CITRIX®

Leitfaden für sichere Citrix Systeme

Entwurf / Planung / Umsetzung

von André Dannbacher und Fabian Kienle

White Paper



COPYRIGHT

Die Informationen in dieser Broschüre entsprechen dem Kenntnisstand zum Zeitpunkt der Veröffentlichung. Es wird ausdrücklich darauf hingewiesen, dass die vorliegenden Informationen aufgrund unregelmäßiger Änderungen nicht mehr aktuell sein können. Diese Informationen enthalten keine wie auch immer gearteten Zusicherungen, und es wird weder Gewährleistung noch Haftung für Schäden übernommen, die aus der Nutzung dieser Informationen entstehen.

Die in den Beispielen verwendeten Firmen, sonstigen Namen und Daten sind frei erfunden, soweit nichts anderes angegeben ist.

Ohne ausdrückliche schriftliche Erlaubnis darf kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden – unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln – elektronisch oder mechanisch – dies geschieht.

Alle genannten Handelsbezeichnungen sind die Servicemarke, Marke oder eingetragene Marke des jeweiligen Herstellers.

Oktober 2002

DIE AUTOREN

André Dannbacher ist Technical Consultant bei der DNS Deutschland GmbH. Seine Tätigkeiten: Pre-Sales, Consulting und Training von Server-Based-Computing-Lösungen mit Citrix-Produkten auf Microsoft Windows- und Sun Solaris-Systemen.

Fabian Kienle ist Systems Engineer bei Citrix Systems GmbH. Seine Tätigkeiten: Pre-Sales, das Training sowie die technische Betreuung der CSN-Partner in den Projekten. Neben MetaFrame-Plattformen ist sein Schwerpunkt IT-Security.

Ein herzlicher Dank gilt Josef Zeiler für das Fachlektorat.

Einleitung und Überblick

Die Dokumentation „Securing a MetaFrame Environment“ dient als ergänzender Leitfaden für Entwurf, Planung und Umsetzung sicherer Citrix-Systeme.

Für die sichere Datenübertragung über das Internet mit geschütztem Zugang ins Firmennetz gibt es mittlerweile wirkungsvolle Technologien, welche sich durchgesetzt und bewährt haben.

Allerdings zeigt sich bei gründlicher Betrachtung eines IT-Gesamtsystems, dass dennoch einige Sicherheitslücken vorhanden sind, die ein nicht akzeptables Restrisiko bedeuten. Hierbei beschäftigen wir uns in dieser Broschüre schwerpunktmäßig mit Sicherheitslösungen im Bereich des Betriebssystems Microsoft Windows, auf dem die Citrix-Produkte installiert sind.

Unternehmenswichtige Ressourcen eines IT-Systems sind Daten, Kommunikation, Dienste und Anwendungen. Diese gilt es wirkungsvoll vor unbefugtem Zugriff sowie vor Manipulation und Sabotage zu schützen.

Um Daten und Informationen darzustellen, auszuwerten oder weiter zu verarbeiten, greifen die Benutzer eines IT-Systems anhand lokaler oder veröffentlichter Anwendungen auf Dienste und Server zu und nutzen hierfür entsprechende Kommunikationsverbindungen (z.B. Internet).

Was haben die Angreifer vor?

Angriffe auf Rechnersysteme und Netzwerkkomponenten erfolgen aus ganz unterschiedlichen Beweggründen. Mit gezielten Angriffen wird versucht, an Informationen zu kommen oder gezielt Schaden zu verursachen. Diese Angriffsziele können privat, politisch oder wirtschaftlich begründet sein. Die damit verursachten Ausfälle sind in jedem Fall unberechenbar und verursachen hohe Schäden.

Was die typische Vorgehensweise betrifft, versuchen Angreifer zunächst Informationen und Angaben über das Zielsystem sowie über das Netzwerk zu sammeln. Dabei werden weder Daten modifiziert noch der Betrieb gestört, denn das würde ja auffallen, noch bevor man die gewünschte Wirkung erzielt. Vorerst geht es nur darum, die Systeme, die Zugangsdaten und ein Konfigurationsschema zu ermitteln.

Erst anschließend werden die Systeme gezielt attackiert, um Daten bzw. Informationen auszuspionieren, zu verändern oder zu zerstören.

Somit sind für jedes Unternehmen eine sichere EDV-Technik und qualifiziertes Sicherheitsmanagement die Eckpfeiler der IT-Sicherheit. Nur so lassen sich wichtige Geschäftsprozesse durchgängig aufrechterhalten und sensible Daten wirkungsvoll schützen.

Den gesamten Sicherheitsprozess – von der Erarbeitung des richtigen Sicherheitskonzeptes und der entsprechenden Sicherheitsrichtlinien, über die Planung und praktische Umsetzung der Sicherheitsmaßnahmen, bis hin zur Wartung und Revision wollen wir im Folgenden erläutern.

Die technische Ausgangslage

Die Citrix-Systeme MetaFrame XP, NFuse Classic (und Enterprise Services for NFuse) sowie Citrix Secure Gateway laufen auf der Microsoft Server-Betriebssystemplattform Windows 2000. Dabei nutzt die Software die Betriebssystemdienste wie Terminal Services und Internet Information Services. Sie bilden ein System, das über Web-Dienste und Authentifizierung die bereitgestellten Anwendungen sicher per SSL (Socket Secure Layer) oder TLS (Transport Layer Security) zum Client übertragen.

Was gilt es zu erreichen?

Bei der Nutzung von Anwendungen und Daten sowie beim Zugriff und der Übertragung via Internet gilt es hohe Sicherheitsforderungen zu erfüllen.

EDV-Sicherheit lässt sich in folgende Aspekte aufgliedern:

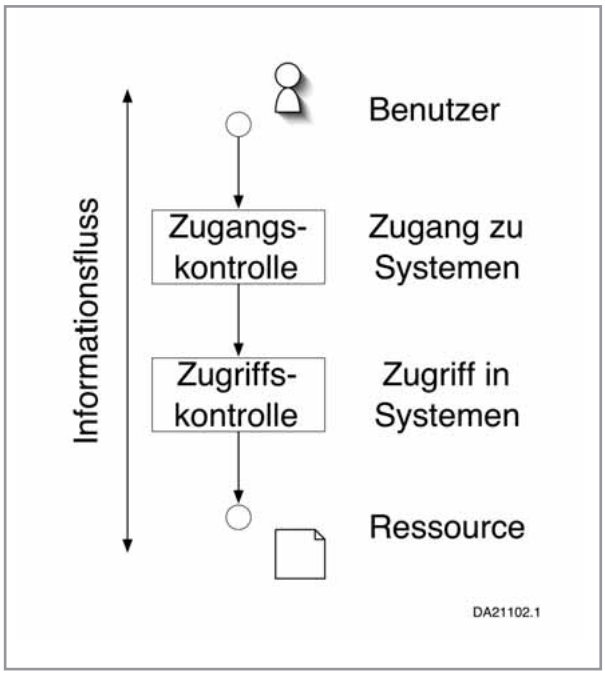
- **Funktionssicherheit (Safety) –** das System hat keine unzulässigen funktionalen Zustände.
- **Informationssicherheit (Security) –** Unbefugte können weder auf Informationen zugreifen noch sie verändern.
- **Datensicherheit (Protection) –** Kein unerlaubter Zugriff auf Systeme und Daten. Im weiteren Sinne Sicherung der Daten anhand von Sicherungskopien, um sich vor Datenverlusten zu schützen.
- **Datenschutz (Privacy) –** Schutz vertraulicher persönlicher Daten im engeren Sinne des Bundesdatenschutzgesetzes (BDSG).

Sicherheit ist ein dynamischer Prozess. Um Sicherheit in einem Gesamtsystem gewährleisten zu können, muss man zunächst die damit verbundenen Anforderungen berücksichtigen, sich die entsprechenden Mechanismen vergegenwärtigen und überlegen, wie man diesen Prozess implementiert und umsetzt.

Sicherheitsanforderungen

Die Sicherheitsanforderungen lassen sich untergliedern in:

- Zugangskontrolle
- Zugriffskontrolle und
- Informationsfluss



Daraus ergeben sich im einzelnen die folgenden Sicherheitsanforderungen:

- **Authentifizierung –** Beweis einer Identität durch Echtheitsprüfung (Authentizität).
- **Autorisierung –** Die Zugriffskontrolle erfolgt nach Authentifizierung und gewährt den Benutzern gemäß deren jeweiliger Befugnis den Zugriff auf die ihnen zugeteilten Ressourcen.
- **Anonymität –** Schutz personenbezogener Daten vor Sammlung und Auswertung durch Datenschutzerklärung (Privacy Statement).
- **Verbindlichkeit –** Übermittlung (Empfängernachweis) und Ursprung (Urhebernachweis) der rechtsverbindlichen Kommunikation und Information werden nach vorgegebenen Kriterien anerkannt.
- **Vertraulichkeit –** Schutz der Informationen beim Transport vor unbefugtem Zugriff. Die Informationen sollen nur für autorisierte Personen zugänglich sein.
- **Integrität –** Die Unversehrtheit von Daten durch Schutz vor Manipulation und Zerstörung: Informationen müssen vor Löschen und ungewollten Veränderungen bewahrt werden.
- **Verfügbarkeit –** Das System muss bereitstehen, wenn es gebraucht wird. Steht das System nicht zur Verfügung, ist auch die dort vorhandene Information nicht zugänglich.
- **Konsistenz –** Das System soll sich so verhalten, wie es die autorisierten Benutzer erwarten.

Die eingeführten und eingesetzten Mechanismen müssen ständig auf ihre Zweckerfüllung und Einhaltung hin überprüft werden.

Formale Methoden allein reichen nicht aus, um hinsichtlich der praktischen Anwendbarkeit die Sicherheitslücken zu schließen. Die Herausforderungen von Sicherheitsstrategien und -anwendungen ist, die Vorgänge mit großer Sorgfalt abzuwickeln und ständig auf dem neuesten Stand zu halten.

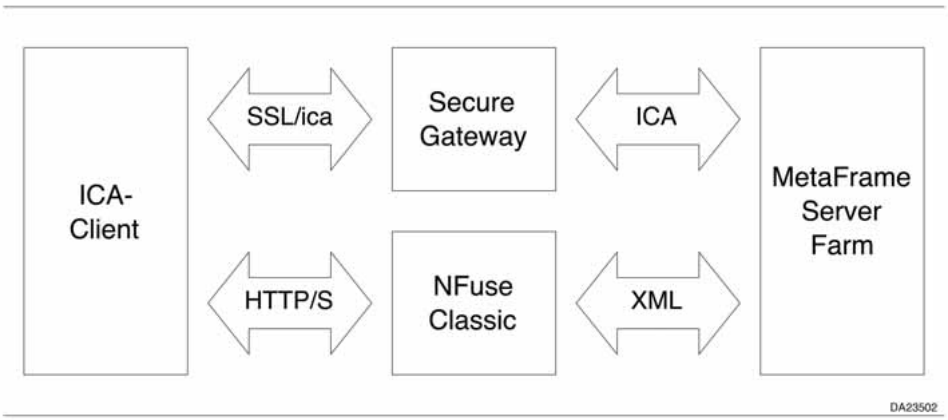
Es gibt Sicherheitslösungen mit unterschiedlichsten Schwerpunkten. Je besser sich die einzelnen Sicherheitslösungen miteinander verzahnen lassen, umso durchgängiger kann man die Anforderungen im Bereich der EDV-Sicherheit umsetzen.

Das Citrix-Gesamtsystem

Ein sicheres Citrix MetaFrame-System in einer Internet/Intranet-Lösung besteht aus einer MetaFrame-Serverfarm, dem ICA-Client sowie NFuse Classic und Citrix Secure Gateway.

Citrix-Systemkomponenten

Um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen sowie den Schutz der EDV-Systeme sicherzustellen, muss man die Kommunikation durch sichere Authentifizierung und Verschlüsselung vor unbefugtem Zugriff schützen.



MetaFrame XP

Eine MetaFrame-Serverfarm besteht aus einer Gruppe von MetaFrame-Servern, die eine Verwaltungseinheit darstellt und ICA-Benutzern Anwendungen bereitstellt. Beim ICA-Clientgerät kann es sich um ein beliebiges Computerendgerät handeln, auf dem sich ein ICA-Client und – im Einsatz mit NFuse – ein Webbrowser ausführen lässt.

