Union, Overland Park KS
Rich Fuchs, Research Libraries Group, Mountain View CA
Mark Gibbons, International Network Services, Minneapolis MN
Dan Goldberg, Rochester NY
Shan Hemphill, Sacramento CA
Michael Hensing, Charlotte, NC, Microsoft
Simon Horn, Brisbane Australia
Bruce Howard, Kanwal Computing Solutions, Jilliby NSW Australia
Tyler Hudak, Akron OH
Delbert Hundley, MPRI Division of L-3COM, Norfolk VA

Chyuan-Horng Jang, Oak Brook IL
Kim Kelly, The George Washington University, Washington DC
Martin Khoo, Singapore Computer Emergency Response Team (SingCERT),
Singapore
Susan Koski, Pittsburgh PA
Kevin Liston, AT&T, Columbus OH
Andre Marien, Ubizen, Belgium
Fran McGowran, Deloitte & Touche, Dublin, Ireland, UK
Derek Milroy, Zurich North America, Chicago IL
Bruce Moore, Canadian Forces Network Operations Center, DND, Ottawa Canada
Castor Morales, Ft. Lauderdale FL
Luis Perez, Boston MA
Reg Quinton, University of Waterloo, Ontario Canada
Bartek Raszczyk, UWM Olsztyn, Olsztyn Poland
Teppo Rissanen, Plasec Oy, Helsinki Finland
Alan Rouse, N2 Broadband, Duluth GA
Denis Sanche, PWGSC ITSD/IPC, Hull, QC Canada
Felix Schallock, Ernst & Young, Vienna, Austria
Gaston Sloover, Fidelitas, Buenos Aires Argentina
Arthur Spencer, UMASS Medical School, Worcester MA
Rick Squires
Jeff Stehlin, HP
Koon Yaw TAN, Infocomm Development Authority of Singapore, Singapore
Steven Weil, Seitel Leeds & Associates, Seattle WA
Lance Wilson, Time Warner Cable/Broadband IS, Orlando FL
Andrew Wortman, Naval Research Laboratory, Washington DC
Carlos Zottman, Superior Tribunal de Justica, Brasilia Brazil

**Zusätzliche Spezialisten, die bei der Top 10 Liste 2000 und der Top 20 Liste 2001
geholfen haben, welche die Grundlage für die Top 20 Liste 2002 bildet**

Billy Austin, Intrusion.com
Phil Benchoff, Virginia Tech CIRT
Tina Bird, Counterpane Internet Security Inc.
Lee Brotzman, NASIRC Allied Technology Group Inc.
Mary Chaddock
Steve Christey, MITRE
Scott Conti, University of Massachusetts
Kelly Cooper, Genuity
Scott Craig, KMart
Sten Drescher, Tivoli Systems
Kathy Fithen, CERT Coordination Center
Nick FitzGerald, Computer Virus Consulting Ltd.
Igor Gashinsky, NetSec Inc.
Bill Hancock, Exodus Communications
Robert Harris, EDS
Shawn Hernan, CERT Coordination Center
Bill Hill, MITRE
Ron Jarrell, Virginia Tech CIRT
Jesper Johansson, Boston University
Christopher Klaus, Internet Security Systems
Clint Kreitner, Center for Internet Security
Jimmy Kuo, Network Associates Inc.

Jim Magdych, Network Associates Inc.
Dave Mann, BindView
Randy Marchany, Virginia Tech
Mark Martinec "Jozef Stefan" Institute
William McConnell, Trend Consulting Services
Peter Mell, National Institutes of Standards and Technology
Larry Merritt, National Security Agency
Mudge, @stake
Tim Mullen, AnchorIS.com
Ron Nguyen, Ernst & Young
David Nolan, Arch Paging
Hal Pomeranz, Deer Run Associates
Chris Prorise, Foundstone Inc.
Jim Ransome
RAZOR Research - BindView Development
Martin Roesch, Snort
Vince Rowe, FBI, NIPC
Marcus Sachs, JTF-CNO US Department of Defense
Tony Sager, National Security Agency
Gene Schultz, Lawrence Berkeley Laboratory
Eric Schultze, Foundstone
Derek Simmel, Carnegie Mellon University
Ed Skoudis, Predictive Systems
Lance Spitzner, Sun Microsystems, GESS Team
Wayne Stenson, Honeywell
Jeff Stutzman
Frank Swift
Bob Todd, Advanced Research Corporation
Jeff Tricoli, FBI NIPC
Laurie Zirkle, Virginia Tech CIRT

Spezialisten, die diese Top 20 Liste übersetzt haben

Andreas Floriani / Oesterreichische Nationalbank
Hans Chvojka
Jess Garcia / LAEFF-INTA

[zum Anfang ^](#)