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

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 vom Würmern, wie Blaster, Slammer und Code Red können auf Systeme zurückgeführt werden, die Patches nicht installiert haben.

Vor drei 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

Top Schwachstellen in UNIX Systemen

- 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 Internet Information Services (IIS)

W1.1 Beschreibung

Die standardmäßige Installationen der Internet Information Services ist bekannterweise 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
- Komplette Kompromittierung des Servers

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), Server Side Includes (SSI) und webbasierendes Druckersharing zu verarbeiten. Viele der ISAPI Filter, die mit dem IIS standardmäßig 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.

Wie viele Webserver, enthält IIS auch Applikationsbeispiele, die dazu dienen, die Funktionalität des Webservers 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.

Eine IIS Installation die nicht ordnungsgemäß instand gehalten wird, ist ebenfalls anfällig für Schwachstellen, die seit der Softwareveröffentlichung bekannt geworden sind. Beispiele dafür sind die WebDAV ntdll.dll Schwachstelle in Version 5, die Denial of Service Attacken ermöglichen und die es jeden Besucher einer Webseite ermöglichen, Scripts auf dem Server auszuführen oder die Unicode Schwachstelle, wodurch die Ausführung von beliebigen Befehlen beim Besuch einer anfälligen Webseite durch speziell geschriebene URLs ermöglicht wird.

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.

Zusätzliche Information über die letzten WebDAV spezifischen Sicherheitsschwachstellen (CAN-2003-0109 CA-2003-09) können auf den folgenden Seiten gefunden werden.

http://www.cert.org/advisories/CA-2003-09.html

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0109
http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q241520

W1.2 Betroffene Betriebssysteme
Windows NT 4 (alle Versionen) mit IIS 4
Windows 2000 Server mit IIS 5
Windows XP Professional mit IIS 5.1

Zur Zeit des Schreibens waren keine Schwachstellen in Windows 2003 mit IIS6 bekannt; es ist aber vorstellbar, dass Schwachstellen gefunden werden, wenn das Produkt in größerem Masse eingesetzt wird.

W1.3 CVE/CAN Einträge
CVE-1999-0264, CVE-1999-0278, CVE-1999-0874, CVE-1999-0237, CVE-1999-0191, CVE-2000-0770, CVE-2000-0778, CVE-2000-0884, CVE-2000-0886, CVE-2000-0226, CVE-2001-0151, CVE-2001-0241, CVE-2001-0333, CVE-2001-0500, CVE-2001-0507

CAN-1999-0509, CAN-1999-0736, CAN-1999-1376, CAN-2002-0071, CAN-2002-0073, CAN-2002-0079, CAN-2002-0147, CAN-2002-0149, CAN-2002-0150, CAN-2002-0364, CAN-2002-0419, CAN-2002-0421, CAN-2002-0422, CAN-2002-0869, CAN-2002-1180, CAN-2002-1181, CAN-2002-1182, CAN-2002-1309, CAN-2002-1310, CAN-2003-0109, CAN-2003-0223, CAN-2003-0224, CAN-2003-0225, CAN-2003-0226, CAN-2003-0227, CAN-2003-0349

W1.4 Wie Sie herausfinden, ob Sie betroffen sind
Standardmäßig installierte oder nicht aktualisierte IIS Installationen können als anfällig eingestuft werden.

System- oder Netzwerkadministratoren, die für den IIS Einsatz verantwortlich sind, sollten sich mit den Microsoft Werkzeugen vertraut machen und die Sicherheitsdokumentationen lesen, die für die ordnungsgemäße Administration von Internet Information Servern zur Verfügung stehen.

Die Hauptquelle für IIS Sicherheitsdokumente ist das Internet Information Server (IIS) Security Center.

Es wird empfohlen, dass Sie den Microsoft Baseline Security Analyzer herunterladen und ausführen, dieser enthält Erkennungsprozeduren, die für den IIS zugeschnitten sind.

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 dagegen schützen können
Installieren Sie die letztgültigen Sicherheitspatches und halten Sie ihre Systeme aktuell.

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 AutoUpdate sind Möglichkeiten für Einzelinstallationen. HFNetChk, 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.

Wenn Sie Zusatzsoftware von Drittfirmen wie ColdFusion, PerlIIS oder PHP verwenden, denken Sie daran, die Webseiten der Softwareanbieter zu besuchen und etwaige Patches zu installieren und Konfigurationshinweise zu beachten. Microsoft stellt natürlich keine Patches für Programme Dritter zur Verfügung.

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 Sie die folgenden empfohlenen Änderungen der IIS Installation durchführen:

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

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.asp heruntergeladen werden.

zum Anfang ^

W2 Microsoft SQL Server (MSSQL)

W2.1 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 MQSQL 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:

1. SQL/MSDE Server 2000 (Developer, Standard und Enterprise Edition)
2. Visual Studio .NET (Architect, Developer und Professional Edition)
3. ASP.NET Web Matrix Tool
4. Office XP
5. Access 2002
6. 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.

W2.2 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

W2.4 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, dass 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.

W2.5 Wie Sie sich dagegen schützen können

Zusammenfassung:

1. Das Monitorservice für SQL/MSDE auf UDP Port 1434 ausschalten.
2. Die letztgültigen Service Packs für Microsoft SQL/MSDE Server und/oder MSDE 2000 installieren.
3. Die letztgültigen Sammelpatches installieren, die nach dem letzten Service Pack erschienen sind.
4. Die letztgültigen Patches installieren, die nach dem letzten Sammelpatch erschienen sind.
5. SQL Server Authentication Logging einschalten.
6. Die Server auf System- und Netzwerkebene sicher einstellen.
7. Die Rechte des MSSQL/MSDE-Server Dienstes und des SQL/MSDE Server Agents minimieren.

Im Einzelnen:

1. Das Monitorservice 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:

   - SQL/MSDE Server 7.0 Service Pack 4
   - 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:

- Microsoft SQL/MSDE Server 7.0
- Microsoft SQL Server 2000
- 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:

   - Microsoft SQL/MSDE Server 7.0
   - Microsoft SQL Server 2000
   - 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 Wurmattacke 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 ^

W3 Windows Authentifizierung

W3.1 Beschreibung

Kennwörter, Passwortphrasen und Sicherheitscodes werden fast in jeder Interaktion zwischen Anwendern und Systemen verwendet. Die meisten Arten von Anwenderauthentifizierung und auch Dateienschutz 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://www.msdn.miscrosoft.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 Kennworte 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.

W3.2 Betroffene Betriebssysteme

Alle Microsoft Windows Betriebssysteme.

W3.3 CVE/CAN Einträge

CVE-2000-0222

CAN-1999-0504, CAN-1999-0505, CAN-1999-0506

W3.4 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 Sniffern im Netzwerk gelesen werden können.

W3.5 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.

1. **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:
    1. Enthält nicht den Accountnamen, ganz oder Teile davon
    2. Muss mindestens 6 Zeichen lang sein
    3. Muss Zeichen aus drei der folgenden vier Kategorien enthalten:
    4. Großbuchstaben (A - Z)
    5. Kleinbuchstaben (a - z)
    6. Zahlen (0 - 9)
    7. 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 die 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 minimaler 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.

> **Nochmaliger 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.

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.

2. **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 wiederverwendbar 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.

3. **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.

4. **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, Richtlinienentwicklungs-leitfaden, Kennwortsicherheitsgrundlagen und Links zu verschiedenen Webseiten mit Sicherheitsrichtlinien können unter SANS Security Policy Project gefunden werden.

5. **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 stärke 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.

6. **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.

7. **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 geswitchtes Netzwerk verwenden; 2. Erkennung und Entfernung von Netzwerkkarten im "promiscous Mode" (können mit Hilfe der meisten kommerziellen Security Assessment Tools, oder bei Freeware Tools wie PromiScan oder 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 einzelnen Parameter.
- 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.
- New Registry Key to Remove LM Hashes from Active Directory and Security Account Manager

zum Anfang ^

W4 Internet Explorer (IE)

W4.1 Beschreibung

Microsoft Internet Explorer (IE) ist der Standardbrowser von Windows Systemen. Alle Versionen des Internet Explorer haben kritische Schwachstellen, wenn sie nicht aktuell mit den letztgültigen Patches betrieben werden. Ein boshafter Webadministrator kann Webseiten entwickeln, die diese Schwachstellen ausnutzen, während der Anwender diese Webseiten ansurft.

Die Schwachstellen können in mehrere Kategorien geteilt werden. Darunter sind Webseiten- oder

Windows Interface Spoofing, ActiveX Control Schwachstellen, Aktive Scripting Schwachstellen, MIME-Type und Content-Type Missinterpretation und Buffer Overflows. Die Auswirkungen können das Auslesen von Cookies, lokalen Dateien oder sonstiger Daten sein, das Ausführen von lokalen Programmen, den Download und das Ausführen von Code oder die komplette Übernahme des Systems.

W4.2 Betroffene Betriebssysteme
Diese Sicherheitsschwachstellen bestehen auf allen Windows Systeme, die Microsoft Internet Explorer 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, selbst auf Servern, die eher selten zum Browsen verwendet werden.

W4.3 CVE/CAN Einträge
CVE-2001-0002, CVE-2001-0154, CVE-2001-0339, CVE-2001-0727, CVE-2001-0875, CVE-2002-0022, CVE-2002-0027, CVE-2003-0344

CAN-2002-0190, CAN-2002-0193, CAN-2002-1258, CAN-2003-0111, CAN-2003-0113, CAN-2003-0114, CAN-2003-0233, CAN-2003-0309, CAN-2003-1328

W4.4 Wie Sie herausfinden, ob Sie betroffen sind
Wenn Sie den Internet Explorer auf Ihren Systemen verwenden und nicht die letzten cumulative security patch eingespielt haben, sind Ihre Systeme höchst wahrscheinlich anfällig. Wenn Windows-Update auf den Systemen aktiviert ist, können Sie die Systeme überprüfen, in dem Sie die Webseite http:/windowsupdate.microsoft.com ansurfen. Wenn Windows Update deaktiviert ist, können die Programme HFNetChk, Network Security Hotfix Checker oder Microsoft Baseline Security Analyzer (MBSA) verwendet werden.

Es gibt auch Online Internet Explorer Analyse Tools wie Qualys Browser Check, die zur Feststellung des Sicherheitsstatus des IE wertvolle Informationen liefern.

W4.5 Wie Sie sich dagegen schützen können
Es gibt für den Internet Explorer Version 6.0 Sicherheitspatches für diese Schwachstellen. Ältere Versionen des IE sind aber ebenfalls anfällig; für ältere Versionen sind nicht alle Patches verfügbar. Wenn Sie IE 5.5. oder eine frühere Version verwenden, wird ein Upgrade auf Version 6.0 empfohlen, da Service Packs für frühere Versionen nicht mehr zur Verfügung gestellt werden. Wenn IE 6.0 verwendet wird, sollten die letztgültigen Service Packs installiert werden, die unter Internet Explorer 6 SP1 gefunden werden können.

Es sollten auch der letzte Sammelpatch (828750) installiert werden, wodurch zusätzliche Sicherheitsschwachstellen behoben werden. Für mehr Information über die Schwachstellen, welche durch den Patch repariert werden und wie durch ordentliche Konfiguration das Risiko minimiert werden kann lesen Sie die entsprechenden Security Bulletins sowie Artikel in der Microsoft Wissensdatenbank.

Um die Systeme sicher zu halten, müssen immer die aktuellsten Sicherheitspatches installiert werden. Damit Sie immer auf dem neuesten Stand sind, verwenden Sie Windows Update, HFNetChk oder den Microsoft Baseline Security Analyzer (MSBA). Sie können auch generelle Update Informationen von der Microsoft Internet Explorer Seite erhalten.

W4.6 Wie wird der Internet Explorer sicher

Die Sicherheitseinstellungen des Internet Explorers werden folgendermaßen konfiguriert:

1. Internetoptionen unter Extras auswählen.
2. Den Sicherheits-Tab anklicken, Internet auswählen und Stufe anpassen anklicken.

   Die meisten Fehler im IE werden durch ActiveX Steuerelemente oder Active Scripting ausgenützt.

3. Unter Scripting soll in dem Punkt Einfügeoperation über ein Script zulassen Eingabeaufforderung ausgewählt. Dadurch wird verhindert, dass Informationen aus dem Clipboard automatisch ausgelesen werden können.

   Hinweis: Active Scripting sollte nicht ausgeschaltet werden, da viele Webseiten dies verwenden.

   ActiveX Steuerelemente sind nicht so populär und stellen eine größere Gefahr dar, da sie mehr Zugang auf den Systemen erlauben.