ICA-Client

Mit Hilfe der ICA-Clientsoftware von Citrix können Anwender von den verschiedensten Clientplattformen aus eine Verbindung mit Citrix MetaFrame-Servern herstellen.

NFuse Classic

NFuse Classic ist ein webbasiertes System, um Anwendungen anhand eines Standardwebbrowsers via Internet bereitzustellen. So kann der Benutzer über geschützte Verbindungen auf MetaFrame-basierende Anwendungen zugreifen. In einem auf Intranet- und Internetstrukturen basierenden Citrix-System übernimmt der NFuse Classic-Server die Rolle einer webbasierten Program-Neighborhood-Oberfläche, über die Verbindungen zu veröffentlichten Anwendungen einer MetaFrame-Serverfarm hergestellt werden. Der NFuse Classic-Server fragt die MetaFrame-Serverfarm nach den Informationen zur Anwendungsgruppe ab und formatiert die Ergebnisse dann in HTML-Seiten, die der Benutzer sich per Webbrowser anzeigen lassen kann. NFuse Classic setzt Java-Objekttechnologie ein, die auf einem Webserver ausgeführt wird und dynamisch HTML-basierte Darstellungen der MetaFrame-Serverfarm für die einzelnen Benutzer erstellt. Dabei werden jedem Benutzer genau jene Anwendungen bereitgestellt, die in der MetaFrame-Serverfarm für ihn veröffentlicht wurden.

Citrix Secure Gateway

MetaFrame XP und NFuse Classic unterstützen Verschlüsselung gemäß SSL (Secure Sockets Layer) und TLS (Transport Layer Security). TLS ist die neueste standardisierte Version des SSL-Protokolls zur Sicherung der Kommunikation. SSL und TLS sind Standard-Protokolle, die Datenverschlüsselung, Serverauthentifizierung, Nachrichtenintegrität und optionale Clientauthentifizierung für eine TCP/IP-Verbindung bereitstellen. Die auf MetaFrame verwendeten Serverzertifikate funktionieren für SSL wie auch TLS.

Die SSL-Unterstützung wird durch Erweiterung der NFuse Classic-Java-Objekte bereitgestellt und erfordert die Verwendung von Citrix SSL-Relay in der Serverfarm. Das Implementieren von SSL auf dem Webserver und die Verwendung von Webbrowsern, die SSL unterstützen, gewährleisten eine sichere Datenübertragung im Netzwerk. Citrix Secure Gateway stellt zusammen mit NFuse Classic einen zentralen und sicheren, verschlüsselten Zugangspunkt über das Internet zu MetaFrame-Servern in internen Unternehmensnetzwerken bereit.

Citrix Secure Gateway vereinfacht die Zertifikatverwaltung, da nur der Secure-Gateway-Server und nicht jeder MetaFrame-Server in der Serverfarm ein Serverzertifikat benötigt.

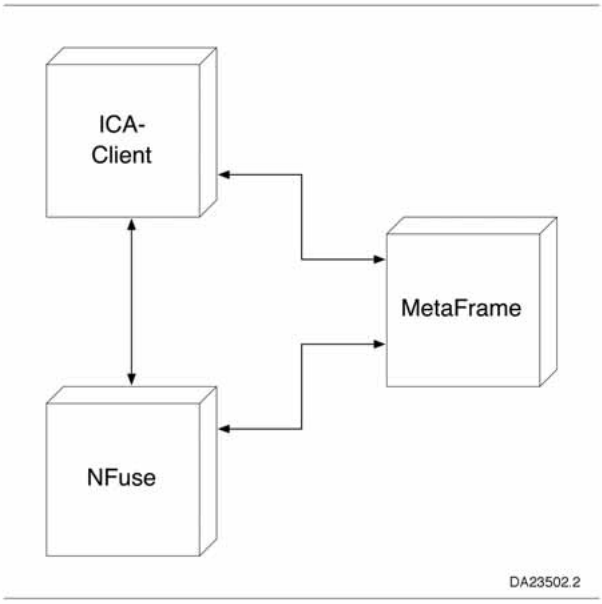
Erhöhte Sicherheit bei der Authentifizierung bietet das sogenannte Ticketing. Das bedeutet: NFuse kann Tickets erstellen, mit denen Benutzer für Citrix-Anwendungen authentifiziert werden. Tickets haben eine konfigurierbare Gültigkeitsdauer und gelten nur für eine einzige Anmeldung. Nach Benutzung oder Ablauf ist das Ticket ungültig und für den Zugriff auf Anwendungen nicht mehr brauchbar.

Durch die Verwendung von Ticketing müssen Anmeldeinformationen nicht explizit in den ICA-Dateien enthalten sein, mit denen NFuse Classic Anwendungen startet. NFuse Classic ermöglicht die Konfiguration verschiedener NAT-Typen (Network Adress Translation = Netzwerkadressübersetzung). So lässt sich zum Beispiel, abhängig von der Konfiguration der Firewalls und der MetaFrame-Server, das Verhalten der standardmäßigen Adressübersetzung angeben, oder man kann die Einstellungen für bestimmte Adressen konfigurieren. Außerdem ist die Konfiguration der Portadressen möglich. Hiermit lässt sich der Datenverkehr unter Verwendung einer einzelnen externen IP-Adresse über verschiedene Ports an die jeweiligen internen MetaFrame-Server weiterleiten.

Benutzer können sich unter NFuse Classic auch mit einer Smartcard authentifizieren, die von einem Smartcardleser gelesen wird, der an das Clientgerät angeschlossen ist. Mit Smartcards müssen sich Benutzer nicht mehrere Anmeldemethoden, Benutzer-IDs und Kennwörter merken. Allerdings muss für diese Funktion NFuse Classic auf IIS ausgeführt werden, und Benutzer benötigen den Internet Explorer (ab Version 5.0) auf Windows 2000 oder höher.

Sicherheitsanforderungen an Citrix-Systeme

Kommunikationsbeziehungen zwischen Citrix-Komponenten in einer konventionellen Citrix NFuse-Umgebung



Kommunikation zwischen ICA-Clientgerät und NFuse-Classic-Server

Risiken ergeben sich bei der Übergabe von NFuse-Classic-Daten zwischen Webbrowsern und Webservern. Folglich werden Strategien zum Schutz der Daten bei der Übermittlung sowie bei der Speicherung auf dem Client notwendig.

Kommunikation zwischen NFuse-Classic-Server und MetaFrame-Server

Hier geht es um die Sicherung der Authentifizierung und der Informationen über veröffentlichte Anwendungen, die zwischen dem NFuse Classic-Server und der Citrix Serverfarm ausgetauscht werden.

Kommunikation zwischen ICA-Client und MetaFrame-Server

Hier beschreiben wir die Risiken, welche mit dem Übertragen von ICA-Sitzungsinformationen zwischen ICA-Clients und MetaFrame-Servern verbunden sind sowie die Implementierung der NFuse-Classic- und MetaFrame-Sicherheitsfunktionen, die solche Daten schützen.

Kommunikation zwischen ICA-Clientgerät und NFuse-Classic-Server

Bei der Kommunikation zwischen ICA-Clientgeräten und dem NFuse-Classic-Server werden verschiedene Datentypen übergeben. Wenn sich der Benutzer identifiziert, Anwendungen durchsucht und dann eine Anwendung für die Ausführung auswählt, tauschen der Webbrowser und der Webserver Anmeldeinformationen, Anwendungsgruppenlisten und Dateien für die Sitzungsinitialisierung aus. Folgende Daten werden im Rahmen dieser Übertragungen auf dem Netzwerk weitergeleitet:

- **HTML-Formulardaten –** NFuse Classic-Websites übertragen die Anmeldeinformationen des Benutzers zum Anmeldezeitpunkt mit Hilfe eines HTML-Standardformulars an den Webserver. Das NFuse-Classic-Formular übergibt den Benutzernamen im Klartext und verwendet für den Domänennamen und das Kennwort nur den Verschlüsselungsgrad „Basic“.
- **HTML-Seiten und Sitzungscookies –** Hat der Benutzer die Anmeldeinformationen auf der NFuse-Classic-Anmeldeseite eingegeben, werden seinen Anmeldeinformationen auf dem Webserver gespeichert und von einem Sitzungscookie geschützt. Die HTML-Seiten, die vom Webserver an den Browser gesendet werden, enthalten Anwendungsgruppen. Auf diesen Seiten werden jene Anwendungen genannt, die für den Benutzer verfügbar sind.

- **ICA-Dateien –** Sobald der Benutzer eine Anwendung auswählt, sendet der Webserver eine ICA-Datei für diese Anwendung an den Browser. Die ICA-Datei enthält ein Ticket, das für die Anmeldung beim MetaFrame-Server verwendet werden kann (außer bei Smartcard-Authentifizierung).

Risiken

Angreifer können NFuse-Classic-Daten abfangen, während diese im Netzwerk zwischen dem Webserver und dem Browser übertragen oder auf das Clientgerät geschrieben werden:

- Ein Angreifer kann Anmeldedaten, das Sitzungscookie und HTML-Seiten abfangen, die zwischen dem Webserver und dem Webbrowser übermittelt werden.
- Zwar ist das von NFuse Classic verwendete Sitzungscookie temporär und wird entfernt, wenn der Benutzer den Webbrowser schließt. Ein Angreifer mit Zugriff auf den Webbrowser des Clientgeräts kann das Cookie jedoch abrufen und die Anmeldeinformationen verwenden.
- Die ICA-Datei enthält zwar keine Anmeldeinformationen, aber ein Einmalticket, das standardmäßig nach 200 Sekunden abläuft. Ein Angreifer kann ggf. mit der abgefangenen ICA-Datei eine Verbindung zum MetaFrame-Server herstellen, bevor der autorisierte Benutzer mit dem Ticket eine Verbindung herstellt.
- Falls auf dem ICA-Win32-Client die Passthrough-Authentifizierung aktiviert ist, könnte ein Angreifer dem Benutzer eine ICA-Datei übermitteln, welche die Anmeldeinformationen des Benutzers an einen unbefugten oder gefälschten MetaFrame-Server weiterleitet.

Empfehlungen

Die folgenden Empfehlungen kombinieren Sicherheitspraktiken gemäß Industriestandard bezüglich sicherer Protokolle einerseits und von Citrix zur Verfügung gestellte Sicherheitsmaßnahmen andererseits. Auf diese Weise werden Daten geschützt, die zwischen Clientgeräten und dem Webserver übertragen werden sowie die Daten, die auf Clientgeräte geschrieben werden.

Implementierung SSL/TLS-fähiger Webserver und Webbrowser

Das Sichern der Webserver-zu-Webbrowser-Komponente in der NFuse-Classic-Kommunikation beginnt mit dem Implementieren sicherer Webserver und Webbrowser. Sichere Webserver verwenden die SSL/TLS-Technologie zum Sichern des Webverkehrs.

In einer typischen Webserver-zu-Webbrowser-Transaktion überprüft der Webbrowser zuerst die Identität des Webservers, indem er das Serverzertifikat des Webservers mit einer Liste der vertrauenswürdigen Zertifizierungsstellen vergleicht. Nach dieser Überprüfung verschlüsselt der Webbrowser Seitenanfragen des Benutzers und entschlüsselt dann die Dokumente, die vom Webserver zurückgegeben werden. Am Ende der Transaktion stellen TLS- oder SSL-Nachrichtenintegritätsprüfungen sicher, dass die Daten bei der Übertragung nicht manipuliert wurden.

In einer NFuse-Classic-Bereitstellung sorgt die Authentifizierung und Verschlüsselung mit SSL/TLS für eine sichere Verbindung, über die der Benutzer Anmeldeinformationen übergeben kann, welche dann auf der NFuse-Anmeldeseite hinterlegt werden. Vom Webserver gesendete Daten einschließlich des Cookies mit den Anmeldeinformationen, der ICA-Dateien und der HTML-Anwendungslistenseiten sind gleichfalls sicher.

Für die Implementierung der SSL/TLS-Technologie im Netzwerk benötigt man SSL/TLS-fähige Webserver und SSL/TLS-fähige Webbrowser. Die Verwendung dieser Produkte ist für NFuse Classic transparent. Eine Konfiguration der Webserver oder Webbrowser für NFuse Classic ist nicht erforderlich. Weitere Informationen zur Konfiguration des Webservers für die Unterstützung von SSL/TLS finden Sie in der Webserverdokumentation.

TIPP

Viele SSL/TLS-fähige Webserver verwenden den TCP/IP-Anschluss 443 für die HTTP-Kommunikation. Standardmäßig verwendet das Citrix SSL-Relay diesen Anschluss ebenfalls. Sofern der Webserver zugleich ein MetaFrame-Server ist, auf dem das SSL-Relay ausgeführt wird, stellen Sie sicher, dass der Webserver oder das SSL-Relay einen anderen Anschluss verwenden.

PKI - Public Key Infrastructure

Mit den Windows-2000-Zertifikatsdiensten (Certificate Services) können eigene unternehmensweite Public Key Infrastruktures aufgebaut werden, die eine Verteilung und Verwaltung von Zertifikaten ermöglichen. Die Zertifikate lassen sich u.a. für Dateiverschlüsselung, E-Mail-Verschlüsselung und -Signierung, und Smart-Cards verwenden.

Passthrough-Authentifizierung

Die Passthrough-Authentifizierung sollte in einer sichereren Installation nicht aktiviert sein, um ein mögliches Weiterleiten der Anmeldeinformationen der Benutzer an einen nicht autorisierten oder gefälschten MetaFrame-Server zu verhindern. Das Aktivieren dieser Funktion sollte nur in einem kleinen, vertrauenswürdigen Umfeld erfolgen.

TIPP

Passthrough für Desktop-Anmeldeinformationen (Single-Sign-On) ist eine Internet-Explorer- und IIS-Funktion, mit deren Hilfe die Benutzer bei NFuse Classic anhand der Anmeldeinformationen authentifiziert werden können, welche während der Anmeldung beim Windows-Desktop eingegeben wurden. Verwendet man diese Funktion zusammen mit Passthrough-Authentifizierung (eine Funktion des ICA-Win 32-Clients), melden sich Benutzer nur einmal an und müssen sich beim Zugriff auf eine veröffentlichte Anwendung nicht nochmals anmelden. Passthrough für Desktop-Anmeldeinformationen über externen Zugriff ist nicht zu empfehlen.

Kommunikation zwischen NFuse-Classic-Server und MetaFrame-Server

Zur Kommunikation zwischen dem Webserver und dem MetaFrame-Server in einer NFuse-Classic-Bereitstellung gehört auch die Übergabe von Anmeldeinformationen der Benutzer und von Anwendungsgruppeninformationen zwischen den NFuse-Classic-Java-Objekten auf dem Webserver und dem Citrix XML-Dienst in der Serverfarm. In einer typischen NFuse-Classic-Sitzung übergeben die Java-Objekte für die Benutzerauthentifizierung Anmeldeinformationen an den XML-Dienst, und der XML-Dienst gibt Anwendungsgruppeninformationen aus. Zum Übergeben der Informationen verwenden Webserver und Serverfarm eine TCP/IP-Verbindung sowie das NFuse-XML-Protokoll.

Risiken

Das NFuse-XML-Protokoll verwendet Klartext für den Austausch aller Daten. Eine Ausnahme stellen Kennwörter dar, die mit einem Verschlüsselungsgrad „Basic“ übergeben werden. Die XML-Kommunikation kann folgenden Angriffen ausgesetzt sein:

- Ein Angreifer kann den XML-Verkehr abfangen und Anwendungsgruppeninformationen sowie Tickets an sich bringen. Ein Angreifer mit der Fähigkeit, den Verschlüsselungsgrad „Basic“ aufzulösen, kann außerdem Anmeldeinformationen erhalten.
- Ein Angreifer kann die Identität des MetaFrame-Servers annehmen und Authentifizierungsanfragen abfangen.

Empfehlungen

Das Implementieren dieser Sicherheitsmaßnahmen dient zum Sichern der XML-Datenübertragungen zwischen dem Webserver und der Serverfarm:

- Verwenden des Citrix SSL-Relays als Sicherheitsbarriere zwischen dem Webserver und der Serverfarm. Das Citrix SSL-Relay führt die Hostauthentifizierung und die Datenverschlüsselung aus.
- Verwenden des HTTPS-Protokoll für das Übermitteln von NFuse-Classic-Daten über eine sichere HTTP-Verbindung mit SSL.

Kommunikation zwischen ICA-Client und MetaFrame-Server

Bei der NFuse-Classic-Kommunikation zwischen Clientgeräten und MetaFrame-Servern werden verschiedene Typen von ICA-Sitzungsdaten übergeben, einschließlich Initialisierungsanfragen und ICA-Sitzungsinformationen.

- **Initialisierungsanfragen –** In der ersten Phase beim Herstellen einer ICA-Sitzung, die Initialisierung genannt wird, fordert der ICA-Client eine ICA-Sitzung an und erstellt eine Liste der Konfigurationsparameter für die ICA-Sitzung. Diese Parameter steuern zahlreiche Aspekte der ICA-Sitzung, u. a. welcher Benutzer angemeldet wird, die Größe des angezeigten Fensters und das in der Sitzung ausgeführte Programm.
- **ICA-Sitzungsinformationen –** Nach der Sitzungsinitialisierung übergibt der ICA-Client Tastatur- und Mauseingaben des Benutzers an den Meta Frame-Server, während der Benutzer zur ausgewählten Anwendung navigiert. Als Antwort sendet der MetaFrame-Server dem ICA-Client grafische Aktualisierungen.

Risiken

Um die Netzwerkkommunikation zwischen dem ICA-Client und dem MetaFrame-Server abzufangen und zu interpretieren, muss ein Angreifer dazu fähig sein, das binäre ICA-Protokoll zu entschlüsseln. Ein Angreifer, der das binäre ICA-Protokoll kennt, kann Folgendes tun:

- Abfangen der Informationen zu den Initialisierungsanforderungen, die vom ICA-Client gesendet werden, einschließlich der Anmeldeinformationen.
- Abfangen der ICA-Sitzungsinformationen, einschließlich vom Benutzer eingegebenen Text und Mausklicks sowie Bildschirmaktualisierungen, die vom MetaFrame-Server gesendet werden.

Empfehlungen

- Verwenden von SSL/TLS- oder ICA-Verschlüsselung.
- Verwenden von Citrix Secure Gateway.

Sicherheitsprotokolle und Citrix-Sicherheitskomponenten

Dieser Abschnitt enthält einführende Informationen zu den SSL- und TLS-Sicherheitsprotokollen sowie zu Citrix SSL-Relay und Citrix Secure Gateway nebst der ICA-Verschlüsselung. Außerdem sind Verweise zu weiteren Informationen zu Sicherheitsprotokollen und -lösungen enthalten, mit denen die Bereitstellung von Anwendungen über NFuse Classic gesichert werden kann.

Secure Sockets Layer (SSL)

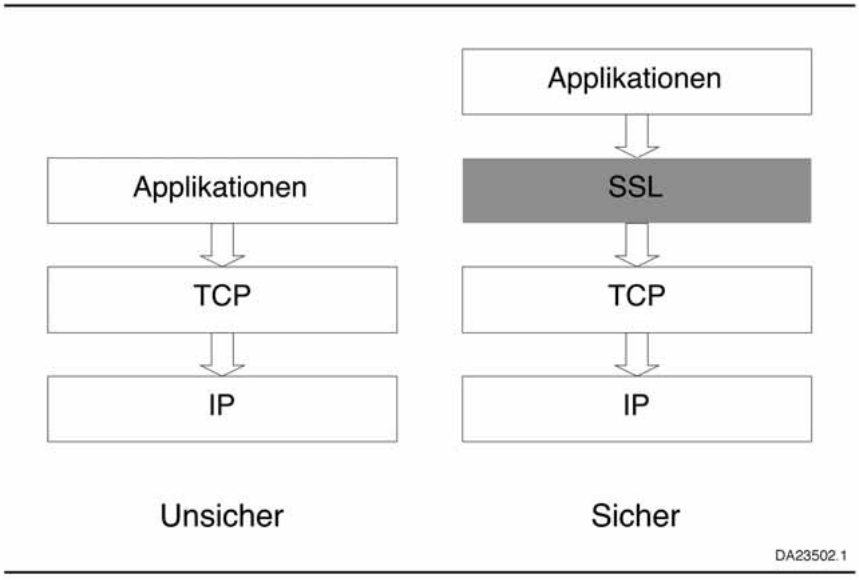
Was ist SSL? – Funktionsweise des Security-Standards

Das SSL(Secure Sockets Layer)-Protokoll sichert die Datenkommunikation in Netzwerken. SSL bietet Serverauthentifizierung, Verschlüsselung des Datenstroms und die Prüfung der Nachrichtenintegrität. SSL verschlüsselt dabei Nachrichten mit Kryptografie, authentifiziert die Identität und gewährleistet die Integrität der Inhalte. Dies schützt vor Abhören, falschem Weiterleiten und Datenmanipulation. SSL prüft die Identität mit Zertifikaten, die öffentliche Schlüssel enthalten und von Zertifizierungsstellen ausgegeben sind.

Einer der größten Vorteile von SSL ist seine Applikationsunabhängigkeit. Dadurch behandelt TCP SSL (TCP = Transport Control Protocol)einfach als eine Art „weitere Applikation“ und kann somit ohne Einschränkungen und vor allem ohne Aufwand eingesetzt werden. Ein Gegenbeispiel wäre hier IPsec, welches auf allen Maschinen die entsprechende Installation erfordert, und somit unflexibel ist.

Einen Algorithmus, welcher verschlüsselt und entschlüsselt, nennt man *Cipher*. Einen solchen Cipher-Algorithmus und dessen notwendigen Parameter zur Spezifizierung der genauen Verwendung (z.B. Größe der Schlüssel) nennt man *Ciphersuites*.

Jeder kryptographische Algorithmus wird auf „Session Basis“ verhandelt. So genannte „Session Identifiers“ werden zugewiesen, so dass bei abgebrochenen Verbindungen eine „Neuverhandlung“ auf Basis der im Cache gehaltenen Credentials stattfinden kann.



Eine solche Ciphersuite besteht in der Regel aus:

- Compression Algorithm
- Public Key Encryption Algorithm (z.B. RSA)
- Public Key Signing Algorithm (z.B. RSA)
- Shared Key Encryption Algorithm (z.B. 3DES Encrypt-Decrypt-Encrypt mit sog. Cipher Block Chaining)
- Message Authentication Algorithm (z.B. SHA-1)

Welche Ciphersuites gibt es?
Die Ciphersuites werden generell in zwei Kategorien unterteilt.

Kommerzielle Ciphersuites, die RC4 verwenden:

- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA

Behördliche Ciphersuites, erkennbar daran, dass DES (Data Encryption Standard) verwendet wird:

- SSL_RSA_WITH_3DES_EDE_CBC_SHA

Wie funktioniert der Aufbau einer SSL-Verbindung?
Die Aufnahme einer durch SSL geschützten Verbindung erfordert eine Vereinbarung über die zu verwendenden kryptographischen Verfahren und Parameter. Die Authentifizierung der beteiligten Kommunikationspartner wird durch das SSL-Handshake-Protokoll erreicht. Die Übertragung von Zertifikaten zur Identifizierung des Clients und des Servers ist optional.