4. Wählen Sie Eingabeaufforderung bei dem Punkt Download von sicheren ActiveX Steuerelementen.
5. Wählen Sie deaktiviert bei dem Punkt Download von unsicheren ActiveX Steuerelementen.
6. Deaktivieren Sie ActiveX-Steuerelemente initialisieren und ausführen, die nicht sicher sind.

   Java Applets haben typischerweise mehr Möglichkeiten als Scripts.

7. Wählen Sie Hohe Sicherheit unter Microsoft VM für Java-Einstellungen aus um die Java Applets ordnungsgemäß in einer Sandbox auszuführen und nicht privilegierten Zugang zum System zu ermöglichen.
8. Unter Verschiedenes soll der Punkt Auf Datenquellen über Domaingrenzen hinweg zugreifen deaktiviert werden. Dadurch werden Cross-Site Scripting Attacken vermieden.

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

zum Anfang ^

W5 Windows Remote Access Services

W5.1 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 bösartigen 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 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 Registierungszugriffen führen. Angreifer können diese Besonderheit ausnutzen um das System zu kompromittieren oder um Dateitypen oder Rechte so zu verändern, dass bösartiger 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, bösartigen 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.

W5.2 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.

W5.3 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

W5.4 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 Ihnen erleichtern, festzustellen, ob Ihre Systeme auf NETBIOS bezogene Schwachstellen anfällig sind.

NAT (NETBIOS Auditing Tool) ist von Afentis Security verfügbar. NAT versucht, das NETBIOS Dateifreigabeservice, das auf Zielsystemen verfügbar ist, Schritt für Schritt zu erforschen bevor ein Zugriff auf Systemebene versucht wird. NAT ist unter der GNU General Public Lizenz
http://www.afentis.com/resources/win32/nat/ verfügbar.

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 Analyzer 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 freigegeben 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 Sie diese freigegebenen Ressourcen verändern, stellen Sie sicher, dass Sie wissen, 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
Special 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:\Documents and Settings\All Users\Gemeinsame 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, Sie die Meldung bekommen, 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 Sie die Meldung bekommen, dass Ihr System nicht anfällig ist, kann das System noch immer von anderen DSL Anwendern ausgenützt 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 zu einem Share (IPC$) über eine verborgene Interprozeßkommunikation zu öffnen. Auf dem System mit der angegebenen IP Adresse wird mit dem Anonymous 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 Hotfixes und Tools zur Verfügung, die Systeme auf diese Schwachstelle überprüfen. 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/Tools/MBSAhome.asp heruntergeladen werden. Dieses Programm prüft, ob die Systeme aktuell sind, welche Hotfixes nicht installiert sind und ob Konfigurationsschwächen vorhanden sind. Es gibt auch ein 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.

W5.5 Wie Sie sich dagegen schützen können

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:

- Freigaben immer ausschalten, wenn nicht benötigt. Wenn der Computer keine Dateien speichert, die freigegeben werden müssen, dann sollten keine Freigaben aktiviert sein. Um die Freigabe von Ressourcen zu deaktivieren, können Sie den Explorer verwenden, den Server Manager für Domänen oder den Gruppenrichtlinien Editor.
- 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 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 Sie die Registrierung ändern, sollten Sie ein Backup der Registry durchführen und Sie sollten auch verstehen, 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 Sie Windows NT Domänen oder Windows 2000/2003 Active Directory im gemischten Modus verwenden, können Sie den Registrierungsschlüssel RestrictAnonymous nicht auf 1 setzen 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 3 (SP3) installiert sein, bevor die Registrierung verändert wird.

> **WICHTIGER Hinweis:** Dieser Artikel enthält Informationen über Änderungen in der Registrierung. Bevor Sie die Registrierung ändern, sollten Sie ein Backup der Registry durchführen und Sie sollten auch verstehen, 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 Sie zu einem späteren Zeitpunkt die Liste der User oder Gruppen ändern wollen, führen Sie die Schritte ab Punkt 10. durch.

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

Für zusätzliche Informationen:

Microsoft Knowledge Base Article Q153183. 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 ^

W6 Microsoft Data Access Components (MDAC)

W6.1 Beschreibung

Microsoft Data Access Components (MDAC) sind eine Reihe von Datenbanktechnologien, die in den gängigen Versionen von Windows enthalten sind. Es gibt eine Anzahl von unterschiedlichen Instanzen, wo ein Angreifer Schwachstellen in MDAC bösartige Befehle oder Code ausführen kann. Es gibt sowohl ältere RDS bezogene Themen, die unten beschrieben werden, als auch neuere Probleme wodurch ein Angreifer, der sich als SQL Server ausgibt, einen Buffer Overflow erzeugen kann und dadurch eine komplette Systemkompromittierung mit sorgsam geschriebene UDP Paketen erwirken kann.

Die Remote Data Service (RDS) Komponenten in älteren Versionen von Microsoft Data Access Components (MDAC) haben einen Programmfehler, wodurch Remote Angreifer Befehle lokal mit administrativen Rechten ausführen können. In Verbindung mit einem Fehler in der Microsoft Jet Database Engine 3.5 (Teil von Microsoft Access) kann ein anonymer externer User Zugriff auf interne Datenbanken erlangen. Diese Fehler sind gut dokumentiert und Lösungen stehen seit mehr als 3 Jahren zur Verfügung. Veraltete oder falsch konfigurierte Systeme sind nach wie vor Ziel dieser.

Aktuellere Schwachstellen die viele Windows Versionen betreffen sind bekannt geworden. Der Buffer Overflow in MDAC wird in dem Microsoft Security Bulletin MS03-033 und CAN-2003-0353 beschrieben. Viele Microsoft Versionen die heutzutage verwendet werden sind davon betroffen. Die MDAC Implementierung in Windows 2003 scheint davon nicht betroffen zu sein.

W6.2 Betroffene Betriebssysteme

Die meisten Windows NT 4.0 Systeme, die IIS 3.0 oder 4.0, Remote Data Services 1.5 oder Visual Studio 6.0 verwenden. Systeme mit Windows 2000 und XP, wie auch Systeme mit Office 2000 SR1 oder höher. SQL Server 7 SP2 und höher und SQL Server 2000 enthalten ebenfalls MDAC Schwachstellen.

Die meisten Windows Versionen können als anfällig eingestuft werden.

W6.3 CVE/CAN Einträge

CVE-1999-1011, CVE-2002-0700

CAN-2002-1142, CAN-2003-0353

W6.4 Wie Sie herausfinden, ob Sie betroffen sind

Wenn Sie Windows NT 4.0 und IIS 3.0 oder 4.0 verwendet, überprüfen Sie ob die Datei msadcs.dll existiert (typischerweise ist diese Datei in C:\Programme\CommonFiles\System\Msadc\msadcs.dll, aber das kann von System zu System unterschiedlich sein). Wenn das der Fall ist, wäre die beste Lösung, das System zu aktualisiert und Patches zu installieren. Es hat sich gezeigt, dass veraltete Softwarepakete mehrere Schwachstellen enthalten.

Wenn Sie eine der vorhin erwähnten Softwarepakete verwenden oder eines der genannten Betriebssysteme, sind die Systeme höchst wahrscheinlich anfällig für die MDAC Schwachstellen. Eine genaue Beschreibung, wie die aktuellen MDAC Schwachstellen erkannt und eliminiert werden können finden Sie unter Microsoft Security Bulletin MS03-033.

Eine einfache Möglichkeit um festzustellen, ob Ihre Systeme die Schwachstellen im MDAC haben, ist der Besuch der Windows Update Seite. Sie überprüfen das System auf nicht aktuelle

Software. Das Windows Update Tool identifiziert veraltete MDAC Versionen und ermöglicht die Aktualisierung.

W6.5 Wie Sie sich dagegen schützen können

Eine hervorragende Beschreibung über die RDS und Jet Schwachstellen und wie diese korrigiert werden können finden Sie unter http://www.wiretrip.net/rfp/txt/rfp9907.txt.

Microsoft has ebenfalls mehrere Security Bulletins veröffentlicht, die detailliert die Angriffsmöglichkeit und die Fehlerbehebung durch Änderung der Konfiguration beschreiben:

- http://support.microsoft.com/support/kb/articles/q184/3/75.asp
- http://www.microsoft.com/technet/security/bulletin/ms98-004.asp
- http://www.microsoft.com/technet/security/bulletin/ms99-025.asp
- http://www.microsoft.com/security/security_bulletins/ms03-033.asp
- http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-033.asp
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823718

Alternativ dazu können die Fehler durch eine Aktualisierung der MDAC Komponenten auf Version 2.8 behoben werden (es kann aber zu Kompatibilitätsproblemen führen). Die aktuellste MDAC Version und zusätzliche Stand Alone Data Access Downloads stehen http://msdn.microsoft.com/library/default.asp?url=/downloads/list/dataaccess.asp zur Verfügung.

Die Verwendung von Windows Update (http://windowsupdate.microsoft.com) um die Probleme zu identifizieren und die Systeme zu aktualisieren oder manuelle Updates der MDAC Implementierungen sind die empfohlene Behebung der Schwachstellen.

zum Anfang ^

W7 Windows Scripting Host (WSH)

W7.1 Beschreibung

Windows Scripting Host (WSH) ist eine Microsoft Technologie, die dazu dient, die Windows Funktionalität zu erweitern und unterstützt JavaScript und Visual Basic Script. WHS wurde erstmals mit Explorer 5 implementiert und ist seit dem eine Standardfunktionalität in den Windows Betriebssystemen seit Windows 98.

Der Windows Scripting Host ermöglicht die Automatisierung von Windows Anwendungen. Durch relativ einfachen Scripting Code wird der Zugriff auf Windows Shell, das Dateisystem, die Registrierung und noch mehr ermöglicht. Scripts können direkt vom Desktop durch anklicken der Scriptdatei oder von Programmen wie dem Mailclient gestartet werden.

In dieser automatische Ausführung des WSH wurde im Frühjahr 2000 eine Schwachstelle ausgenutzt, die zu dem "I Love You" Wurm geführt hat. Dieser Visual Basic Script (VBScript) Wurm verursachte einen Schaden in einer Höhe von mehreren Millionen Dollar. Dieser und auch nachfolgende Würmer verwendeten den Windows Scripting Host, der die automatische Ausführung von Visual Basic Scripts mit den Dateierweiterungen .vbs, .vbe, .js, .jse und .wsf erlaubt und mit Systemrechten oder Applikationsrechten ausgeführt wird.

Obwohl Systemadministratoren bemüht sein sollen, Applikationen und Betriebssysteme auf den möglichst aktuellen Stand zu halten (Einspielen der letzten Patches und Sicherheitsupdates),

sollten gegen die Bedrohungen weitere Schritte unternommen werden, die unter dem Punkt W7.5 "Wie Sie sich dagegen schützen können" nachgelesen werden.

W7.2 Betroffene Betriebssysteme
Windows Scripting Host (WSH) kann manuell installiert werden oder kann mit dem Explorer 5 oder höher auf Systemen mit dem Betriebssystem Windows 95 oder NT installiert werden. Standardmäßig wird WSH mit Windows 98, Windows 98SE, ME, 2000, XP und 2003 installiert.

Sie können die aktuellste Version auf der Microsoft MSDN Seite hier finden:
Download Windows Script (inkludiert Windows Scripting Host)

W7.3 CVE/CAN Einträge
CVE-2001-0149

CAN-2001-1325

W7.4 Wie Sie herausfinden, ob Sie betroffen sind
Computer mit dem Betriebssystem Windows 95 oder NT mit IE 5 oder höher und Windows 98, ME, 2000, XP und 2003 sind anfällig, wenn WSH nicht ausdrücklich ausgeschaltet wird. Es wird empfohlen, dass Anwender ihre Systeme manuell überprüfen, wie es im Punkt W7.5 beschrieben ist und wenn notwendig korrigierend eingreifen.

W7.5 Wie Sie sich dagegen schützen können

> **Wichtiger Hinweis:** Einige Applikationen bzw. administrative Funktionen benötigen den Windows Scripting Host. Wenn Windows Scripting Host ausgeschaltet ist stehen diese Funktionen nicht mehr zur Verfügung.

Windows Scripting Host ausschalten

Security Response von Symantec gibt die folgende Beschreibung von WSH und die Möglichkeit wie dieser ausgeschaltet werden kann.

> Windows Scripting Host ist ein optionaler Teil des Windows Betriebssystems und kann sicher von Computern entfernt oder ausgeschaltet werden. Um sich gegen Bedrohungen und Sicherheitsbedenken in Bezug auf WSH zu schützen, sollte dieses ausgeschaltet werden und nur dann aktiviert werden, wenn dies unbedingt notwendig ist (siehe den Absatz "Änderung des Standardverhaltens von Windows Scripting Host").

Das Programm Nopscript.exe von Symantec schaltet den Windows Scripting Host aus, in dem die Dateiassoziationsklassen für jene Klassen umbenannt werden, die entweder Wscript.exe oder Cscript.exe in der Registrierung unter Shell\Open\Command oder Shell\Open2\Command stehen haben. Dadurch werden alle Scripts unterbunden, egal ob bösartig oder nicht.

Installationsanweisungen von Symantecs Security

1. Noscript.exe herunterladen (auf Festplatte oder Verzeichnis).
2. Doppelklick auf das Noscript.exe Icon. Der Norton Disabler/Enabler erscheint.

- Wenn der WSH am System eingeschaltet ist, werden Sie gefragt, ob Sie diesen ausschalten wollen. Um das zu tun, klicken Sie auf Disable und dann auf OK.
- Wenn der WSH am System ausgeschaltet ist, werden Sie gefragt, ob Sie diesen einschalten wollen. Um das zu tun, klicken Sie auf Enable und dann auf OK.

Änderung des Standardverhaltens von Windows Scripting Host
Um die Funktionalität für administrative Zwecke und Desktop Automation nutzen zu können, aber trotzdem das System gegen Bedrohungen zu schützen, ist es möglich, das Standardverhalten von WSH zu verändern. Dies bezieht sich auf Script Dateien (mit den Dateierweiterungen .vbs, .vbe, .js, .jse und .wsf), die genauso wie ausführbare Windows Dateien behandelt werden (.exe und .com), sie werden sofort ausgeführt.

Durch das Entfernen des Standardverhaltens "Automatic Execution" für WSH Scripts ist es möglich, das unerlaubte Ausführen von Scripts zu verhindern. Die Empfehlung ist, die Konfiguration so zu ändern, dass standardmäßig alle Scripts in einem Texteditor geöffnet werden. Zusätzlich zu dem Schutz vor automatischem Ausführen von Scripts ohne Berechtigung wird dadurch dem Anwender die Möglichkeit gegeben, das Script durchzulesen und jedes einzelne Script individuell zu erlauben oder zu verbieten. Dieser Ansatz kann auch davor schützen, dass Scripts hinter erlaubten Dateierweiterungen versteckt werden, in dem doppelte (oder mehrfache) Dateierweiterung en verwendet werden.

Berechtigte Scripts können noch immer ausgeführt werden, indem der Dateiname explizit als Argument von wscript.exe oder cscript.exe angegeben wird, z.B.:

cscript.exe myscript.vbs
oder
wscript.exe myscript.vbs

Referenz: Symantec Security Response How to Disable or Remove the Windows Scripting Host
http://www.symantec.com/avcenter/venc/data/win.script.hosting.html

Anti-Virus
Es wird empfohlen, das eine aktuelle Antivirenlösung auf Gateways, Servern und Computern installiert ist - zusätzlich zum Ausschalten von WSH - um einen mehrstufigen Schutz zu erhalten. Es wird auch empfohlen, E-Mailanhänge mit den Dateierweiterungen .vbs, .vbe, .js, .jse, .wsf, .bat, .exe, .pif und .scr zu blockieren. Diese Überwachung kann auch dabei hilfreich sein, Dateien mit doppelten (mehrfachen) Dateierweiterungen zu blockieren, die mit hoher Wahrscheinlichkeit bösartig sind. Zum Beispiel bietet Norton Antivirus 2001 und später die Funktionalität Scriptblocking an, wodurch individuelle Systeme gegen WSH Viren geschützt werden.

Script Engine aktualisieren
WSH wurde in den letzten Jahren mehrere Male korrigiert, wodurch höhere Sicherheit und mehr Stabilität erreicht wurden. Die aktuellste Version ist auf Microsofts MSDN Website unter Download Windows Script (beinhaltet auch Windows Scripting Host) zu finden.

NTFS Berechtigungen
NTFS Zugriffsberechtigungen können dazu verwendet werden, die Zugriffsrechte von wscript.exe und cscript.exe zu definieren. Die Rechte für die ausführbaren Programme des Windows Scripting Hosts können für spezifische User oder Gruppen mit gültigen Windowsaccounts zugewiesen werden.

Wenn Verzeichnisse oder Dateien freigegeben werden, sind die standardmäßigen Rechte Vollzugriff für die Windowsgruppe "Jeder", in der alle User enthalten sind. Das heißt, dass alle User die Rechte haben, Dateien oder Verzeichnisse zu ändern, zu verschieben und zu löschen, auch die NTFS Rechte zu verändern. Diese standardmäßigen Einstellungen sind ungeeignet für wscript.exe und cscript.exe. Dateien und Verzeichnisse sicher zu verwalten inkludiert nicht benötigte User und Gruppen zu entfernen oder Gruppen, die keine Notwendigkeit haben, auf diese Ressourcen zuzugreifen, zu entfernen.

Um NTFS Berechtigungen zu ändern sind folgende Schritte notwendig:

Die Anleitungen sind aus der Windows Server Dokumentation - Setting NTFS Permissions for a Directory or File:

1. Öffnen Sie Arbeitsplatz, selektieren Sie den Datenträger, Verzeichnis oder Datei und öffnen Sie die Eigenschaften.
2. Am Sicherheitseinstellungsblatt selektieren Sie den Windowsaccount, den Sie ändern wollen.
3. Unter Berechtigungen selektieren Sie die Art des Zugriffs für den ausgewählten User oder die Gruppe. Verwenden Sie Zulassen um Zugriff zu erlauben und Verweigern um Zugriff nicht zu erlauben. Für mehr Optionen klicken Sie auf Erweitert. Für mehr Information über die Einstellungen und Konfiguration von Berechtigungen lesen Sie in der Windows Dokumentation nach.

   Hinweis: Wenn Sie das Sicherheitseinstellungsblatt beim Datenträger, Verzeichnis oder Datei oder die Eigenschaften nicht sehen, ist das Dateisystem nicht NTFS.

Wie das Dateisystem auf NTFS konvertiert wird, können Sie in der Windowsdokumentation nachlesen. Wichtig ist, dass die Option "Verweigern" Vorrang über der Option "Zulassen" hat. Wenn Sie Verweigern für die Gruppe Jeder anwenden, kann es passieren, dass diese Ressourcen für alle, auch den Administrator nicht mehr verfügbar sind.

Referenz: Setting NTFS Permissions for a Directory or File - http://www.microsoft.com/windows2000/en/server/iis/htm/core/iidfpsc.htm

zum Anfang ^

W8 Microsoft Outlook und Outlook Express

W8.1 Beschreibung

Microsoft Outlook, Teil der Microsoft Office Suite, ist ein persönlicher Informationsmanager und E-Mail Programm von Microsoft. Obwohl Outlook hauptsächlich als E-Mail Applikation verwendet wird, hat es auch Kalenderfunktionen, Aufgaben- und Kontaktmanagementfunktionen inkludiert. Wenn Outlook zusammen mit einem Exchange Server verwendet wird, können zusätzliche 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 Version von Outlook, jedoch mit geringerer Funktionalität. Outlook Express ist mit dem Internet Explorer verbunden, seit der IE Version 1.0 verfügbar und war bereits in Windows 95 integriert. Durch die Integration der Produkte Internet

Explorer und Outlook Express in andere Produkte wie Office, Backoffice und das Windows Betriebssystem können gemeinsame Technologien und Programmcode plattformunabhängig verwendet werden. Zum Beispiel verwendet Microsoft Outlook 98 und Outlook Express die gleiche HTML-Analyse- und Parsingfunktionen des Internet Explorers. Wenn Sie Outlook 98 auf einem Computer installieren, der noch Internet Explorer Version 4 oder geringer installiert hat, wird auch eine neue Version des Internet Explorers mitinstalliert. Dieser Ansatz ist sinnvoll und ermöglicht eine effizientere Verwendung des Programmcodes. Allerdings werden dadurch die Auswirkungen, die durch einen Fehler entstehen können, auch erhöht. Es entsteht ein "Single Point of Failure". Der Aufwand für einen gesicherten Betrieb wird dadurch erhöht.

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 einer Ausnutzung der Schwachstellen; es wurden vermehrt E-Mails mit Viren und Würmern versendet, ebenso mit bösartigem Code, der das lokale System kompromittierte.

W8.2 Betroffene Betriebssysteme

Outlook Express ist eine kostenlose E-Mail-Applikation, die mit allen Versionen des Internet Explorers und Windows gebündelt ist.

Um die verwendete Version von OE zu eruieren, starten Sie den Internet Explorer, dann selektieren Sie das Hilfe Menü, und danach Info. Versionen unter 5.0 sollten sofort aktualisiert werden, die Empfehlungen dazu finden Sie unter W8.5 „“Wie Sie sich dagegen schützen können“.

Outlook ist ein komplette Informationsmanagerapplikation, die als Einzelprodukt oder in Kombination mit der Office Suite erworben werden kann. Outlook wird nur installiert, wenn das auch gezielt durchgeführt wird. Folgende Outlook Versionen sind für Windows verfügbar:

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

Um die verwendete Version von Outlook zu eruieren, starten Sie Outlook, dann selektieren Sie das Hilfe Menü (?), und danach Info über Microsoft Outlook. Versionen unter Outlook 2000 sollten sofort aktualisiert werden.

Referenz:
Outlook Express http://www.microsoft.com/windows/oe/
Outlook http://www.microsoft.com/office/outlook/

W8.3 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

W8.4 Wie Sie herausfinden, ob Sie betroffen sind
Alle Systeme, die Microsoft Windows Betriebssysteme oder den Internet Explorer verwenden, haben auch Outlook Express installiert. Die manuelle Installation der Office Suite kann Outlook enthalten, neben anderen Produkten wie Word, Excel, PowerPoint oder Access.

Für Microsoft Outlook und Outlook Express für Macintosh wurden einigen Sicherheitsprobleme identifiziert.

Es wird empfohlen, die Systeme einzeln zu überprüfen (wie beschrieben in Punkt W8.2 Betroffene Betriebssysteme) und gegebenenfalls Maßnahmen zur Behebung der Sicherheitsprobleme durchzuführen.

Ein System hat Schwachstellen, wenn es entweder

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

W8.5 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 zu sicherer zu machen und die Software immer aktuell zu halten.

1. Besuchen Sie regelmäßig die Windows Update Site http://windowsupdate.microsoft.com, und installieren Sie die kritischen Updates.
2. Schalten Sie die Vorschau aus, in dem Sie auf Ansicht > Layout klicken und die Vorschaufenster anzeigen Option ausschalten.
3. 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.

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 es sich auch um die Originaldateien handelt.

Anti-Virus
Antivirenprogramme schützen vor den meisten Viren, Würmern, Trojanern und anderem bösartigen Programmcode wie Scriptattacken (siehe W10). Es ist absolut notwendig, die Signaturendatenbank immer auf dem letzten Stand zu halten. Mindestens 1 x wöchentlich, am besten täglich 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 bösartige Scripts oder Programme blockiert werden, bevor sie Schaden anrichten können.

Es ist empfohlen, ein aktuelles Virenprogramm zu installieren, bevor Sie E-Mail oder das Internet verwenden, da sich die meisten Viren über E-Mail in Form von Anhängen verbreiten. Bösartige Scripts können auch schon durch die Vorschau ausgeführt werden.

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 von Microsoft 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 XP lesen Sie das Office XP Security white paper.

> **Hinweis:** Wenn Ihr Computer Teil eines betreuten Netzwerkes ist, kontaktieren Sie Ihre Systembetreuer oder Systemadministratoren, bevor Sie Änderungen durchführen. Administratoren finden detaillierte technische Informationen über

Outlook E-Mail Sicherheitsupdates im Office Resource Kit.

Deinstallation von Outlook und Outlook Express
Wenn Sie ein anderes E-Mailprogramm verwenden, 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 Betriebssystemupgrade installieren.

zum Anfang ^

W9 Windows Peer to Peer File Sharing (P2P)

W9.1 Beschreibung

Diese Schwachstellen unterscheiden sich von den anderen, wenn man bedenkt, dass Peer to Peer Programme Anwendermodusapplikationen sind. 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). Oft sind die Daten entweder urheberrechtlich geschützt oder von fragwürdigen Quellen. Nachdem Napster rechtliche Erfahrungen sammeln musste, werden die meisten Programme jetzt über ein Netzwerk von Clients betrieben, die Verzeichnisse freigeben, Dateien oder manchmal ganze Festplatten. Die Anwender verwenden Suchfunktionen, die in der Client Software enthalten sind. 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 angeforderter binärer Inhalt geändert oder entstellt wird. Die rechtlichen Probleme können aus urheberrechtlichen Gründen oder aus rechtlich fragwürdigen Inhalten entstehen.