Funktionsweise:

- SSL-Client schlägt ein Verfahren (kryptographische Funktion) vor
- SSL-Server bestätigt (mit optionalem Server-Zertifikat) und übersendet Public Key
- SSL-Client erzeugt geheimen Sitzungsschlüssel (und überprüft das Server-Zertifikat)
- SSL-Client übermittelt Sitzungsschlüssel mit Public Key
- SSL-Server entschlüsselt Sitzungsschlüssel

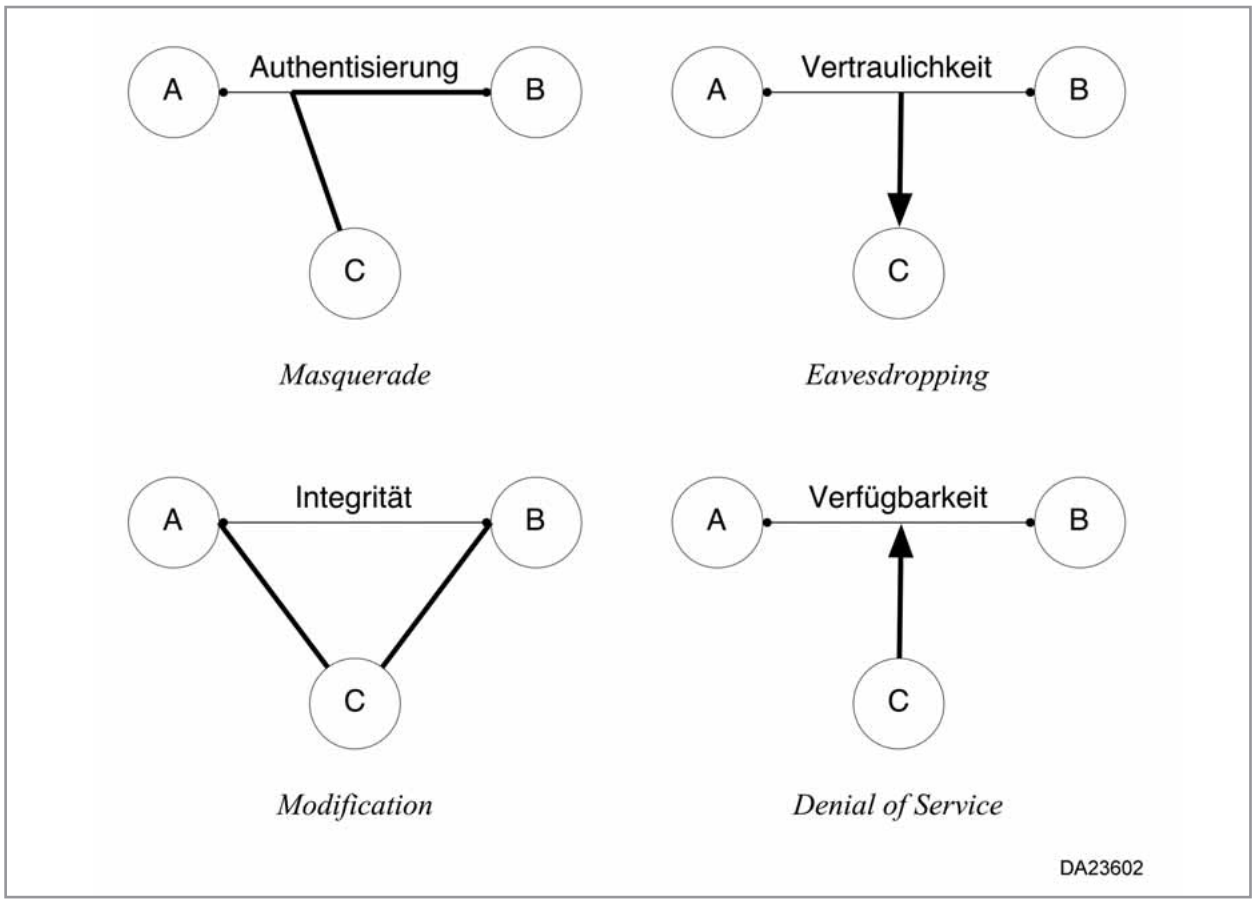
Welche Sicherheitsziele erreiche ich mit SSL?
Die Angriffe auf Institutionen und Computer nehmen immer mehr zu, je mehr das Internet als preisgünstiges Datentransportmittel von immer mehr Firmen und Privatleuten genutzt wird. Häufig werden die vielen Gefahren und Risiken, die das Internet birgt, unterschätzt. Die monetär bezifferbaren potentiellen Schäden durch Datenverlust oder „Lahmlegen“ von Ressourcen werden sträflich vernachlässigt. Denn gerade auf dem Weg der Daten von A nach B ist eine Kontrolle dessen, „WAS“ über das Netz geschickt wird, sehr schwierig und oft gar nicht mehr möglich.

Nüchtern betrachtet ist das Internet „ein riesig großes TCP/IP-Netzwerk“, in dem lediglich die angeschlossenen Rechner nicht überwacht bzw. beeinflusst werden können. Ebenso kann man sich kaum sicher sein, ob die, welche Zugriff auf meine Ressourcen haben möchten, tatsächlich stets jene sind, für die sie sich ausgeben.

Das heißt, ohne Vorkehrungen wie Verschlüsselung, Authentifizierung und Zugriffskontrollen ist das Internet lediglich das Medium, welches die Kommunikation grenzenlos und weltweit ermöglicht, mehr aber auch nicht.

Welche Arten der Bedrohung gibt es, und wie kann man sich schützen?

Generell kann man vier verschiedene Arten des Angriffs auf Systeme unterscheiden:



1. *a) Masquerading:*
   Unter einer „Masquerade" versteht man den Angriff gegen eine sichere Verbindung, bei der ein Angreifer versucht, die Identität eines der beiden Teilnehmer der Verbindung anzunehmen.

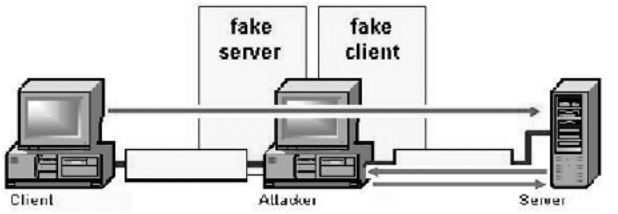
   b) Man-in-the-Middle-Attack:
   Auch hierunter versteht man den Angriff auf eine sichere Verbindung, bei welcher der Angreifer dem Client und Server dieser Verbindung jeweils vorgibt sein offizielles Gegenüber zu sein. Auf diese Weise kann der Angreifer Datenaustausch betreiben.

2. *Eavesdropping:*
   Darunter versteht man den Lauschangriff gegen eine sichere Verbindung, in welcher der Angreifer versucht, den Inhalt der Datenübermittlung abzuhören.

3. *Modification:*
   Unter einer „Veränderung" versteht man einen Angriff, bei dem gezielt versucht wird, die Daten zu verändern, während diese zwischen A und B ausgetauscht werden – also den Versuch, deren Integrität (Unversehrtheit) zu manipulieren. Diese Form der Attacke wurde in der Öffentlichkeit durch Manip-

ulationen bei Online Banking verschiedener Kreditinstitute bekannt. Um dies zu verhindern, haben Banken bei Online-Überweisungen beispielsweise die so genannten TAN (Transaktionsnummern) eingeführt.

4. *Denial of Service:*
   Dies ist wohl eine der häufigsten Angriffsvarianten: Durch gezielten „Beschuss" von Rechnern (häufig Webserver) mit Requests (Aufrufen) durch Angreifer, die getürkte IP-Adressen angeben, wird der anzugreifende Rechner lahm gelegt, weil dieser die Flut an Anforderungen nicht mehr verarbeiten kann, und den „Dienst verweigert".



SSL verhindert DNS-Angriffe

Durch die Verwendung von Zertifikaten bei SSL werden diese potentiellen Angriffsmethoden ausgeschlossen. Aufgrund dieser Zertifikate liegt nämlich das Hauptaugenmerk bei SSL nicht nur auf der Verschlüsselung, sondern auch darauf, die Authentifizierung absolut sicherzustellen. Durch das Hinterlegen von Serverzertifikaten auf den Servern und den Rootzertifikaten auf dem Client werden quasi „Schlüssel" hinterlegt, welche „Man-in-the-Middle"-Angriffe ausschließen. Hat ein Angreifer keinen passenden Schlüssel (Rootzertifikat) zum Serverzertifikat, wird dieser nicht vom DNS-Server authentifiziert, der Zugriff verweigert.

Funktionsweise von Zertifikaten

Wer nun beide Teilnehmer einer Verbindung identifizieren können will, bevor Daten verschlüsselt und übertragen werden, muss hierzu eindeutige Merkmale verwenden, nämlich Zertifikate. Ein Zertifikat ist eine digitale Information, welches ein Objekt und den Public Key eines solchen Objekts identifiziert und durch eine digitale Signatur einer autorisierten Stelle vergeben wurde.

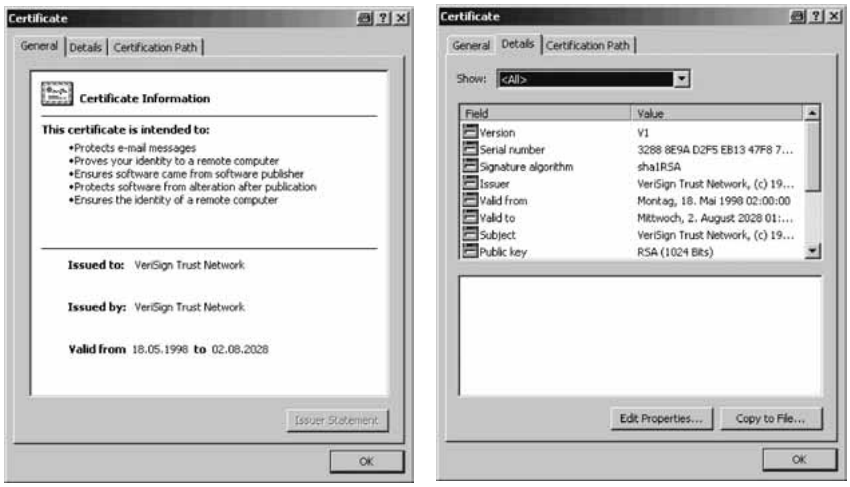
Eine solche autorisierte Vergabestelle nennt man Certificate Authority (CA). Dies ist eben jene Instanz oder Organisation, welche Zertifikate ausstellt und die Identität des Objekts belegt, auf welche die Zertifikate ausgestellt werden. Zertifikate werden meist für die Dauer eines Jahres ausgestellt, um dann erneut mit einer Neuausstellung zu überprüfen, ob sich Berechtigungen geändert haben.

Auch ein Führerschein ist z.B. ein Zertifikat, in dem Informationen über das Objekt, in diesem Falle dem Führerscheininhaber, vermerkt sind. Die Certificate Authority wäre in diesem Falle das Landratsamt, welches den Führerschein (das Zertifikat) ausstellt.

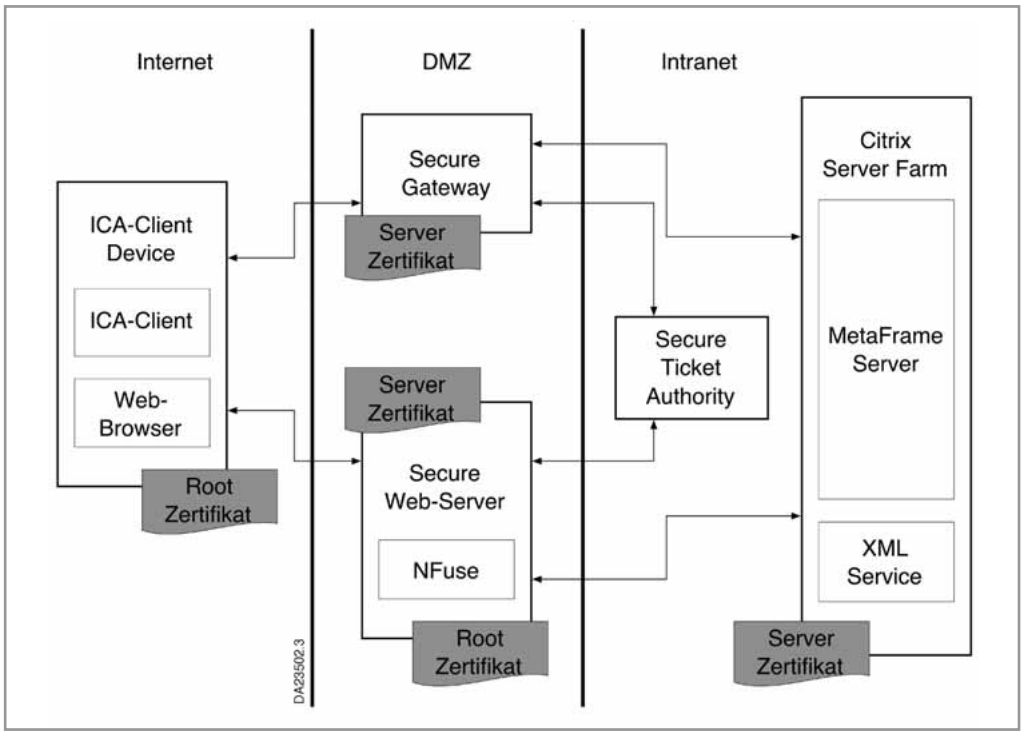
Das Ausstellen eines Zertifikats mittels einer Certificate Authority

DIE ROOT-ZERTIFIKATE

Rootzertifikate (oder CA Zertifikate) sind selbstsignierte Einheiten, welche zum Überprüfen von Serverzertifikaten verwendet werden. Wenn man einer CA vertraut, installiert man deren Rootzertifikat. Windows verfügt über viele vorinstallierte CA Zertifikate für bekannte CAs wie beispielsweise VeriSign, Entrust, Baltimore, RSA oder Thawte.