Wie oben erwähnt, können 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 bösartiger User oder ein bereits infiziertes System Daten erstellt oder so verändert, dass andere User diese als begehrenswert finden. Viren, Trojaner, Würmer und andere bösartigen 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.

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.

W9.2 Betroffene Betriebssysteme
Alle Versionen von P2P Programmen die auf Windows Plattformen funktionieren, sowie Versionen unter Linux und UNIX.

W9.3 CVE/CAN Einträge
CVE-2001-0368

CAN-2000-0412, CAN-2002-0314, CAN-2002-0315, CAN-2003-0397

W9.4 Wie Sie herausfinden, ob Sie betroffen sind
Herauszufinden, ob P2P Aktivitäten in Ihrem Netzwerk stattfinden, kann eine Herausforderung darstellen. Sie können versuchen P2P Software zu erkennen, 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, ebenfalls können die Links zu Snort Regeln hilfreich sein. Das Programm PacketPup von der Firma Pallisades Software kann zum Monitoring von P2P Verkehr verwendet werden. Speichermedien können auch nach Dateien durchsucht werden, die oft heruntergeladen werden. Dazu zählen die Dateien *.mp3, *.wma, *.avi, *.mpeg, *.jpg, *.gif, *.zip und *.exe. Durch regelmäßige Überprüfung des Plattenspeichers kann auch plötzlich ansteigenden Speicherverbrauch auf eine Verwendung von P2P Programmen hinweisen.

W9.5 Wie Sie sich dagegen schützen können
Firmenrichtlinien::

1. Ihr Unternehmen sollte eine Richtlinie haben, die das Herunterladen von urheberrechtlich geschützten Daten verbietet.
2. Ihr Unternehmen sollte eine Richtlinie für den angemessenen Gebrauch der Internetverbindung haben.
3. Netzwerkplatten und PCs sollten regelmäßig auf nicht erlaubte Daten überprüft werden.

Netzwerkrestriktionen:

1. Normale Anwender sollten nicht in der Lage sein, Software - im speziellen P2P - zu installieren.
2. Ein Proxyserver sollte für die Kontrolle des Internetzuganges überlegt werden.
3. Die Accesslisten für ausgehende Services sollten nur geschäftsrelevante Ports erlauben. Da immer mehr P2P Programme HTTP verwenden, ist diese Regelung jedoch kaum effektiv.
4. Das Netzwerk sollte auf P2P Aktivitäten überprüft werden und etwaige Verstöße sollten an die zuständigen Stellen weitergeleitet werden.
5. Unternehmensweite Antivirensoftware soll installiert und täglich aktualisiert werden.

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

Napster	eDonkey	Gnutella	Kazaa
tcp 6699	udp 4665	tcp/udp 6347	

tcp 6699	udp 4665	tcp/udp 6347
		tcp/udp 6348
		tcp/udp 6349

Snort Signaturdatenbankeinträge finden Sie unter http://www.snort.org/cgi-bin/sigs-search.cgi?sid=p2p

549 # 556 # 1432
550 # 557 # 1669
551 # 558 # 2180
552 # 559 # 2181

zum Anfang ^

W10 Simple Network Management Protocol (SNMP)

W10.1 Beschreibung

Das Simple Network Management Protokoll wird für das Monitoring und die Konfiguration von allen Arten von modernen TCP/IP-Geräten häufig verwendet. Obwohl SNMP auf den meisten Netzwerkplattformen weit verbreitet ist, wird es sehr oft für die Konfiguration und das Management von Geräten wie Drucker, Router, Switches, Wireless Access Points und Bridges wie auch als Input für Monitoring verwendet.

Simple Network Management Kommunikation besteht aus verschiedenen Typen von Meldungen, die zwischen SNMP Managementstationen und Netzwerkgeräten ausgetauscht werden (üblicherweise als Agentsoftware bekannt). Die Methode, wie diese Meldungen bearbeitet werden sowie die Authentifizierungsmechanismen hinter diesen Meldungen haben gravierende Schwachstellen.

Die Methode, mit der SNMP Version 1 Meldungen bzw. Traps bearbeitet hat Schwachstellen, die im CERT Advisory CA-2002-03 genau beschrieben sind. Die Sicherheitsschwachstellen beziehen sich auf die Art und Weise wie Requests und Traps auf Management Stationen und Agents verarbeitet werden. Diese Fehler sind nicht auf einzelne SNMP Implementierungen beschränkt sondern betreffen eine Vielzahl von Produkten von verschiedenen Herstellern. Die Ausnutzung dieser Schwachstellen kann von Denial of Service Attacken bis zu unerwünschten Konfigurationsänderungen und Management der SNMP-Geräte reichen.

Die Authentifizierungsmechanismen in älteren SNMP Systemen enthalten ebenfalls signifikante Schwachstellen. SNMP Versionen 1 und 2 verwenden den unverschlüsselten "Community String" als Authentifizierungsmechanismus. Nicht nur das die Authentifizierung unverschlüsselt erfolgt stellt ein Sicherheitsproblem dar. Der "Community String" ist bei den meisten Geräten standardmäßig auf "public" eingestellt, einige besonders kluge Hersteller haben für sensitive Informationen den String auf "private" geändert. Angreifer können diese Schwachstellen dazu verwenden, SNMP-Geräte umzukonfigurieren oder diese Geräte ganz abzuschalten. Ausspionierter SNMP Verkehr kann eine Menge an Informationen über die Netzwerkstruktur und die am Netzwerk angeschlossenen Geräte enthalten. Angreifer verwenden diese Art von Information um sich ein Angriffsziel auszusuchen und Angriffe zu planen.

Die meisten Hersteller verwenden SNMP Version 1 als Standard, und viele bieten nicht einmal die Möglichkeit SNMP Version3 zu verwenden. Das Sicherheitsmodell in SNMP Version 3 kann so

konfiguriert werden, dass die Authentifizierung sicher wird. Es gibt jedoch frei verfügbaren Ersatz der SNMP v3 unterstützt und der unter GPL oder BSD Lizenz verwendet werden kann.

SNMP ist üblicherweise in Windows nicht standardmäßig aktiviert, es wird aber oft von gutmeinenden Administratoren als Service aktiviert. Andere Netzwerkmanagement Produkte verwenden manchmal das Windows Service oder installieren ihr eigenes. SNMP wird auch oft als Kommunikationsmethode verwendet, um Drucker, USV Systeme und Wireless Access Points und Bridges zu managen. SNMP wird in verschiedenen UNIX und Linux Distributionen, Netware Versionen, Netzwerkequipment, Drucker und eingebauten Systemen gefunden. Die meisten SNMP Angriffe scheinen jedoch auf UNIX Systemen mit schlecht konfigurierten SNMP durchgeführt werden.

W10.2 Betroffene Betriebssysteme
Fast alle Windows Betriebssysteme werden mit SNMP als mögliche Installationsoption geliefert, SNMP wird jedoch standardmäßig nicht installiert oder eingeschaltet. Die meisten anderen SNMP-Geräte und Betriebssysteme sind auch anfällig.

W10.3 CVE/CAN Einträge
CVE-1999-0294, CVE-1999-0815

CAN-1999-0499, CAN-2002-0053

W10.4 Wie Sie herausfinden, ob Sie betroffen sind
Sie können überprüfen, ob SNMP auf dem im Netzwerk angeschlossenen Geräten aktiviert ist, in dem Sie dies mit einem Scanner oder manuell überprüfen.
SNMPing - Sie können das SNMP Scanning Tool SNMPing vom SANS Institute beziehen, in dem Sie eine leere E-Mail an snmptool@sans.org schicken. Sie bekommen in der Antwort eine URL, von der Sie das Programm herunterladen können.
SNScan - Foundstone hat ebenfalls ein einfaches SNMP Scanning Tool. SNScan welches unter http://www.foundstone.com/knowledge/free_tools.html gefunden werden kann.

Wenn Sie keines der oben angeführten Tools verwenden können, sollten Sie manuell überprüfen, ob SNMP auf Ihren Geräten aktiviert ist. Lesen Sie in Ihrem Betriebssystemhandbuch nach, wie eine SNMP Implementierung erkannt werden kann. Das Basisservice kann üblicherweise erkannt werden, in dem überprüft wird, welche Services gestartet sind, welche Prozesse aktiviert sind, durch das Ausführen des Befehls "net start" in der Kommandozeile oder indem Sie mittels des Befehls "netstat -an" überprüfen, ob Services auf Port 161 oder 162 aktiviert sind.

Eine aktivierte SNMP Instanz ist wahrscheinlich genug Evidenz, dass die Systeme anfällig für die Sicherheitsschwachstellen "pervasive trap" und "request handling" sind. Bitte lesen Sie das CERT Advisory CA-2002-03 für mehr Information.

Wenn SNMP aktiviert ist und eine der unten genannten Schwachstellen zutreffen, haben Sie wahrscheinlich eine standarmlässige, oder einfach zu erratende String Schwachstelle:

1. Leerer oder standardmäßiger SNMP Community String.
2. Erratbarer SNMP Community String.
3. Versteckter Community String.

Bitte lesen Sie http://www.sans.org/resources/idfaq/snmp.php für nähere Information über die

Erkennung von diesen Konditionen.

W10.5 Wie Sie sich dagegen schützen können

Trap und Request Handling Schwachstellen:

1. Wenn SNMP nicht absolut notwendig ist, deaktivieren Sie es.
2. Wenn möglich, verwenden Sie das SNMPv3 User basierendes Sicherheitsmodell mit Messageauthentifizierung und möglicherweise Verschlüsselung der Protokolldateneinheit.
3. Wenn Sie SNMP Version 1 oder 2 verwenden müssen, dann sollten die letztgültigen Sicherheitspatches vom Hersteller installiert sein. Ein guter Startpunkt für herstellerspezifische Informationen ist Appendix A - CERT Advisory CA-2002-03.
4. Filtern Sie SNMP (Port 161 TCP/UDP und 162 TCP/UDP) an den Eingangspunkten zu Ihren Netzwerk, außer es ist unbedingt notwendig Zugang von außen zum managen der Geräte zu haben. Dann sollte, wenn möglich, SNMP nur zwischen vertrauenswürdigen Subnetzen erlaubt bzw. gefiltert werden.
5. Verwenden Sie hostbasierende Zugriffskontrolle für die SNMP Agent Systeme. Obwohl die Kapazität des SNMP Agent Systems dadurch eingeschränkt werden kann, erhöht sich die Kontrollmöglichkeit, welche Systeme Anfragen stellen können. In den meisten Windows 2000 Systemen (und späteren) kann das durch IPSec Filter bewerkstelligt werden. Ein hostbasierende Firewall am Agent kann auch dazu verwendet werden, unerwünschte SNMP Anfragen zu blocken.

Standardmäßige und einfach zu erratende String Schwachstelle:

1. Wenn SNMP nicht absolut notwendig ist, deaktivieren Sie es.
2. Wenn möglich, verwenden Sie das SNMPv3 Userbasierende Sicherheitsmodell mit Messageauthentifizierung und möglicherweise Verschlüsselung der Protokolldateneinheit.
3. Wenn Sie SNMP Version 1 oder 2 verwenden müssen, wenden Sie die gleichen Richtlinien an wie für die Userkennwörter. Stellen Sie sicher, dass diese schwer zu erraten und zu knacken sind und dass sie regelmäßig geändert werden.
4. Validieren und überprüfen Sie die Community Namen mit snmpwalk. Zusätzliche Information kann unter http://www.zend.com/manual/function.snmpwalk.php gefunden werden. Eine gute Einführung für dieses Tool können Sie unter http://www.sans.org/resources/idfaq/snmp.php finden.
5. Filtern Sie SNMP (Port 161 TCP/UDP und 162 TCP/UDP) an den Eingangspunkten zu Ihren Netzwerk, außer es ist unbedingt notwendig Zugang von außen zum managen der Geräte zu haben. Dann sollte, wenn möglich, SNMP nur zwischen vertrauenswürdigen Subnetzen erlaubt bzw. gefiltert werden.
6. Wenn möglich erlauben Sie auf allen MIBs nur Lesezugriff. Zusätzliche Information kann unter http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315 gefunden werden.

zum Anfang ^

Top Schwachstellen von UNIX Systemen (U)

U1 BIND Domain Name System

U1.1 Beschreibung

Berkeley Internet Name Domain (BIND) ist die am meisten verwendete Implementierung der

Domain Name Services (DNS), einem wichtigen System, das die Auflösung von Hostnamen (z.B. www.sans.org) in registrierte IP Adressen ermöglicht. Dass BIND nahezu überall verfügbar und ein grundlegender Dienst ist, hat diesen Dienst zu einem häufigen Ziel, besonders von Denial of Service (DoS)-Angriffen gemacht, was zum Verlust der kompletten Verfügbarkeit des Internets für Rechner und Dienste führen kann. Während die Entwickler von BIND in der Vergangenheit schnell beim Beseitigen von Schwachstellen waren, sind noch immer eine große Zahl von veralteten, schlecht konfigurierten oder verwundbaren Servern vorhanden.

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 kann 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 verwendet der Angreifer verwundbare Implementierungen der DNS Resolver Bibliotheken. Durch Senden von bösartigen DNS-Antworten kann 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

Beinahe alle UNIX- und Linux-Systeme sind mit einer Version von BIND ausgestattet. Typischerweise ist das nur bei Rechnern der Fall, die als Server konfiguriert sind. Binäre Versionen von BIND existieren auch für Windows.

U1.3 CVE/CAN Einträge

CVE-1999-0009, CVE-1999-0024, CVE-1999-0184, CVE-1999-0833, CVE-1999-0837, CVE-1999-0835, CVE-1999-0849, 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

U1.4 Wie Sie herausfinden, ob Sie betroffen sind

Wenn Sie eine Version von BIND verwenden, die mit Ihrem Betriebssystem ausgeliefert wurde, dann vergewissern Sie sich, dass Sie mit allen vom Hersteller veröffentlichten Patches auf dem aktuellen Stand sind. Verwenden Sie BIND, erzeugt aus den Quelltexten vom Internet Software Consortium (ISC), dann überprüfen Sie ob das die neueste Version ist. Nicht gepatchte oder veraltete Versionen von BIND haben sehr wahrscheinlich Schwachstellen.

Auf den meisten Systemen zeigt der Befehl „named –v“ die installierte Version von BIND als X.Y.Z, wobei X die Hauptversion, Y die Unterversion und Z der Patchlevel ist. Derzeit sind drei Hauptversionen von BIND verfügbar: 4, 8 und 9. Wenn Sie BIND selbst kompiliert haben, sollten Sie die Version 4 durch die Version 9 ersetzen. Sie können die neuesten Quelltexte, Version 9.2.2, 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, Symantec oder Afentis. Weiters kann ein aktualisierter Scanner von Schwachstellen sehr hilfreich sein um periodisch DNS Systeme nach potentiellen Schwachstellen zu untersuchen.

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. Um zu verhindern, dass diese Änderung rückgängig gemacht wird, ist es empfehlenswert, BIND zu deinstallieren.
  2. Spielen Sie alle Patches des Herstellers ein oder steigen Sie auf die neueste Version um. Für detaillierte Informationen über das Härten Ihrer 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 Ihres 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 Ihrer Domäne. Deaktivieren Sie Zone Transfers zu über- oder untergeordneten Domänen, indem Sie stattdessen delegieren oder weiterleiten.
  5. „Die Gummizelle“: Um zu verhindern, dass ein kompromittierter „named“ Ihr gesamtes System öffnet, schränken Sie BIND so ein, dass er als nicht-privilegierter User in einem gechroot()etem 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

Exzellente Anleitungen zum Härten von BIND auf Solaris Systemen sowie weitere Referenzen auf BIND Dokumentation finden Sie in Running the BIND9 DNS Server Securely und in den Archive von Arbeiten über die Sicherheit von BIND bei Afentis.

zum Anfang ^

U2 Remote Procedure Calls (RPC)

U2.1 Beschreibung

Remote Procedure Calls (RPCs) ermöglichen Programmen auf einem Computer durch Senden von Daten und Empfang der Ergebnisse, Prozeduren auf einem zweiten Computer auszuführen. RPC wird daher oft für verteilte Netzwerkdienste wie Fernwartung, NFS Dateien-Sharing und NIS verwendet. Allerdings sind zahlreiche Defekte in RPC, die aktiv ausgenutzt werden. Einige RPC Services arbeiten mit erweiterten Rechten, durch die ein Angreifen unerlaubten Zugriff als Root auf verwundbare Systeme erhalten kann.

Es gibt zwingende Beweise, dass der Großteil der Distributed Denial of Service-Angriffe, die zwischen 1999 und im frühen Jahr 2000 stattfanden, von Systemen ausgeführt wurden, die durch solche RPC Schwachstellen geknackt wurden. Der großteils erfolgreiche Angriff auf Systeme des U.S. Militärs während des Solar Sunrise incident hat auch einen RPC Fehler ausgenützt, der auf hunderten Computern des Departement of Defense zu finden war. Vor kurzer Zeit hatte eine Schwachstelle im MS Windows DCOM Remote Procedure Call einen wesentlichen Anteil an der rasanten Verbreitung eines Wurms.

U2.2 Betroffene Betriebssysteme
Beinahe alle Versionen von UNIX und Linux haben RPC-Dienste installiert und aktiviert.

U2.3 CVE/CAN Einträge
CVE-1999-0002 , CVE-1999-0003 , CVE-1999-0008 , CVE-1999-0018 , CVE-1999-0019 , CVE-1999-0168 , CVE-1999-0170 , CVE-1999-0208 , CVE-1999-0211 , CVE-1999-0493 , CVE-1999-0693 , CVE-1999-0696 , CVE-1999-0977 , CVE-1999-0320 , CVE-2000-0666 , CVE-2001-0717 , CVE-2001-0779 , CVE-2001-0803 , CVE-2002-0033 , CVE-2002-0391 , CVE-2002-0573 , CVE-2002-0679

CAN-2002-0677 , CAN-2003-0028 , CAN-2003-0252

U2.4 Wie Sie herausfinden, ob Sie betroffen sind
Verwenden Sie eine Schwachstellenscanner oder den ‚rpcinfo' Befehl um herausfinden, ob einer der am öftesten ausgenutzten RPC Dienste läuft:

RPC Dienst	RPC Programmnummer
rpc.ttdbserverd	100083
rpc.cmsd	100068
rpc.statd	100024
rpc.mountd	100005
rpc.walld	100008
rpc.yppasswdd	100009
rpc.nisd	100300
sadmind	100232
cachefsd	100235
snmpXdmid	100249

RPC Dienste werden typischerweise durch Buffer Overflow Angriffe ausgenützt, die erfolgreich sind, da RPC Programme keine ausreichend Überprüfung auf Fehler oder der Eingabe vornehmen. Buffer Overflow Schwachstellen erlauben einem Angreifer unerwartete Daten (oft in der Form von bösartigem Code) in den Speicherbereich des Programmcodes zu senden. Durch schwache Überprüfung auf Fehler beziehungsweise Validierung der Eingabewerte können Daten Schlüsselbereiche des Speichers, die als nächstes vom Prozessor ausgeführt werden, überschreiben. Bei einem erfolgreichen Overflow Angriff wird der bösartige Code dann vom Betriebssystem ausgeführt. Da viele RPC Dienste mit erweiterten Rechten ausgeführt werden, kann erfolgreiches Ausnützen dieser Schwachstellen unautorisierten Root-Zugriff auf das System

ermöglichen.

U2.5 Wie Sie sich dagegen schützen können
Führen Sie die folgenden Schritte durch um Ihr System vor RPC Angriffen zu schützen:

1. Deaktivieren oder entfernen Sie alle RPC Dienste die nicht absolut notwendig für den Betrieb Ihres Netzwerks sind.
2. Installieren Sie die neuesten Patches für alle Dienste, die Sie nicht entfernen können:

   Für Solaris Software Patches:
   http://sunsolve.sun.com

   Für IBM AIX Software Patches:
   http://www.ibm.com/support/us
   http://techsupport.services.ibm.com/server/fixes

   Für SGI Software Patches:
   http://support.sgi.com

   Für Compaq (Digital UNIX) Software Patches:
   http://www.compaq.com/support

   Für Linux Software Patches:
   http://www.redhat.com/apps/support/errata
   http://www.debian.org./security

   Für HP-UX Software Enhancements und Patch Bundles:
   http://www.software.hp.com/portal/swdepot/displayProductsList.do?category=ER

3. Durchsuchen Sie regelmäßig die Patch-Datenbank des Herstellers nach neuen Patches und installieren Sie diese sofort.
4. Blockieren Sie den RPC portmapper, Port 111 (TCP und UDP), und Windows RPC, Port 135 (TCP und UDP) auf den Border Routern oder Firewalls.
5. Blockieren Sie die RPC “lookback” Ports, 32770-32789 (TCP und UDP).
6. Aktivieren Sie einen nicht-ausführbaren Stack auf den Betriebssystemen, die diese Funktion zur Verfügung stellen. Ein nicht-ausführbarer Stack schützt nicht gegen alle Buffer Overflows, aber es verhindert die Verwendung von einigen im Internet frei verfügbaren Standard Buffer Overflow Exploits.
7. Für über NFS exportierte Systeme sollten die folgenden Schritte unternommen werden:
   1. Verwenden Sie Host/IP basierte Export Listen.
   2. Konfigurieren Sie nur lesbare oder no-suid exportierte Dateisysteme wo immer möglich.
   3. Verwenden Sie 'nfsbug' um nach Schwachstellen zu suchen.

   Eine Übersicht, die genauere Informationen zu den drei Hauptschwachstellen von RPC - Tooltalk, Calendar Manager und Statd – bietet, kann unter folgender Adresse gefunden werden: http://www.cert.org/incident_notes/IN-99-04.html.

   Übersichtsdokumente, die genauere Informationen zu den oben genannten RPC

Schwachstellen bieten, können an folgenden Adressen gefunden werden:

- Statd: http://www.cert.org/advisories/CA-2000-17.html

  http://www.cert.org/advisories/CA-1999-05.html
  http://www.cert.org/advisories/CA-1997-26.html

- Tooltalk: http://www.cert.org/advisories/CA-2002-26.html

  http://www.cert.org/advisories/CA-2002-20.html
  http://www.cert.org/advisories/CA-2001-27.html

- Calendar Manager: http://www.cert.org/advisories/CA-2002-25.html

  http://www.cert.org/advisories/CA-1999-08.html

- Cachefsd: http://www.cert.org/advisories/CA-2002-11.html
- Sadmind: http://www.cert.org/advisories/CA-1999-16.html

  http://www.cert.org/advisories/CA-2001-11.html

- Mountd: http://www.cert.org/advisories/CA-1998-12.html
- SnmpXdmid: http://www.cert.org/advisories/CA-2001-05.html
- Rwalld: http://www.cert.org/advisories/CA-2002-10.html
- XDR: http://www.cert.org/advisories/CA-2003-10.html
- Microsoft RPC: http://www.cert.org/advisories/CA-2003-16.html

  http://www.cert.org/advisories/CA-2003-19.html

zum Anfang ^

U3 Apache Web Server

U3.1 Beschreibung

Apache war in der Vergangenheit und ist auch heute noch der am weitesten verbreitete Web-Server im Internet. Im Vergleich mit dem Microsoft Internet Information Server hat Apache wahrscheinliche weniger Sicherheitsprobleme, jedoch hat er noch immer genügend Schwachstellen.

Neben den Exploits für den Kern und die Module des Apache (CA-2002-27, CA-2002-17), sind auch die Verwendung von Schwachstellen von SQL, Datenbanken, CGI und PHP durch den Web-Server möglich.

Behebt man die Schwachstellen im Apache und den damit verbundenen Komponenten nicht, so kann das zu Denial of Service, unerwünschter Enthüllung von Informationen, Verunstaltung von

Web-Sites, unerlaubtem Root-Zugang oder zahlreichen anderen ungewollten Ergebnisse führen.

U3.2 Betroffene Betriebssysteme
Apache kann auf allen UNIX Systemen laufen. Viele Linux und UNIX Varianten werden mit installiertem und manchmal auch aktiviertem Apache ausgeliefert. Weiters kann Apache auch auf einem Computer mit anderen Betriebssystemen inklusive Windows laufen und hat wahrscheinlich auch in diesen Implementierungen viele Schwachstellen.