Beispiel einer Zertifikatsplatzierung



DIE SERVER-ZERTIFIKATE

Bei Einsatz des Citrix Secure Gateway Servers (CSG-Server) muss nur auf diesem ein einziges Serverzertifikat installiert werden, anstatt auf jedem MetaFrame-Server. Das Rootzertifikat wird über den SSL-fähigen ICA-Client ab der Version 6.20 ermöglicht.

Das Zertifikat muss auf den FQDN (Full Qualified Domain Name) des CSG-Servers ausgestellt werden.

HINWEIS

Informationen zur Installation bzw. Ausstellung von Zertifikaten sind im Citrix Secure Gateway Administrator Guide verfügbar.

Transport Layer Security (TLS)

TLS (Transport Layer Security) ist die neueste, standardisierte Version des SSL-Protokolls. Die Organisation IETF (Internet Engineering Taskforce) hat das Protokoll in TLS umbenannt, als diese die Verantwortung für die Entwicklung von SSL als offenen Standard übernahm. TLS bietet – wie SSL – Serverauthentifizierung, Verschlüsselung des Datenstroms und Prüfung der Nachrichtenintegrität.

Feature Release 2 von MetaFrame XP unterstützt TLS Version 1.0. Da zwischen SSL Version 3.0 und TLS Version 1.0 nur geringfügige technische Unterschiede bestehen, können die Serverzertifikate, die Sie für SSL auf MetaFrame-Servern verwenden, auch für TLS eingesetzt werden.

Einige Organisationen, u. a. die amerikanische Regierung und die Staatsbehörden, verlangen den Einsatz von TLS zur Sicherung der Datenkommunikation. Diese Organisationen fordern unter Umständen auch die Verwendung von verifizierter Kryptografie, wie z. B. FIPS140. FIPS (Federal Information Processing Standard) ist ein Standard für Kryptografie.

HINWEIS
NFuse Classic unterstützt eine maximale Länge des SSL- bzw. TLS-Zertifikatschlüssels von 2048 Bit.

Citrix SSL-Relay

Das Citrix SSL-Relay ist eine MetaFrame-Komponente, die SSL zum Sichern der Kommunikation zwischen NFuse Classic-Servern und Serverfarmen verwendet. Das SSL-Relay stellt Serverauthentifizierung, Datenverschlüsselung und Nachrichtenintegrität für eine TCP/IP-Verbindung zur Verfügung.

Das SSL-Relay fungiert als Sicherheitsbarriere bei der Kommunikation zwischen dem NFuse- Classic-Server und dem Citrix-XML-Dienst. Bei Verwendung des SSL-Relays überprüft der Webserver zuerst die Identität des SSL-Relays, indem das Serverzertifikat des Relays mit einer Liste der vertrauenswürdigen Zertifizierungsstellen verglichen wird.

Nach dieser Authentifizierung handeln der Webserver und das SSL-Relay eine Verschlüsselungsmethode für die Sitzung aus. Der Webserver sendet dann alle Informationsanfragen in verschlüsselter Form an das SSL-Relay.

Das SSL-Relay entschlüsselt die Anfragen und übergibt sie an den Citrix-XML-Dienst. Bei der Rückgabe der Informationen an den Webserver sendet der MetaFrame-Server alle Informationen über den SSL-Relay-Server, der die Daten verschlüsselt und dann seinerseits an den Webserver zur Entschlüsselung weiterleitet. Nachrichtenintegritätsprüfungen bestätigen, dass die Kommunikation nicht manipuliert wurde.

ICA-Verschlüsselung (Citrix SecureICA)

Mit der ICA-Verschlüsselung (Citrix SecureICA) lassen sich die zwischen einem MetaFrame-Server und einem ICA-Client übermittelten Informationen verschlüsseln. Unbefugten Benutzern ist es fast unmöglich, eine verschlüsselte Übertragung zu öffnen. Sollte dies jedoch gelingen, gewährleistet die ICA-Verschlüsselung, dass der Angreifer nur bedeutungslose Bildschirmbefehle, aber keinerlei vertrauliche Daten zu sehen bekommt.

ICA-Verschlüsselung bietet Datenschutz und schützt vor einem möglichen Abhören. Trotzdem bleiben noch einige Sicherheitsrisiken, so dass die Verwendung von Verschlüsselung nur ein Aspekt einer umfassenden Sicherheitsrichtlinie sein kann. Im Gegensatz zu SSL/TLS authentifiziert ICA-Verschlüsselung nicht den MetaFrame-Server. Somit könnten zumindest theoretisch Informationen im Netzwerk abgefangen und an einen gefälschten Server weitergeleitet werden. Auch wird durch ICA-Verschlüsselung nicht die Integrität überprüft.

Citrix Secure Gateway (CSG)

Citrix Secure Gateway – Grundlagen
Citrix Secure Gateway stellt zusammen mit NFuse Classic einen zentralen, sicheren und verschlüsselten Zugangspunkt über das Internet auf MetaFrame-Server in internen Unternehmensnetzwerken bereit.

Citrix Secure Gateway ist ein sicheres Internet-Gateway zwischen SSL/TLS-fähigen ICA-Clients und MetaFrame-XP-Servern. Die ICA-Datenübertragungen via Internet zwischen Clientgeräten und Citrix-Secure-Gateway-Server werden per SSL/TLS verschlüsselt. Dies ermöglicht dem Benutzer, ohne Gefährdung der Sicherheit von außerhalb des lokalen EDV-Netzes auf Unternehmensinformationen zuzugreifen. Citrix Secure Gateway vereinfacht auch die Zertifikatverwaltung, da nur auf dem Secure-Gateway-Server ein Serverzertifikat installiert wird und nicht auf jedem MetaFrame-Server in der Serverfarm.



Citrix Secure Gateway – Voraussetzungen
Die Citrix-Secure-Gateway-Lösung setzt sich aus drei Komponenten zusammen. In der Windows-Variante müssen diese drei Instanzen auf der Basis von Windows 2000 Server mit SP2 installiert sein.

Zusätzlich muss beim CSG Gateway Server neben der eigentlichen CSG-Installationskomponente das Serverzertifikat installiert werden. Bei der Secure Ticket Authority (STA) ist neben der CSG-Komponente lediglich noch der Internet Information Server (IIS) erforderlich und beim NFuse Webserver ebenfalls nur der IIS.

HINWEIS
Die sog. NFuse CSG Extensions sind nur bei NFuse unterhalb der Version 1.7 erforderlich. Ab dieser Version ist die CSG-Komponente in NFuse bereits integriert und muss lediglich noch konfiguriert werden.

Citrix Secure Gateway ist ein sicheres Internet-Gateway zwischen ICA-Client und dem CSG Gateway Server. Unterstützt werden ICA-Clients ab Version 6.20 unter Win32, JAVA, MAC oder Linux.

Citrix Secure Gateway – die Architektur
Grundvoraussetzung ist die Tatsache, dass CSG im sog. Gateway-Modus operiert, d.h. in jedem Fall muss eine DMZ (Demilitarisierte Zone) vorhanden sein.

Neben verschiedenen Anordnungsvarianten ist die meistinstallierte wohl jene, in welcher der Gateway-Server sowie der NFuse-WebServer in der DMZ stehen und die STA im Corporate Network liegt.

Zur bekannten Funktionsweise von NFuse fügt sich die Citrix-Secure-Gateway-Technologie folgendermaßen:

Nach der Authentifizierung des Users per NFuse wird beim unmittelbaren Anklicken des publizierten Icons die Datei launch.ica erstellt. CSG entnimmt hier nun den Eintrag der (von NFuse erstellten) IP-Adresse der verfügbaren MetaFrame Resource (nach Load-Balancing-Kriterien) und ersetzt diese durch ein Ticket, welches dann an den ICA-Web-Client heruntergeladen wird. Sowohl der Vermerk für das Ticket als auch die Information der IP-Adresse werden zur STA übermittelt. Die Secure Ticket Authority fungiert also als eine Art „Information Cache“, auf dem eben jene MetaFrame-Server-Ressourcen abgelegt werden.

Durch diesen Vorgang wird verhindert, dass die IP-Adressen an den Client transferiert werden müssen, sondern sie verbleiben im Firmennetz – wodurch eine potenzielle Sicherheitslücke für Angreifer geschlossen wird. Dies ist durchaus als eine Art Ersatz für NAT (Network Address Translation) in diesem Zusammenhang zu sehen.

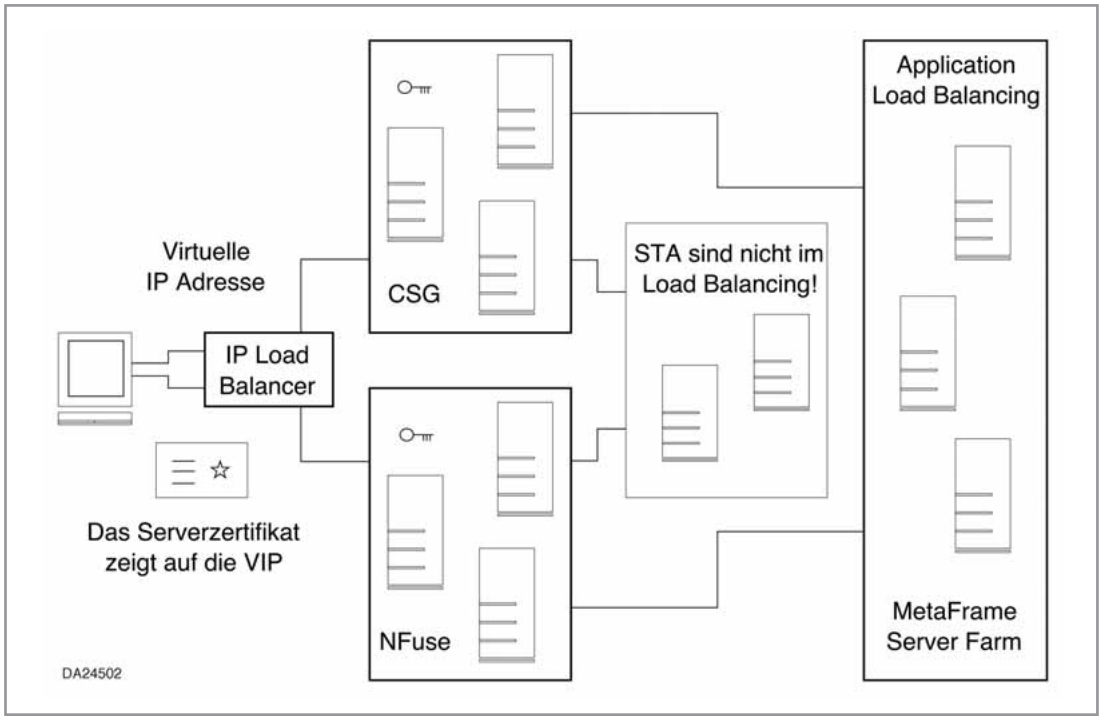
Nach dem Download der erforderlichen Parameter an den ICA-Web-Client wird nun der Sitzungsaufbau zunächst zum Secure Gateway Server per DNS und den Zertifikaten aufgebaut.

Der Gateway-Server überprüft nun das von NFuse zuvor ausgestellte Ticket mit dem entsprechenden Vermerk dazu auf der STA. Ist die Überprüfung positiv, wird der Zugriff auf die MetaFrame Server zugelassen. Kann zu dem Ticket kein passender Vermerk mit zugehöriger IP-Adresse auf dem STA-Server gefunden werden, wird dem Anwender der Zugriff verweigert.

Citrix Secure Gateway – Skalierbarkeit und Redundanz

Um den Zugriff via Internet und CSG auf die MetaFrame-Umgebung nicht zu einem „Single Point of failure“ zu machen, stellt sich unweigerlich die Frage, wie die drei Serverinstanzen abgesichert werden können.

Die Redundanzschaffung der NFuse WebServer auf die gleiche Art und Weise ist keine Funktion, welche das Secure Gateway mitbringt, sondern eine Funktionalität (Columbia), welche NFuse schon seit der Version 1.5 als zusätzlich installierbare Funktion zur Verfügung stellt, und ab NFuse 1.6 ein integraler Bestandteil der Software ist.