U3.3 CVE/CAN Einträge
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-2000-0010, CVE-2000-0208, CVE-2000-0287, CVE-2000-0941, CVE-2002-0082, CVE-2002-0392

CAN-1999-0509, CAN-2000-0832, CAN-2002-0061, 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

U3.4 Wie Sie herausfinden, ob Sie betroffen sind
Informationen bezüglich Sicherheitshinweisen für Apache 1.3.x kann man unter http://www.apacheweek.com/features/security-13 finden, Informationen über die Sicherheit von Apache 2.0 sind unter http://www.apacheweek.com/features/security-20. Diese Links enthalten detaillierte Beschreibungen durch die man herausfinden kann, ob man angreifbar ist, welche Versionen von der jeweiligen Schwachstelle betroffen sind, und welche Workarounds – so verfügbar – empfohlen werden. Weiters führen Links von http://httpd.apache.org zu den oben genannten Seiten.

U3.5 Wie Sie sich dagegen schützen können

1. Stellen Sie sicher, dass sie die aktuellste Version verwenden.
   - http://httpd.apache.org hat die aktuellsten Versionen und Patch Level verfügbar.
   - Der Quellcode für die aktuellste(n) Version(en) von Apache kann man von http://httpd.apache.org/download.cgi herunterladen.
   - Die neuesten Patches sind auf http://www.apache.org/dist/httpd/patches/
2. Stellen Sie sicher, dass zentrale Betriebssystemkomponenten, die von Apache verwendet werden gepatcht sind. Nur die Module, die für die Funktion Ihres Webservers unbedingt notwendig sind sollten in Apache kompiliert werden.

   Anmerkung: Der mod_ssl Wurm (CA-2002-27) ist ein sehr gutes Beispiel, das durch Schwachstellen innerhalb von OpenSSL (CA-2002-23) verursacht wurde.

3. Lassen Sie Apache nicht als root laufen. Ein eigener Benutzer mit eigener Gruppe und minimalen Rechten sollte für den Apache erzeugt werden. Kein anderer Prozess des Systems sollte als dieser User oder diese Gruppe laufen
4. Reduzieren Sie die über den Server verfügbare Information.

   Obwohl dieser Vorschlag Widerspruch von Leute hervorruft, die der Meinung sind, dass „Security by Obscurity“ nichts bringt, und obwohl einige Exploit-Versuche, die Sie sehen werden, blindlings durchgeführt werden (erkennbar an vielen Apache Logs, die zahlreiche Einträge von Versuchen von Exploits für IIS enthalten), gibt es dennoch einige Exploits, die abhängig von den Versionsinformationen im Header ausgeführt werden.

- Verändern Sie den Apache HTTP response token.
    1. Für Apache 1.3.x lesen Sie unter http://httpd.apache.org/docs/mod/core.html#servertokens http://httpd.apache.org/docs/mod/core.html#serversignature.
    2. Für Apache 2.0.x lesen Sie unter http://httpd.apache.org/docs-2.0/en/mod/core.html#servertokens.
- Stellen Sie sicher, dass man vom Internet aus nicht auf mod_info zugreifen kann.
- Directory indexing sollte deaktiviert sein.

5. Sie sollten sich überlegen, ob Apache nicht in einer chroot-Umgebung laufen sollte. Wenn Apache mit chroot gestartet wurde, kann der Prozess auf keinen Teil des Verzeichnisbaums außerhalb des chroot-Verzeichnisses zugreifen, was sehr oft helfen kann, Exploits zu verhindern. Zum Beispiel könnte ein Exploit versuchen eine Shell zu starten, und da /bin/sh sehr wahrscheinlich nicht im chroot-Verzeichnisbaum zu finden ist (was auf jeden Fall so sein sollte!), wäre dieser Exploit harmlos.

   ACHTUNG: Apache in eine chroot-Umgebung zu installieren kann nachteilige Auswirkungen auf CGI, PHP, Datenbanken und andere Module oder Verbindungen haben, die möglicherweise erfordern, dass die Umgebung des Web-Servers Zugriff auf externe Bibliotheken oder Programme hat.
   Da es zahlreiche Methoden der Installation in chroot-Umgebungen gibt, sollte man die Dokumentation der Programme zur Hilfe heranziehen. Für weitere Informationen lesen Sie bitte dazu unter den folgenden Links nach.

   - http://www.w3.org/Security/Faq/wwwsf3.html#SVR-Q5
   - http://www.modsecurity.org/documentation/apache-internal-chroot.html

6. Effizientes und gründliches Logging ist wesentlich um etwaige Sicherheitsprobleme beziehungsweise unerklärbares Verhalten Ihres Web-Servers rasch zu finden. Es wird empfohlen, regelmäßig die Logs zu rotieren und alte Logs zu archivieren. Das führt zu kleineren Logs und macht es leichter, sie zu durchsuchen, falls es notwendig sein sollte.

   Verschiedene Informationen bezüglich Formaten und der Rotation von Logfiles gibt es unter folgenden Links:

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

   In einigen Szenarien wird der Inhalt der Logfiles nicht ausreichen. Besonders wenn Sie PHP, CGI oder andere Scripting-Methoden verwenden, ist es eine gute Idee, GET und POST-Daten mitzuschreiben. Das kann wichtige Daten und Beweise im Fall eines Sicherheitsproblems liefern. Die Aufzeichnung von GET und POST Daten kann mit mod_security implementiert werden.

   - http://www.modsecurity.org
   - http://www.securityfocus.com/infocus/17064.152.44.126 152.44.126

7. PHP, CGI, SSI und andere Scripting-Methoden.
    - Sofern nicht unbedingt notwendig, deaktivieren Sie PHP, CGI, SSI und andere Skriptsprachen.
    - Deaktivieren Sie Server Side Includes (SSI) die möglicherweise missbraucht werden können und den Web-Server Code ausführen lassen können, für den er

nicht bestimmt war.

- Wenn PHP, CGI, SSI oder andere Skriptsprachen notwendig sind, überlegen Sie sich die Verwendung von suEXEC. suEXEC ermöglicht es, Scripts mit Apache zu verwenden, die unter einer andern Userid laufen als der Apache.

  ACHTUNG: Es ist wichtig, dass suEXEC genau verstanden wird. Wird es falsch verwendet, so können neue Sicherheitsprobleme entstehen.

  1. Für Apache 1.3.x: http://httpd.apache.org/docs/suexec.html
  2. Für Apache 2.0.x: http://httpd.apache.org/docs-2.0/suexec.html
- Überprüfen Sie den Inhalt von cgi-bin und anderen Skript-Verzeichnissen. Alle Beispiele und Standard-Skripts sollten entfernt werden.
- Absichern von PHP:

  Das ist ein sehr großes Gebiet, daher folgen gute Ansatzpunkte um sicherzustellen, dass Ihre Implementierung von PHP sicher ist.

  1. Deaktivieren Sie alle Parameter, die dazuführen, dass PHP Informationen im http Header preisgegeben werden.
  2. Stellen Sie sicher, dass PHP im Safe Mode läuft.

  Detaillierte Informationen gibt es unter:
  http://www.securityfocus.com/printable/infocus/1706

- Weitere Module können die Sicherheit erhöhen. Das mod_security (www.modsecurity.org) Modul kann Ihnen helfen, sich gegen Cross Side Scripting (XSS) und SQL Injection zu schützen. Eine detaillierte Anleitung kann auf der oben genannten Web-Site gefunden werden.
- Überprüfen Ihrer Scripts nach Schwachstellen inklusive XSS und SQL Injection ist auch wichtig. Es gibt einige Open Source Tools die das erledigen. Nikto (verfügbar unter http://www.cirt.net/code/nikto.shtml) ist eines der umfangreicheren CGI scanning Tools

zum Anfang ^

U4 Allgemeine UNIX Benutzerkonten mit schwachen oder ohne Passwörtern

U4.1 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 Passwörter; explizite Regeln für Benutzer um sicherzustellen, dass ihre Passwörter sicher bleiben; Definition eines Prozess für die IT-Mitarbeiter um schwache/unsichere/Standard- oder allgemein bekannte Passwörter rasch zu ersetzen und um sofort 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.

U4.2 Betroffene Betriebssysteme
Jedes Betriebssystem beziehungsweise jede Anwendung auf einer beliebigen Plattform wo sich ein Anwender durch Userid und Passwort anmelden.

U4.3 CVE/CAN Einträge
CVE-1999-0502

U4.4 Wie Sie herausfinden, ob Sie betroffen sind
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 Ihren Systemen hat.

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 Ihr 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, die Hashwerte zu speichern. Werden Ihre lokalen Accounts nicht durch /etc/shadow geschützt, dann ist das Risiko für Ihre Passwörter sehr hoch. Die meisten neuen Betriebssysteme verwenden standardgemäß /etc/shadow um Passworthashes zu speichern, sofern das nicht bei der Installation geändert wurde. Es kann sogar sein, dass Sie den MD5-Algorithmus zum hashen Ihrer Passwörter verwenden können, was sicherer ist als der ältere crypt-Algorithmus.

NIS ist eine Sammlung von Diensten, die als Datenbank dienen um Ortsinformationen, genannt Maps, für andere Netzwerksdienste, 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.

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.

U4.5 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 benützen Wörterbuch-Attacken. Da die üblichen Passwortverschlüsselungsverfahren weitreichend 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 zusammengefügten 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 der 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, umschauen. 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 Ablaufen der Gültigkeit von Passwörtern sollte eingehalten werden damit Passwörter, die den Regelungen entgehen nur für kurze Zeit angreifbar sind und alte Passwörter nicht wiederverwendet werden können. Administratoren sollen sicherstellen, dass die Anwender vor dem bevorstehenden Ablaufen 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.** 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. 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. 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.

zum Anfang ^

U5 Klartextdienste

U5.1 Beschreibung
Viele der von UNIX Systemen verwendeten Netzwerkdienste arbeiten mit Klartext (auch „plain text“ genannt). Das heißt, dass diese Dienste keine Verschlüsselung verwenden. Das Fehlen der Verschlüsselung ermöglicht es jedem, der den Netzwerkverkehr beobachten („snifft“), Zugriff auf entweder die Inhalte der Kommunikation oder die Anmeldedaten zu erhalten.

Zum Beispiel um FTP oder Telnet Anmeldedaten zu stehlen, muss ein Angreifer irgendwo entlang der Verbindung einen Netzwerksniffer installieren, zum Beispiel auf dem LAN-Segments des FTP Servers oder des Clients. Die Übertragung der Information zwischen r-Befehl-Clients und R-Diensten im Klartext erlaubt das Abhören von Daten oder Tastendrücken. Angreifer haben oft Sniffer bei Sicherheitsvorfällen und oft auf kompromittierten Systemen installiert. Benutzernamen und Passwörter in gesnifften Daten zu finden ist sehr einfach.

Hier ist eine zusammenfassende Aufstellung der am weitesten verbreiteten UNIX Netzwerkdienste, die im Klartext übertragen.

Dienst	Port	Inhalt im Klartext	Anmeldung im Klartext	Wie wird übertragen
FTP	21,20	J	J	Text, binär
TFTP	69	J	N/A	Text, binär
Telnet	23	J	J	Text
SMTP	25	J	N/A	Text, binär
POP3	110	J	J	Text, binär
IMAP	143	J	J	Text, binär
rlogin	513	J	J	Text
rsh	514	J	J	Text
HTTP	80	J	J	Text, binär

Dienste wie Telnet und FTP, bei denen sowohl Inhalte als auch Anmeldeinformationen im Klartext übertragen werden, stellen das größte Risiko dar, da Angreifer diese Anmeldeinformationen wiederverwenden können und so das System nach Belieben verwenden können. Weiters können Befehlsverbindung im Klartext auch entführt werden und so von einem Angreifer verwendet werden um Befehle ohne Anmeldung auszuführen.

Hier ist eine Zusammenfassung der Risiken von Klartextdiensten:

Mögliche Aktivität	Risiko
Sniffen des Benutzernamens	Erleichtert Brute Force-Angriffe
Sniffen des Passworts	Ermöglicht Fernzugriff
Sniffen von FTP Inhalten	Diebstahl von Dateien
Entführung von Sitzungen	Befehle ausführen auf dem Zielsystem
Sniffen von HTTP Sitzungen	Enthüllt Web Anmeldeinformationen

U5.2 Betroffene Betriebssysteme
Alle UNIX Varianten enthalten Klartextdienste (Telnet und FTP sind am meisten verbreitet). Alle UNIX/Linux Varianten mit der möglichen Ausnahme der letzten Ausgaben von Free/OpenBSD kommen mit manchen dieser Dienste standardmäßig aktiviert.

U5.3 CVE/CAN Einträge
CVE-2000-0087

CAN-2002-0322, CAN-2000-0086

U5.4 Wie Sie herausfinden, ob Sie betroffen sind
Der effektivste und zuverlässigste Weg um herauszufinden, ob Klartextdienste verwendet werden ist, ein Sniffer Werkzeug zu verwenden, ähnlich den von Angreifern verwendeten.