Beim Gateway Server selbst und auch beim NFuse Server bedient man sich einfach der bewährten Network-LoadBalancing(NLB)-Methodik, welche Microsoft ab der Windows 2000 Advanced Server Version zur Verfügung stellt.

Auf Basis dessen und durch Einrichten eines sog. „CSG Arrays“ ist man in der Lage, den Ausfall eines oder mehrerer Server zu kompensieren. In diesem Fall ist pro Gateway Server ein Serverzertifikat erforderlich.

Auch hier dient das NLB nicht zur Lastenverteilung, sondern für den Fall des Ausfalls eines der Webserver.

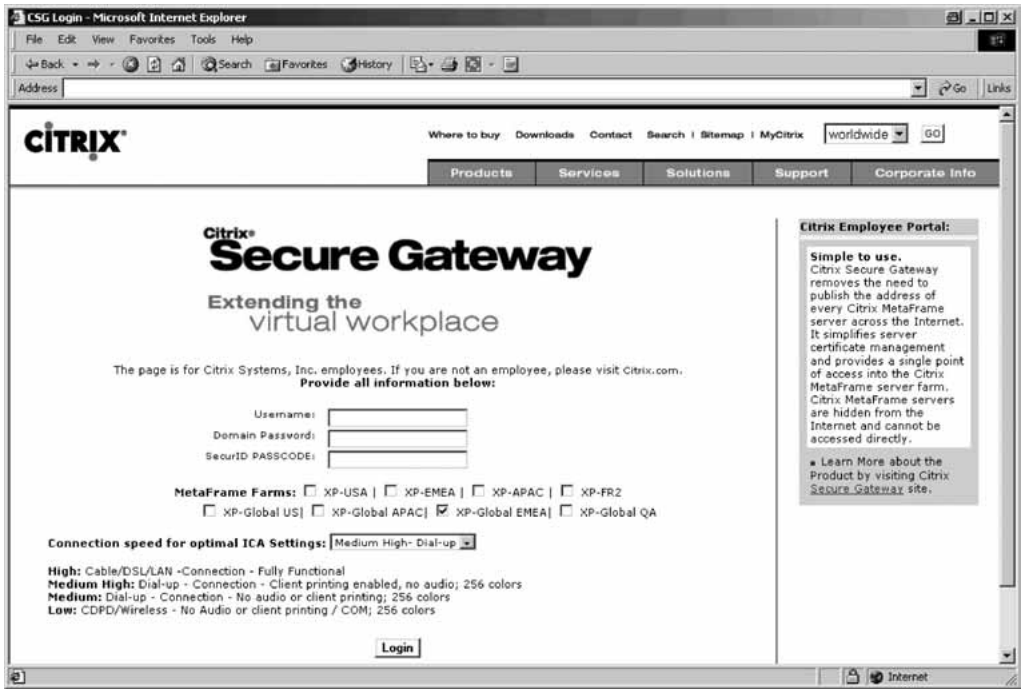
Ganz anders verhält sich die Situation bei der Secure Ticket Authority. Da aus technischen Gründen im Gegensatz zu Gateway Server und NFuse Webserver nur eine einzige Instanz vorhanden sein darf, kann diese Instanz der CSG-Lösung mit bewährten Methoden wie Aufnahme dieses Servers in ein Cluster oder Einbindung ist eine Backup-Strategie in Form eines kompletten Server-Backups erfolgen.

HINWEIS
Ein tägliches Backup der STA ist nicht notwendig, da im Gegensatz zu beispielsweise Datenbankservern kein „letzter aktueller Status“ zur Verfügung stehen muss, da nach Aufbau der ICA-Sitzung über den Gateway Server das Ticket auf der STA entfernt wird. Theoretisch würde auch ein Image für diesen Server ausreichen, wird aber nicht empfohlen.

Citrix Secure Gateway-Authentifizierung und RSA-Integration

Um noch höhere Sicherheitsansprüche bei der Authentifizierung zu erfüllen, bietet Citrix (siehe Schaubild CSG Architektur) eine Form der Integration für sog. „harte Authentifizierung“ mittels der SecurID-Lösungen von RSA.

NFuse bzw. MetaFrame benötigen die Logon Creditials des User Accounts aus dem entsprechenden Betriebssystem, um für den Anwender das Application Set zu erstellen. Außerdem ist ein zweiter, paralleler Login für RSA SecurID notwendig. Um nun den Anwender nicht dazu zu zwingen, sich zweimal hintereinander anzumelden, stellt die RSA- Integration für CSG sicher, dass sich die Authentifizierung für der Anwender durch Eingabe von Domänen-Benutzername, Domänenpasswort sowie seinem SecurID-Token wie ein einziger Loginprozess darstellt. Technisch werden trotzdem zwei getrennte Authentifizierungsversuche ausgeführt, für der Benutzer spielt es sich dennoch als ein einziger Login ab.



Sicherheitskonzeption

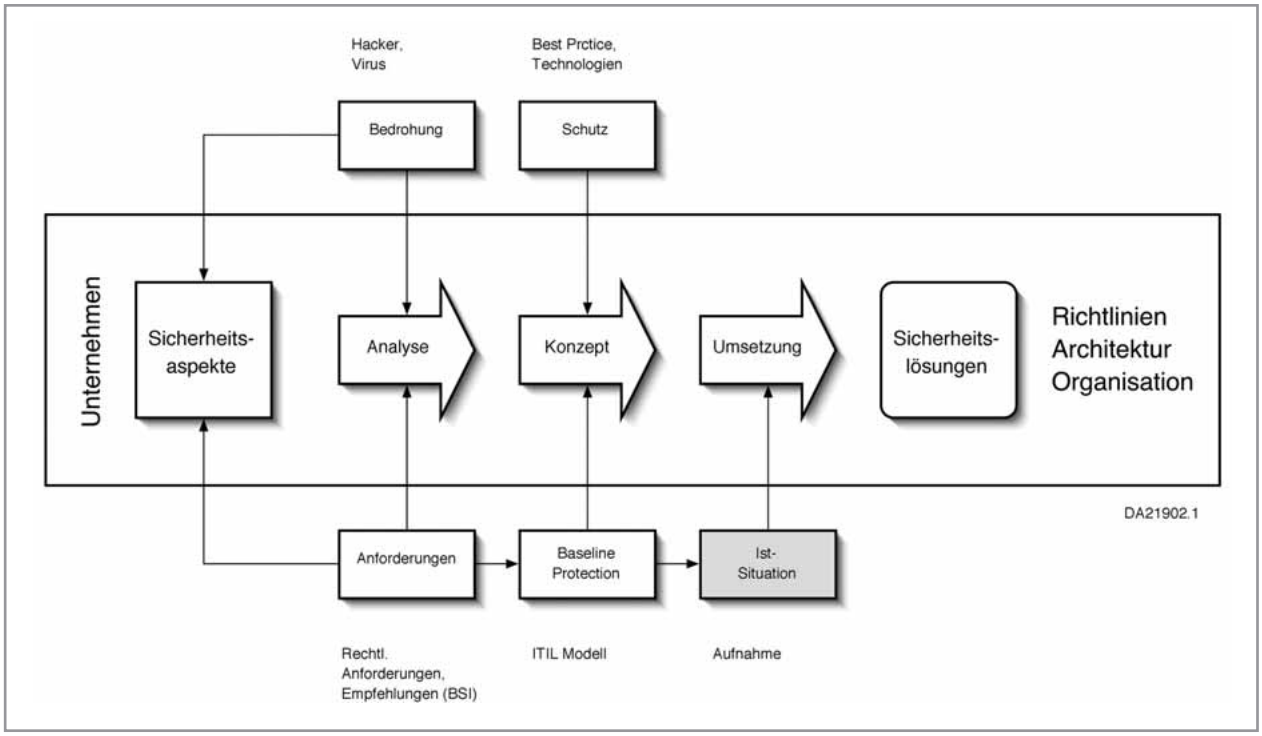
Das ganzheitliche IT-Sicherheitskonzept eines Unternehmens besteht aus den Vorgaben für die IT-Sicherheit (Sicherheitspolitik) sowie den technischen und organisatorischen Richtlinien. Die IT-Sicherheitsorganisation legt die Verantwortlichkeiten für die Maßnahmen innerhalb der technischen Sicherheitsarchitektur fest.

- Festlegung der Internet-Sicherheitsrichtlinien
- Beschreibung organisatorischer Maßnahmen
- Beschreibung technischer Maßnahmen

Der Sicherheitsprozess beginnt mit dem Erstellen firmeninterner Sicherheitsleitlinien und ist Grundlage für den Aufbau des Sicherheitskonzeptes. Planung und Umsetzung sowie Wartung und Revision von Sicherheitsmaßnahmen sind ständige Prozesse zur Sicherstellung der IT-Sicherheit.

Systematisches Vorgehen unterstützt beim Aufbau einer adäquaten IT-Sicherheit. Die wichtigsten Gesichtspunkte:

- Motivation potenzieller Angreifer und Zielsetzung der Sicherheitsvorkehrungen
- Planung
- Analyse und Bewertung
- Umsetzung
- Prüfen und Überwachen
- Reaktion und Anpassungen
- Aktualisierung



Der hier skizzierte Ablauf soll beispielhaft die Vorgehensweise bei einem Sicherheits-Vorhaben veranschaulichen:

- **Ermittlung des Sicherheitsbedarfs**
  Der erste Schritt in Richtung Sicherheit beginnt mit der Analyse. Es gilt die Netzwerkstrukturen und Systeme zu durchleuchten sowie die organisatorischen Rahmenbedingungen festzulegen. Damit werden der Sicherheitsbedarf ermittelt und die Anforderungen an die geplante Lösung festgelegt.

- **Planung und Anpassungen**
  Ausgehend von der Ermittlung des Sicherheitsbedarfs wird ein Sicherheitskonzept erstellt. Die Planung umfasst die Integration der Komponenten und die Definition der notwendigen Netzwerkobjekte, Nutzergruppen und Dienste. Diese werden zu Regelsätzen verknüpft, die den festgelegten Sicherheitsbedarf abbilden.

- **Konfiguration und Test**
  Auf den ausgewählten Systemen erfolgt nun die abgesicherte Überprüfung der Betriebssysteme sowie der Firewall-Software und weiterer Komponenten. Diese werden gemäß der Planung konfiguriert und getestet.

- **Wartung und Kontrolle**
  Um ein gleichbleibend hohes Maß an Sicherheit und so dauerhaften Schutz zu gewährleisten, muss die Sicherheit kontinuierlich überwacht, gepflegt und angepasst werden.

Schritt 1: Planung

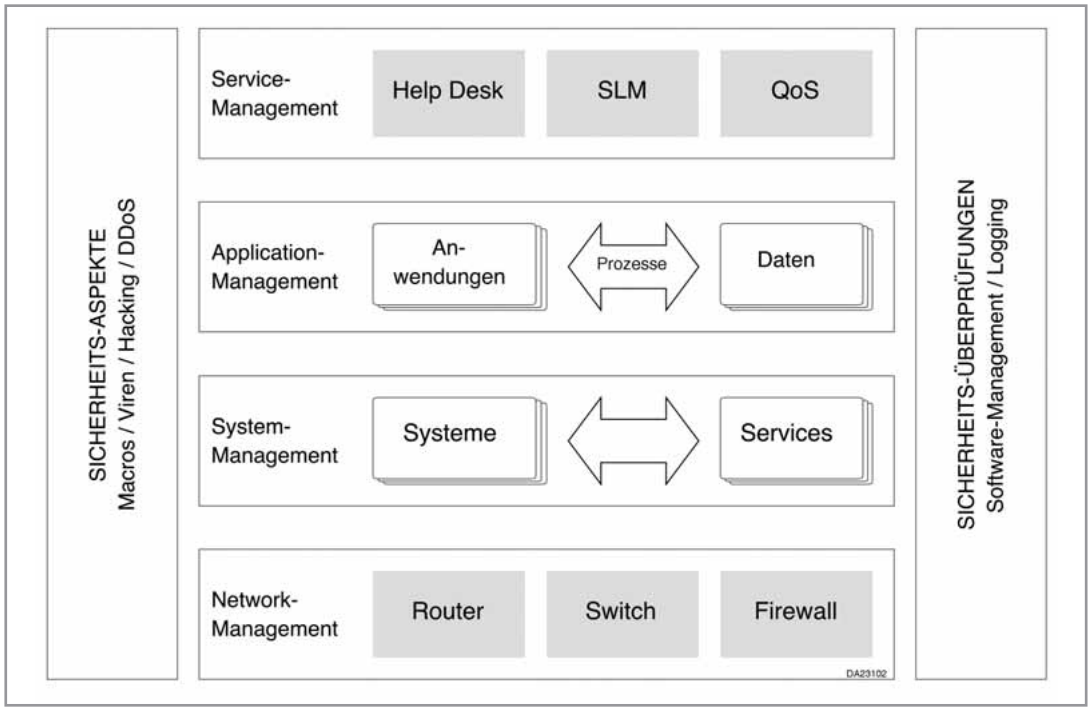
Sicherheitsstrategien, IT-Services und Security-Lösungen

Der Grundschutz stützt sich auf ein angemessenes Sicherheitsniveau (Baseline Protection) mit anerkannten Industriestandards, die aus bewährten Vorgehensweisen in der Praxis hervorgehen (Best Practices).