Der am meisten verwendete Sniffer ist „tcpdump“. Starten Sie es mit:

```
# tcpdump -X -s 1600
```

um Klartextverbindungen zu entdecken. "Tcpdump" ist erhältlich auf http://www.tcpdump.org.

Ein anderes Werkzeug ist „ngrep”. Es erlaubt, nach bestimmten Mustern in der Netzwerkkommunikation wie „sername“ oder „assword“ (die Anfangsbuchstaben wurden aufgrund möglicher Großschreibung entfernt) zu suchen. Starten Sie das Programm mit:

```
# ngrep assword
```

„Ngrep“ ist erhältlich auf http://www.packetfactory.net/projects/ngrep/.

Es gib noch weitere raffinierte Werkzeuge, die speziell zur Erkennung von Anmeldeinformationen auf dem Netzwerk entwickelt wurden. „Dsniff“ ist das populärste Werkzeug dieser Art. Einfach starten mit:

```
# /usr/sbin/dsniff
```

so wird das Programm alle Username – Passwort Paare entdecken und ausgeben, die es auf dem Netzwerk in vielen Klartextprotokollen wie FTP, Telnet oder POP3 findet. Dsniff ist erhältlich auf http://www.monkey.org/~dugsong/dsniff/.

U5.5 Wie Sie sich dagegen schützen können
Es hilft, wenn Sie Ende-zu-Ende- oder zumindest Link-Level-Verschlüsselung verwenden. Manche Protokolle haben verschlüsselte Äquivalente wir POP3S oder HTTPS. Protokolle, die über keine eigenen Verschlüsselungsmöglichkeiten verfügen, können durch SSH (Secure Shell) oder SSL-Verbindungen getunnelt werden.

Zum Beispiel: FTP könnte durch sicherere Lösungen wie SFTP oder SCP (Teile des Secure Shell Pakets) ersetzt werden oder Sie verwenden einen Web Server um Dateien an ein breites Publikum zu verteilen.

Die populärste und flexibelste SSH Implementierung ist OpenSSH (erhältlich auf

http://www.openssh.org). Es läuft auf den meisten UNIX Varianten und kann für interaktiver Verbindungen (ersetzt Telnet, rlogin und rsh) und zum Tunneln (von POP3, SMTP, X11 und vieler anderer Protokolle) verwendet werden.

So können Sie zum Beispiel POP3 durch einen SSH-Verbindung tunneln. Auf dem POP3 Server muss auch der SSH Server laufen. Zuerst führen Sie auf dem Client folgenden Befehl aus:

```
# ssh -L 110:pop3.mail.server.com:110 username@pop3.mail.server.com
```

Jetzt verwenden Sie den E-Mail Client mit localhost, TCP port 110 (statt des üblichen ‚pop3.mail.server.com', port 110). Die gesamte Kommunikation zwischen Ihrem Rechner und dem POP3 Mail Server wird nun durch SSH getunnelt und so verschlüsselt.

Eine weitere populäre Lösung für verschlüsselte Tunnel ist „stunnel". Stunnel implementiert das SSL Protokoll (durch das OpenSSL Toolkit) und kann zum tunneln von verschiedenen Klartextprotokollen verwendet werden. Stunnel ist erhältlich bei http://www.stunnel.org/.

zum Anfang ^

U6 Sendmail

U6.1 Beschreibung

Sendmail ist das Programm, das die meisten auf UNIX und Linux Systemen verarbeiteten Mails sendet, empfängt und weiterleitet. Sendmail ist der populärste Mail Transfer Agent (MTA), und seine weite Verbreitung im Internet hat es zu einem Hauptziel von Angreifern gemacht, was über die Jahre zu zahlreichen Exploits geführt hat.

Die meisten dieser Exploits sind nur bei älteren oder nicht gepatchten Versionen des Programms erfolgreich. Obwohl die bekannten Schwachstellen gut dokumentiert sind und in neueren Versionen behoben wurden, sind heute noch immer so viele veraltete und falsch konfigurierten Versionen in Verwendung, weshalb Sendmail einer der am häufigsten angegriffenen Dienste bleibt. Unter den aktuellsten kritischen Schwachstellen sind:

- CERT Advisory CA-2003-12 Buffer Overflow in Sendmail
- CERT Advisory CA-2003-07 Remote Buffer Overflow in Sendmail
- CERT Advisory CA-2003-25 Buffer Overflow in Sendmail

CERT Advisory CA-2003-12 Buffer Overflow in Sendmail liefert die folgende exzellente Beschreibung eines Sendmail Buffer Overflows und der Gefahr, die es für die Unversehrtheit des Netzwerks darstellt.

> Diese Schwachstelle ist Nachricht-orientiert im Gegensatz zu Verbindungs-orientiert. Das bedeutet, dass diese Schwachstelle durch Inhalte einer speziell gestalteten Email-Nachricht ausgelöst wird, anstatt von Netzwerkverkehr einer tieferen Schicht. Das ist wichtig, da ein MTA, der diese Schwachstelle nicht besitzt diese bösartige Nachricht an andere Mailserver weitergibt, die mitunter auf der Netzwerkebene geschützt sind. Mit anderen Worten, anfällige Sendmail Server im Inneren des Netzes sind noch immer bedroht, sogar wenn der äußere Mailserver einen anderen MTA als Sendmail verwendet. Außerdem können Nachrichten, die diese Schwachstelle ausnützen können, oft ungehindert an vielen Packet-Filtern

und Firewalls vorbei.

Die Risiken, die durch die Verwendung von Sendmail verursacht werden, können in zwei große Gruppen unterteilt werden: Erhöhung der Rechte verursacht durch Buffer Overflows und falsche Konfiguration, wodurch Ihre Maschine ein Relay für Email beliebiger anderer Maschinen ist. Ersteres ist ein Problem auf allen Systemen, die noch immer alte oder nicht gepatchte Versionen des Programms verwenden. Das Zweite kommt von entweder fehlerhaften oder Standard Konfigurationsdateien und ist eines der Haupthindernisse bei der Bekämpfung der Fortpflanzung von Spam.

U6.2 Betroffene Betriebssysteme
Beinahe alle UNIX und Linux Systeme kommen mit einer installierten Version von Sendmail, die standardmäßig aktiviert ist und gestartet wird.

U6.3 CVE/CAN Einträge
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

U6.4 Wie Sie herausfinden, ob Sie betroffen sind
Sendmail hatte in der Vergangenheit eine große Zahl von Schwachstellen. Vertrauen Sie nicht unbedingt der Version, die Ihnen vom daemon gezeigt wird, da das nur aus einer Textdatei auf dem System gelesen wird, die vielleicht nicht richtig aktualisiert wurde.

Jede veraltete oder nicht gepatchte Version des Programms hat wahrscheinlich Schwachstellen.

Um die Version von Sendmail herauszufinden, verwenden Sie den folgenden Befehl:

```
echo \$Z | /usr/lib/sendmail -bt -d0
```

Abhängig von Ihrem System kann der Pfad zu Sendmail anders sein, und Sie müssen den Befehl entsprechend modifizieren damit er auf den richtigen Pfad zeigt.

Um herauszufinden, ob die Version, die Sie gerade verwenden aktuell ist, überprüfen Sie die aktuelle Version von Sendmail unter:
http://www.sendmail.org/current-release.html

U6.5 Wie Sie sich dagegen schützen können
Die folgenden Schritte sollten unternommen werden um Sendmail zu schützen:

1. Aktualisieren Sie auf die letzte Version und/oder implementieren Sie Patches. Der Quellcode kann auf http://www.sendmail.org/ gefunden werden. Wenn Ihre Version von Sendmail im Paket mit Ihrem Betriebssystem kam, sollten Patches auf der Site des Herstellers Ihres Betriebssystems verfügbar sein (verschiedene Hersteller-spezifische Informationen, inklusive Vorschläge bezüglich Kompilieren und Konfiguration sind auch auf http://www.sendmail.org verfügbar).
2. Sendmail ist typischerweise auf den meisten UNIX und Linux Systeme standardmäßig

aktiviert, auch auf jenen, die nicht als Mailserver oder –relay laufen. Lassen Sie auf diesen Maschinen Sendmail nicht als daemon auf diesem Maschinen laufen (deaktivieren Sie den "-bd" Schalter). Sie können noch immer Mails von diesem System senden, indem Sie es so konfigurieren, dass Sie es auf ein Mail Relay in der Sendmail Konfigurationsdatei (typischerweise /etc/mail/sendmail.cf) zeigen lassen.

3. Wenn Sie Sendmail als daemon laufen lassen müssen, stellen Sie sicher, dass Ihre Konfiguration so geplant wurde, dass Mail richtig und nur für Ihre Systeme weitergeleitet wird. Lesen Sie http://www.sendmail.org/tips/relaying.html und http://www.sendmail.org/m4/anti_spam.html als Unterstützung bei der richtigen Konfiguration Ihres Servers. Mit Sendmail 8.9.0 wurde allgemeines Relaying standardgemäß deaktiviert. Allerdings haben viele Betriebssystemhersteller es wieder mit deren Konfiguration reaktiviert. Wenn Sie die Version von Sendmail, die mit Ihrem Betriebssystem kommt verwenden, stellen Sie sicher, dass Ihr System nicht für Relaying verwendet wird.
4. Wenn Sie zu einer neuen Version von Sendmail wechseln, wird empfohlen auch die Konfigurationsdateien dieser Version zu verwenden, da ältere Konfigurationsdateien noch immer Relaying erlauben könnten auch wenn sie mit der neuesten Version verwendet werden. Mittlerweile ist es möglich, eine Sendmail Konfigurationsdatei (sendmail.cf) aus den mit der Sendmailversion mitgelieferten Konfigurationsdateien zu erzeugen. Weitere Details zur Konfiguration von Sendmail sind auf http://www.sendmail.org/m4/readme.html erhältlich.
5. Wenn Sie Sendmail herunterladen müssen Sie die PGP Signatur überprüfen um sicherzustellen, dass es eine authentische Version ist. Verwenden Sie Sendmail keinesfalls ohne die Integrität des Qullecodes überprüft zu haben. Es hat bereits in der Vergangenheit Kopien von Sendmail mit Trojanern gegeben. Bitte lesen Sie das CERT Advisory CA-2002-28 Trojan Horse Sendmail Distribution um mehr darüber zu erfahren. Die für die Signatur der Sendmail-Distributionen verwendeten Schlüssel sind auf http://www.sendmail.org/ftp/PGPKEYS erhältlich. Wenn Sie nicht über PGP verfügen, sollten Sie die Integrität des Sendmail Quellcodes mit MD5 Checksummen überprüfen.
6. Zusätzliche Informationen über sicherere Konfiguration und Betrieb von Sendmail ist unter den folgenden Links erhältlich:

   http://www.sendmail.org/secure-install.html
   http://www.sendmail.org/m4/security_notes.html
   http://www.sendmail.org/~gshapiro/security.pdf

zum Anfang ^

U7 Simple Network Management Protocol (SNMP)

U7.1 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 ausgenützt 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.

U7.2 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.

U7.3 CVE/CAN Einträge
CVE-2001-0236, CVE-2002-0797

CAN-1999-0186, CAN-1999-0254, CAN-1999-0516, CAN-1999-0517, CAN-1999-0615, CAN-2002-0012, CAN-2002-0013, CAN-2002-0796

U7.4 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 in dem Sie eine leere Mail an snmptool@sans.org senden. Sie erhalten dann eine Antwort mit der URL, von wo Sie das Programm herunterladen können.
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.

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.

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.

U7.5 Wie Sie sich dagegen schützen können
Schwachstelle 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 herstellerspezifische 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. Einen 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 ^

U8 Secure Shell (SSH)

U8.1 Beschreibung

Secure Shell (SSH) ist ein populärer Dienst für sichere Anmeldungen, Ausführen von Befehlen und Übertragung von Dateien über das Netzwerk. Die meisten UNIX-basierten Systeme verwenden entweder das Open Source Paket OpenSSH der die kommerzielle Version der SSH Communication Security. Obwohl SSH um vieles sicherer ist als Telnet, FTP und die r-Befehle, die es ersetzen soll, wurden viele Fehler in beiden Implementierungen gefunden. Die meisten sind kleinere Bugs, aber einige sind große Sicherheitsprobleme, die sofort repariert werden sollten. Das gefährlichste der aktiv ausgenützten Löcher erlaubt Angreifern, Zugriff als Root auf anfälligen Maschinen.

Es sollte auch beachtet werden, dass eine wachsende Zahl von SSH Clients und Servern in der Windows-Welt existiert, und dass der Großteil der Informationen in diesem Abschnitt sowohl *nix als auch Windows Implementierungen von SSH betrifft.