Proaktives Vorgehen oder: „Act – don't react!"
Ein proaktives Management der IT-Security und Services ist vorrangiger, anstatt nur auf Probleme der IT-Infrastruktur zu reagieren. Hieraus stellen sich die folgenden Fragen:

- Was sind für die Geschäftstätigkeit wichtigsten IT-Services?
- Steht die geeignete Kombination von Mitarbeitern, Prozessen und Technologien für die IT-Sicherheit zur Verfügung?
- Welche IT-Infrastruktur muss bereitgestellt werden, um die benötigten Sicherheitsstrategien und Dienste bereitzustellen?

Um Geschäftsprozesse reibungslos ablaufen zu lassen, sind genaue Kenntnisse über die IT-Infrastruktur und Business-Prozesse nötig. Genauso wichtig ist es, über alle Unternehmensbereiche hinweg Art und Qualität der Sicherheits-Services genau zu definieren, die den Endanwendern bereitgestellt werden.



Modelle

IT-Grundschutzhandbuch des BSI
Das IT-Grundschutzhandbuch des BSI (Bundesamt für Sicherheit in der Informationstechnik) beschreibt detailliert die Standard-Sicherheitsmaßnahmen, die praktisch für jedes IT-System zu beachten sind. Es umfasst:

- Standardsicherheitsmaßnahmen für typische IT-Systeme mit „normalem" Schutzbedarf,
- eine Darstellung der pauschal angenommenen Gefährdungslage,
- ausführliche Maßnahmenbeschreibungen als Umsetzungshilfe,
- eine Beschreibung des Prozesses zum Erreichen und Aufrechterhalten eines angemessenen IT-Sicherheitsniveaus und
- eine einfache Verfahrensweise zur Ermittlung des erreichten IT-Sicherheitsniveaus in Form eines Soll-Ist-Vergleichs.

http://www.bsi.de/literat/faltbl/itgrund.htm

ISO/IEC 17799 (BS 7799-1)
Die ISO/IEC 17799 (BS 7799-1) ist ein international anerkannter Leitfaden für das Management der Informationssicherheit. Eine umfassende Sammlung optimaler Verfahren („Best Practices") der Informationssicherheit, die für Unternehmen unterschiedlichster Größe geeignet sind, stellt eine Basis zur Entwicklung organisationsbezogener Sicherheitsnormen und effektiver Managementpraktiken dar.

http://www.iso17799software.com

BS (British Standard) 7799-2
Der BS (British Standard) 7799-2 (Code of Practise for Information Security Management) ist eine Spezifikation für ein Informationssicherheits-Managementsystem (ISMS). Die einzelnen Anforderungen zur Definition, Implementierung und Dokumentation bieten eine Grundlage für die Bewertung des Systems.

http://www.dti.gov.uk/cii/datasecurity/bs_7799.shtml

Common Body of Knowledge (CBK) General Model
Das Common Body of Knowledge (CBK) General Model von International Systems Security Certification Consortium (ISC) stellt die Elemente und die Zusammenhänge eines IT-Riskmanagements dar.

http://www.isc2.org

IT Infrastructur Library (ITIL)
Die IT Infrastructur Library (ITIL) der Central Computer and Telecommunications Agency (CCTA) stellt eine Sammlung von Best Practice Guides von prozessorientierten und plattformunabhängigen Richtlinien über IT-Sicherheit dar.

http://www.itil-itsm-world.com
http://www.itil.co.uk
http://www.ccta.gov.uk
http://www.ogc.gov.uk

Microsoft Operations Framwork (MOF)
Das Microsoft Operations Framework (MOF) bietet jene technische Unterstützung, die es Unternehmen ermöglicht, Zuverlässigkeit, Verfügbarkeit, Sicherheit, Supportfähigkeit und Verwaltbarkeit von Microsoft-Produkten und Technologien für unternehmenswichtige Systeme zu erreichen. MOF umfasst eine Sammlung von Unterstützungsmöglichkeiten für den Betrieb von IT-Systemen. Microsoft stellt detaillierte Handbücher für den Betrieb von Microsoft Windows 2000 zur Verfügung. Diese basieren auf den Kernprozess im MOF-Prozessmodell. Die Betriebshandbücher dienen zur Bewertung, Identifikation und Entwicklung der Qualität der Betriebsleistung.

Die Windows-2000-Betriebshandbücher sind zum Teil deutschsprachig verfügbar:

- Windows Operations Guide Series Introduction
- Availability Management Operations Guide
- Capacity Management Operations Guide
- Change Management Operations Guide
- Configuration Management Operations Guide
- Directory Services Administration Operations Guide
- Financial Management Operations
- Guide Incident Management Operations Guide
- Network Administration Operations Guide
- Problem Management Operations Guide
- Release Management Operations
- Guide Security Administration Operations Guide
- Service Continuity Management Operations Guide
- Service Level Management Operations Guide
- Service Monitoring and Control Operations Guide
- Service Desk Operations Guide
- Storage Management Operations Guide
- System Administration Operations Guide
- Workforce Management Operations Guide

Die Inhalte beruhen einerseits auf Empfehlungen der Information Technology Infrastructure Library (ITIL) der Central Computer and Telecommunications Agency (CCTA), andererseits auf den Erfahrungen verschiedener Hersteller, der Microsoft Consulting Services (MCS) und der Microsoft Information Technology Group (ITG).

http://www.microsoft.com/germany/mof

Schritt 2: Analyse

Sicherheit ist das Ergebnis der Optimierung vieler Faktoren, die miteinander in Wechselwirkung stehen:

- Mensch (Verhalten, Wissen)
- Prozesse (Richtlinien, Handbücher)
- Technologien und Produkte (Hard- und Software, Netzwerke)

Sicherheitsfaktoren

Mensch

Ein nicht zu unterschätzendes Risiko liegt darin, dass eigene Mitarbeiter unwissentliche oder gar gewollt betriebliche und technische Sicherheitsvorschriften missachten. Deshalb muss man die Anwender (Benutzer und Administratoren) eines IT-Systems regelmäßig durch Ausbildung, Weiterbildung und Schulung darin fördern, sich sicherheitsadäquat zu verhalten. Auf diese Weise wird unbefugten Personen der Zugriff auf Systeme erschwert und durch eine allgemeine Gebäudesicherheit die physikalische Systemsicherheit gewährleistet. Hierzu stellen die unternehmerischen Sicherheitsrichtlinien entsprechende Verfahrens- und Arbeitsanweisungen bereit und unterstützten eine verantwortungsvolle Einstellung zum Thema IT-Sicherheit. Dieses Sicherheitsbewusstsein dient dem Schutz unternehmerischer Daten und Systemen.

Prozesse

Angreifer nutzen Lücken in IT-Systemen, um an Informationen und Daten zu gelangen. Deshalb sollten alle Systeme regelmäßig nach dem aktuellen Stand der Technik und gemäß dem verfügbaren Wissen über Schwachstellen überprüft werden. Die regelmäßige Implementierung aktueller Hotfixes, Service Packs und Updates der Virus Patterns wird durch eine sinnvoll geregelte, konsequente Wartung der Systeme gewährleistet.

TIPP

Die Implementierung von Hotfixes, Service Packs, Virus-Updates sowie sonstige Änderungen und Anpassungen sollten erst nach einem eingehenden Kompatibilitätstest (in einer Testumgebung) erfolgen.

Angriffe sollte man möglichst unmittelbar bzw. möglichst rasch erkennen können. Die Kenntnis von Zwischenfällen, vorzugsweise in Echtzeit, oder die regelmäßige Auswertung von Aufzeichnungen (Logdateien) ermöglicht fundierten Einblick in die Art der Bedrohung und in die Vorgehensweise der Angreifer.

Alle IT-Abläufe müssen regelmäßig getestet oder verbessert werden. Dies gilt vor allem für besonders selten genutzte Prozesse wie Restore von Daten und das Wiederaufsetzen von Systemen für den Notfall. Für die möglichen Ernstfälle sind Notfallpläne und Checklisten dringend erforderlich – diese verhelfen zu einer geordneten Ausführung der Aufgaben.

Die Überwachung der Sicherheitsrichtlinien erfolgt durch organisatorische Maßnahmen und technische Einrichtungen.

Technologien

Die Sicherheitstechnologien dienen dem Schutz von Daten, Informationen, Systemen und Netzwerken. Die Richtlinien des Sicherheitskonzeptes bestimmen die Verhaltensweise der Komponenten, die Schwachstellen und Angriffe erkennen. Ein effektiver Schutz muss alle Ebenen einer IT-Infrastruktur umfassen und dient der Verteidigung (Defense), somit zum Schutz vor Bedrohungen.

- **Die richtige Technologie für jede Ebene –** um eine tief gestaffelte Abwehr zu errichten, also ein effektives Defense in Depth zu realisieren, gilt es, auf den verschiedenen Ebenen eines IT-Systems die richtigen Technologien und Maßnahmen für die Sicherheitsanforderungen zu implementieren.

Aspekte der Sicherheitsanforderungen:

- **Daten –** Restriktive Bedingungen beim Zugriff auf Daten und zentrale (ggf. verschlüsselte) Datenhaltung
- **Anwendungen –** Personalisierte Funktionen und Sicherheitseinstellungen
- **Systeme –** Systemsicherheit und -schutz sowie Verfügbarkeit
- **Netzwerk –** Sichere Anmeldeverfahren und Verschlüsselung von Daten
- **Internet –** Einrichten und Überwachen von Firewalls
- **Physikalische Sicherheit –** Absicherung der kommunikativen Zugänge zu Informationssystemen
- **Richtlinien und Prozeduren –** Technische sowie organisatorische Maßnahmen und Vorgehensweisen

<table>
<tr><td rowspan="4">Physikalische Sicherheit</td><td colspan="2">Internet</td><td rowspan="4">Richtlinien und Prozeduren</td></tr>
<tr><td colspan="2">Netzwerk</td></tr>
<tr><td colspan="2">Host/Client-Systeme</td></tr>
<tr><td>Daten</td><td>Anwendungen</td></tr>
</table>

DATEN UND ANWENDUNGEN

Bei *Microsoft Office*-Anwendungen kann man die Sicherheitsstufen zur Ausführung von Makros benutzerseitig einstellen. Auf der niedrigsten Sicherheitsstufe werden Makros ohne Nachfrage aktiviert und ausgeführt – diese Einstellung ist jedoch nicht zu empfehlen. Auf der mittleren Sicherheitsstufe wird zwar um Zustimmung nachgefragt, die vom Anwender meistens einfach erteilt wird. In der höchsten Sicherheitseinstellung werden Makros nur aktiviert und ausgeführt, wenn diese von einer vertrauenswürdigen Stelle signiert wurden. Diese Einstellung hat den besten Sicherheitseffekt.

http://www.microsoft.com/office/ork/xp/appndx/appc00.htmshtml

Der *Internet Explorer* ermöglicht die Steuerung der Sicherheit in Abhängigkeit der ausgewählten Zone. In den Internet-Explorer-Einstellungen lassen sich die Einstellungen für Web-Zonen und Optionen zur Handhabung von Cookies individuell anpassen.

Um sich gegen die meisten Viren zu schützen, die per E-Mail-Anhängen verbreitet werden, ist es wichtig, Sicherheitserweiterung in die E-Mail-Programme einzubauen oder die E-Mail- Server abzusichern.

UMFASSENDER VIRENSCHUTZ

Viren, Trojaner und Würmer zerstören Software und Daten, spionieren Passworte aus oder versenden Informationen an Unbefugte.