Obwohl SSH hier als eine der Top 20 Schwachstellen präsentiert wird, ist das vor allem aufgrund der falschen Handhabung von SSH. Besonders falsche Konfigurationen und das Versäumnis, rechtzeitig Updates und Patches einzuspielen, sorgen dafür, dass SSH auf dieser Liste zu finden ist.

SSH2 ist eigentlich ein mächtiges Werkzeug, das, wenn es richtig konfiguriert und gewartet wird, helfen kann, viele der anderen Top 20 Schwachstellen, besonders jene, die Daten im Klartext über nicht vertrauenswürdige Netze wie das Internet senden, zu entschärfen. Viele der Schwachstellen in Protokollen wie POP3, FTP (ersetzbar durch SFTP von SSH2), Telnet, http und die rhost-basierten Programme (rlogin, rcp, und rsh) basieren auf Belauschen von Klartext Übertragungen oder der Manipulation von Client-Server-Sitzungen. Das macht die Verschlüsselung und die Verwaltung der Anmeldeschlüssel von SSH2 gemeinsam mit seiner Fähigkeit, Sitzungen weiterzuleiten oder umzuleiten, zu einem attraktiven Typ von VPN für sonst belauschbaren Verkehr.

Es wurde gezeigt, dass das SSH1 Protokoll potentiell anfällig ist, dass Sitzungen unterwegs unter bestimmten Bedingungen entschlüsselt werden können. Daher wird Administratoren empfohlen, wenn möglich das stärkere SSH2 Protokoll zu verwenden.

> **Hinweis:** SSH1 und SSH2 sind nicht kompatibel. Mit wenigen Ausnahmen müssen die Versionen auf Server und Client übereinstimmen.

Weiters sollten Anwender von OpenSSH beachten, dass die OpenSSL Bibliotheken, die üblicherweise für OpenSSH benötigt werden, eigene Schwachstellen haben. Bitte lesen Sie das CERT Advisory 2002-23 für nähere Informationen. Sie sollten auch beachten, dass eine Version von OpenSSH mit Trojaner für eine kurze Zeit im Sommer 2002 verteilt wurde (CAN-1999-0661). Bitte lesen Sie http://www.openssh.org/txt/trojan.adv für nähere Informationen um sicherzustellen, dass Ihre Version nicht betroffen ist.

U8.2 Betroffene Betriebssysteme
Alle UNIX oder Linux Systeme, die OpenSSH 3.3 oder älter (Version 3.6.1 wurde am 1. April 2003 veröffentlich) oder SSH Communication Security's SSH 3.0.0 oder älter (3.2.5 wurde am 30. Juni 2003 veröffentlicht) verwenden.

U8.3 CVE/CAN Einträge
SSH der SSH Communications Security:
CVE-2000-0217, CVE-2000-0575, CVE-2000-0992, CVE-2001-0259, CVE-2001-0361, CAN-2001-0471, CVE-2001-0553

SSH von OpenSSH:
CVE-2000-0525, CVE-2000-1169, CVE-2001-0060, CVE-2001-0144, CVE-2001-0361, CVE-2001-0872, CVE-2002-0002, CVE-2002-0083

CAN-2001-1380, CAN-2002-0575, CAN-2002-0639, CAN-2002-0640, CAN-2002-0765, CAN-2003-0386

Zahlreiche Implementierungen von SSH:
CAN-2002-1357, CAN-2002-1358, CAN-2002-1359, CAN-2002-1360

U8.4 Wie Sie herausfinden, ob Sie betroffen sind
Verwenden Sie einen Schwachstellenscanner um herauszufinden, ob Sie eine anfällig Version verwenden, oder überprüfen Sie die Version des Programms, angezeigt durch den Befehl 'ssh –V'.

Das Programm ScanSSH ist insbesondere brauchbar um SSH Server zu identifizieren, die gefährlicherweise nicht gepatcht wurden. Das Command line Werkzeug ScanSSH scannt eine Liste von Adressen und Netzwerke nach SSH Protokoll Servern und liefert deren Versionen. Es wurde von Niels Provos geschrieben und unter der BSD-Lizenz veröffentlicht, die aktuellste Version wurde am 20. November 2001 freigegeben und ist unter http://www.monkey.org/~provos/scanssh/ verfügbar.

U8.5 Wie Sie sich dagegen schützen können

1. Aktualisieren Sie auf die aktuellste Version von entweder OpenSSH oder SSH. Oder, wenn SSH oder OpenSSH mit Ihrem System installiert geliefert wurden, holen Sie die neuesten Patches vom Hersteller Ihres Betriebssystems. Wenn Sie OpenSSL verwenden, vergewissern Sie sich, dass Sie die neueste Version dieser Bibliotheken verwenden.
2. Wo möglich, steigen Sie von SSH1 auf SSH2 um. Es scheint, als würde SSH1 nicht weiter entwickelt werden, im Gegensatz zu SSH2. Wenn der Wechsel nicht möglich ist, beginnen Sie Pläne und Strategien zu entwickeln, die diesen Wechsel in der Zukunft ermöglicht.
3. Beide SSH Implementierungen enthalten eine Reihe von Konfigurationsoptionen um einzuschränken, welche Maschinen sich verbinden können, welche Benutzer sich

anmelden können und über welche Mechanismen das passiert. Administratoren sollen festlegen, wie diese Optionen am geeignetsten für ihre Umgebung eingestellt werden können.
4. Überprüfen Sie, dass kein SSH Client so konfiguriert ist, dass er auf rsh zurückfällt, wenn er sich zu einem Server, der SSH nicht unterstützt, verbinden will. Der Fallbacktorso Wert sollte auf „No“ in der SSH Konfigurationsdatei gesetzt sein.
5. Bestimmen Sie die Verwendung von Blowfish Verschlüsselung statt 3DES, was der Standard Ihrer Version sein könnte. Das ermöglicht schnellere Verschlüsselung ohne die effektive Stärke der Verschlüsselung zu reduzieren.
6. Ein Rechner mit SSH Server muss selbst ausreichend geschützt sein, andernfalls können Schwachstellen, die die Kompromittierung des Rechners ermöglichen, den SSH Dienst gefährden.

zum Anfang ^

U9 Fehlkonfiguration der Enterprise Dienste NIS/NFS

U9.1 Beschreibung

Das Network File System (NFS) und das Network Information Service (NIS) sind zwei wichtige in UNIX Netzwerke verwendete Dienste. NFS ist ein ursprünglich von Sun Microsystems entwickelter Dienst um Dateien zwischen UNIX Systemen eines Netzwerks zu teilen. 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 bekanntesten Beispiele dieser Maps sind die passwd und group Dateien, die verwendet werden um die Benutzerverwaltung zu zentralisieren.

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 zu verwenden, die Werte aus der 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.

U9.2 Betroffene Betriebssysteme

Beinahe alle UNIX und Linux Systeme werden mit einer installierten und oft auch aktivierten Version von NFS und NIS ausgeliefert.

U9.3 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

CAN-1999-0165, CAN-1999-0169, CAN-2000-0800, CAN-2002-0830, CAN-2002-1228,

CAN-2003-0252, CAN-2003-0379, CAN-2003-0576

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

U9.4 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 veröffentlichen 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 Benutzer die Sicherheitsanweisungen einhalten. Ein Passwortcracker kann dafür verwendet werden.

> **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 aus um zu sehen, was exportiert wird. Überprüfen Sie, ob Ihre Mounts von Ihren Sicherheitsvorschriften gedeckt sind.

U9.5 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 aufführen, wodurch andere Systeme daran gehindert werden, sich als NIS Server auszugeben.
2. Während 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.

Die folgenden Schritte beziehen sich auf die Konfiguration von NFS:

1. Verwenden Sie numerische IP-Adressen oder Voll qualifizierte Domain Namen statt Aliases wenn Sie Clients in der Datei /etc/exports erlauben.
2. 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 Ausnützen verschiedener Lücken um auf das Dateisystem zuzugreifen. ftp://coast.cs.purdue.edu/pub/tools/unix/nfsbug/
3. Verwenden Sie /etc/exports um den Zugriff auf das NFS Dateisystem einzuschränken, indem Sie Parameter hinzufügen:
    - 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)).
    - 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)).
    - 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 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)).
    - Eine komplette Sammlung der Parameter kann in der Man-Page von /etc/exports gefunden werden. http://www.netadmintools.com/html/5exports.man.html
4. Auf Solaris-Betriebssystemen aktivieren Sie Port Monitoring indem Sie die Zeile „set nfssrv:nfs_portmon = 1“ an die Datei /etc/system anhängen.

Linux Systeme verweigern standardmäßig die Zusammenarbeit mit NFS-Clients von einem nicht-privilegierten Port.

Allgemeine Überlegungen bezogen auf NIS und NFS:

1. Überarbeiten Sie Ihre Firewall Policies und vergewissern Sie sich, dass Sie alle nicht benötigen Ports wie auch Port 111 (Portmap) und Port 2049 (Rpc.nfsd) blockieren. Weiters erlauben Sie den Zugriff auf NIS und NFS Server nur von autorisierten Clients aus. Als lokale 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 zu entfernen.

zum Anfang ^

U10 Open Secure Sockets Layer (SSL)

U10.1 Beschreibung

Die Open Source OpenSSL Bibliothek ist ein populäres Paket um kryptographische Sicherheit zu Anwendungen hinzuzufügen, die über das Netzwerk kommunizieren. Obwohl Apache die wahrscheinlich bekannteste Anwendung dieses Pakets ist (um https zu unterstützen: Verbindungen auf Port 443), wurden viele andere Programme verändert um durch OpenSSL ihre Sicherheit zu erhöhen.

Die übliche Anwendung von OpenSSL ist als Toolkit, das andere Applikationen verwenden um kryptographische Sicherheit für Verbindungen zur Verfügung zu stellen. Daher wird selten OpenSSL direkt angegriffen, sondern vielmehr Anwendungen, die es verwenden. Ein populärer Exploit greift den Gebrauch des Apache Servers von OpenSSL an. Nur weil Sie nicht Apache mit OpenSSL-Unterstützung einsetzen heißt das aber nicht, dass Sie sicher sind. Eine geeignete Modifikation des Exploits könnte fähig sein, Sendmail, openldap, CUPS, oder ein anderes Programm, das OpenSSL verwendet und auf der Zielmaschine installiert ist, anzugreifen.

In OpenSSL wurden zahlreiche Schwachstellen gefunden, von welchen die 4 schwerwiegendsten in CAN-2002-0655, CAN-2002-0656, CAN-2002-0557 und CAN-2002-0659 aufgezählt sind. Diese erlauben das Ausführen von beliebigem Code als der Benutzer der OpenSSL Bibliotheken (was in manchen Fällen, wie z.B. Sendmail, der Benutzer „root“ ist).

U10.2 Betroffene Betriebssysteme

Alle Unix und Linux Systeme, die OpenSSL 0.9.7 oder älter verwenden. Beachten Sie, dass sehr oft OpenSSL installiert ist um andere Pakete zu unterstützen. Zum Beispiel verwenden (unter anderem) Systempakete wie Apache, CUPS, Curl, OpenLDAP, Stunnel und Sendmail auf RedHat Linux 9.0 die OpenSSL Bibliotheken um Verbindungen abzusichern.

U10.3 CVE/CAN Einträge

CVE-1999-0428, CVE-2001-1141

CAN-2000-0535, CAN-2002-0655, CAN-2002-0656, CAN-2002-0557, CAN-2002-0659, CAN-2003-0078, CAN-2003-0131, CAN-2003-0147

U10.4 Wie Sie herausfinden, ob Sie betroffen sind

Überprüfen Sie die Ausgabe des Befehls ‚openssl version’. Wenn die Version nicht 0.9.7.a oder neuer ist, sind Sie angreifbar.

U10.5 Wie Sie sich dagegen schützen können

1. Wechseln Sie auf die neueste Version von OpenSSL. Wenn OpenSSL auf Ihrem System

bereits vorinstalliert war, holen Sie sich die neuesten Patches vom Hersteller Ihres Betriebssystems. Beachten Sie, dass es in manchen Fällen notwendig sein kann, Anwendungen neu zu kompilieren oder zu linken um die neuen Bibliotheken zu aktivieren.

2. Wenn in Ihrer Umgebung möglich, überlegen Sie sich, ob Sie nicht ipfilter oder andere Firewalls verwenden können um den Zugriff auf Ihre OpenSSL 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 ^

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
DHCP Client	68	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 Warenzeich  er 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, Alutiiq 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 Prosise, 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 ^