Die größte Infektionsgefahr geht heutzutage vom Internet aus. Daher müssen alle Internet-Verbindungen direkt und tagesaktuell auf schädliche Inhalte hin untersucht werden. Ein ernst genommener Virenschutz darf weder veraltete Virensignaturen verwenden oder nur lokal auf einigen Systemen erfolgen. Außerdem finden Viren auch über Disketten, CDs, selbsterstellte Medien oder dezentrale Datenverbindungen (z.B. für Online-Banking) direkten Zugang in die einzelnen PCs und damit in das Unternehmensnetz.

Um ein gleichbleibend hohes Maß an Sicherheit zu gewährleisten, muss man die Virenschutz-Prozesse selbst kontinuierlich überwachen, pflegen und anpassen. Nur automatische Prozesse gewähren eine ständig aktualisierte und verlässliche Verteilung auf alle Virenschutz-Systeme in Netz.

http://www.microsoft.com/germany/ms/windowsxp/security/viren.htm

Wer Angriffe und Ausfälle nicht erkennt und nicht oder falsch reagiert, ist schutzlos den Viren ausgesetzt, die sich dann rasant im ganzen Unternehmen verbreiten.

SERVER-SYSTEME

Bereits die Anmeldung beim Netzwerk des Unternehmens erfordert Sicherheitsvorkehrungen. Windows 2000 nutzt mit Kerberos ein standardisiertes und sehr sicheres Verfahren, um Manipulationen bei der Anmeldung auszuschließen. Die integrierte Verschlüsselung aller Datenübertragungen erfolgt hierbei mit einem im IPsec-Standard spezifizierten Verfahren.

Das Encrypted File System (EFS) in Windows 2000 ist ein wichtiges Sicherheitsmerkmal, um eine automatische Verschlüsselung einzelner Dateien und ganzer Ordner durchzuführen, die auf der Festplatte von Arbeitsplätzen oder Servern gespeichert sind.

http://www.microsoft.com/germany/ms/windows2000/magazin/artikel71.htm

Windows 2000 verwendet zur Authentifizierung öffentliche Schlüssel, so dass keine Kennwörter übertragen werden müssen. Mit dem Einsatz so genannter Smart Cards, also Chipkarten im Scheckkartenformat, lassen sich Schlüssel, Zertifikate und andere benutzerspezifische Daten speichern.

HUBS, SWITCH UND ROUTER

Der autorisierte Zugriff für die Verwaltung eines Routers oder Switches erfolgt mit (meist vordefinierten) Zugangskennungen. Die erste Konfiguration wird über den Terminal- bzw. Konsolen-Anschluss (RS232), oder einen dedizierten Ethernet-Port vorgenommen, und zwar anhand von Standardkennungen. Die weiteren Einstellungen sowie die Verwaltung werden dann durch herstellereigene Tools, eine Telnet-Sitzung, einen Browser Based Interface (BBI) oder das Simple Network Management Protocol (SNMP) über das Netzwerk durchgeführt. Zur Vermeidung unberechtigten Zugriffs können Administrationsrechte mit verschiedenen Berechtigungsstufen (nur Leserechte, partielle oder uneingeschränkte Schreib-/Leserechte) festgesetzt werden.

Sicherheitslücken bestehen auch in Form von undokumentierten Default-Logins. Neben bekannten Standard-Accounts „admin“, „read“ und „write“, existieren ggf. weitere Default-User, die mit einem standardmäßigen Passwort für einen erfolgreichen Login sorgen. Solche potentiellen Sicherheitslücken müssen nicht sein. Ein Debug-Account besitzt neben den kompletten Administrator-Rechten noch zusätzliche Debug-Kommandos, die von keinem anderen Account angesteuert werden können. Wurde die Remote-Administration über Telnet zugelassen, so können mit diesem Debug-Account die Passwörter aller anderen Benutzer modifiziert werden, ohne Kenntnis über die alten Passwörter zu besitzen. Somit kann ein Angreifer den rechtmäßigen Administrator komplett aus dem Gerät verbannen.

Folglich empfiehlt es sich dringend, die Passwörter der Default-Logins bestmöglich zu modifizieren. Diese Benutzerkennungen sollte man nach der Erstkonfiguration ändern und somit nur den verantwortlichen Administratoren das jeweilige Passwort bekannt sein.

Auch das Netzwerkmanagementprotokoll SNMP hat einige Sicherheitslücken. Um einen Schutz vor Teardrop- oder ICMP-Attacken zu gewährleisten sollte SNMP nur Inbound verwendet werden. Eine tiefergehende Prüfung durch die Oulu University Secure Programming Group (OUSPG) in Finnland stellte zahlreiche mögliche Verletzlichkeiten in der Implementierung des Protokolls SNMPv1 fest. Entsprechend hat die CERT im Februar 2002 über die Verwundbarkeit in vielen Implementierungen des Simple Network Management Protocol [CERT Advisory CA-2002-03] berichtet.

Das **CERT Coordination Center** stellt verschiedene Security Practices & Evaluations zum Thema Sicherheit (Secure Infrastructure Design, Securing an Internet Name Server, Creating a Computer Security Incident Response Team: A Process for Getting Started) sowie eine Vulnerability Notes Datenbank und Quick Fixes bereit.

http://www.cert.org
http://www.kb.cert.org/vuls

Ein gesicherter Zugriff auf Netzwerkkomponenten bedeutet, dass die Zugangs- und Nutzdaten so übertragen werden, dass diese nicht mitgelesen oder manipuliert werden können. Zur Konfiguration von Standardfunktionen wird heutzutage meist eine Browser-basierte Anwendung verwendet. Mit Einsatz von HTTPS, mittels SSL über Port 443, erfolgt die Übertragung der Informationen von und zu einem Web-Browser verschlüsselt. Viele Anwendungsprogramme übertragen ihre Nutzdaten unverschlüsselt. So werden mit Telnet oder FTP die Anmeldedaten im Klartext übertragen.

Über spezielle Outbound-Ports oder definierte Managementports lässt sich ein gesicherter Zugang von Systemadministratoren auf die zu verwaltenden Geräte einrichten. Eine Steuerung über Out-of-Bound (OoB) nutzt andere Kommunikationsverbindungen für die Übertragung von Befehlen. Zwischen dem Gerät und der Konsole wird ein dedizierter Port verwendet. Dies erhöht die Sicherheit, da eine Trennung von den allgemeinen Datenkanälen erfolgt.

Eine weitere Lösung ist anstelle der bekannten Dienste wie FTP, Telnet und RPC die Verwendung der Secure Shell Programme (SSH). Die Secure Tunneling-Funktionen ermöglichen eine stark verschlüsselte Authentifizierung für die Administrations- und Überwachungsfunktionen.

Das Sicherheitsniveau für den Betrieb von aktiven Netzwerkkomponenten orientiert sich an den Vorgaben des betrieblichen Sicherheitskonzeptes. Die ermittelten Sicherheitsanforderungen werden mit den Sicherheitsmerkmalen der eingesetzten Systeme verglichen. Um die allgemeine Schutzwirkung bequem zu erhöhen, können sehr einfache Sicherheitsmaßnahmen verwendet werden. Durch konsequente Änderung und Geheimhaltung von Benutzerkennungen sowie Passwörtern ist nur ein autorisierter Zugriff möglich. Der Einsatz von sicheren Diensten wie SSH, HTTPS und SNMPv3, wo dies möglich ist, schützt die Übertragung. Eine Zusammenfassung der Managementports zu einem VPN (Virtual Private Network), die nur Inbound bzw. Out-of-Bound-Management zulassen, bietet eine sichere Verbindung für die Verwaltung.

Neben der Auswahl technischer Maßnahmen und dem Wissen über deren Zusammenwirken, sind auch gute Kenntnisse über den aktuellen Industriestandard und der verfügbaren Produkte notwendig. Es gilt die identifizierten Sicherheitslücken durch Auswahl von geeigneten Alternativen zu schließen und somit den Anforderungen an die Sicherheit des Gesamtsystems gerecht zu werden.

FIREWALL

Eine Komponente zum Schutz vor Gefahren aus unsicheren Netzen, wie z.B. dem Internet, sind Firewall-Systeme. Eine Enterprise Firewall schützt das Unternehmensnetzwerk von Zugriffen aus dem Internet und regelt die Kommunikation zwischen öffentlichen und privaten Netzwerken. Durch die Integration eines Firewall-Systems wird das Intranet vom Internet oder jedem anderen öffentlichen Zugang entkoppelt.

Eine gute Firewall allein gewährleistet noch keine Sicherheit. Denn vor der Implementierung müssen Anforderungen, Nutzen und Risiken gewissenhaft analysiert werden, um ein durchdachtes, ganzheitliches Sicherheitskonzept zu erstellen. Bei der Bewertung der Sicherheit des Internet-Anschlusses sind alle diese Komponenten eines Systems mit zu berücksichtigen. Es gilt hierbei gefährliche Sicherheitslöcher und spätere Kosten zu vermeiden. Die Absicherung gegenüber dem Internet wird nicht allein durch die Firewall und deren Software erbracht, sondern durch

eine umfassende Konzeption, das die Hardware-Komponenten und die Betriebssysteme einschließt.

DFN-CERT Sicherheitsbulletins:
http://www.cert.dfn.de

Grundforderungen an Firewall-Systeme
Jeglicher Datenverkehr von innen nach aussen (und umgekehrt) läuft über die Firewall. Nur autorisierter („Wer darf was tun") Datenverkehr darf die Firewall passieren. Alles was nicht ausdrücklich erlaubt ist, wird von der Firewall abgewiesen. Die Firewall muss fehlerfreie Software haben, um gegen Angriffe resistent zu sein und darf nur über einen vertrauenswürdigen Pfad administrierbar sein.

Firewall-Funktionen:

- Dynamic Packet Filtering untersucht die Paket Header auf syntaktische Korrektheit und stellt sicher, dass sie innerhalb der definierten Sicherheitsregeln liegen.
- Application Proxies untersuchen nicht nur die Paket-Header, sondern auch den Paketinhalt.
- NAT (Network Address Translation) dynamisch und statisch.
- Routes Network Routes und Host Routes (im Trusted und Optional)
- Site und Port Blocking
- Diese Eigenschaften beziehen sich nur auf den Datenverkehr von der „External" NIC. Die „Trusted" und „Optional" NICs sind davon nicht betroffen.
- Logging und Notification
- Authentification wird normalerweise für die benutzerspezifische Kontrolle nach außen gehender Verbindungen benutzt.

Personal Firewalls
In einer Citrix-Umgebung greifen mobile Anwender über gesicherte Remote-Access-Lösungen (VPN, SSL, etc.) via das Internet auf die bereitgestellten Anwendungen zu. Eine Firewall sollte ebenso das ICA-Client-System vor unberechtigten Zugriff aus dem Internet schützen. Für den Schutz eines direkt ans Internet angeschlossenen PC gibt es sog. Personal Firewalls Software (oder Desktop Firewalls, wie die WindowsXP Internet Connection Firewall). Ihre Aufgabe ist es, den Rechner vor Angriffen von außen zu schützen.

TIPP
Die Windows XP Internet Connection Firewall lässt keinen Datenverkehr von außen nach innen zu. Um die Remoteunterstützung zu aktivieren, muss der RDP Port (3389) geöffnet werden – dieser wird nach Beendigung der Sitzung nicht automatisch deaktiviert.

Konfigurieren von IP-Anschlüssen in Citrix Serverfarmen
Folgende Informationen unterstützen bei der Konfiguration von Firewalls und bei der Überprüfung von Anschlusskonflikten mit anderer Software:

Die IP-Anschlüsse, die MetaFrame XP-Server, ICA-Clients, IMA und andere Citrix-Dienste in einer MetaFrame XP-Serverfarm verwenden, zeigt folgende Tabelle.

Anschlussverwendung	Standardanschluss	Konfiguration
ICA-Sitzungen	1494	Ändern der Anschlussnummer möglich
Citrix XML-Dienst	80	Ändern der Anschlussnummer möglich
Citrix SSL-Relay	443	Ändern der Anschlussnummer möglich
Gerichtete MetaFrame XP-Server zu Server UDP-Kommunikation	2512	Ändern der Anschlussnummer möglich
MetaFrame XP-Server Kommunikation mit Microsoft SQL	139, 1433 oder 443	Ändern der Anschlussnummer möglich
Citrix Management Console zu MetaFrame XP-Server Kommunikation	2513	Nicht konfigurierbar
ICA-Clients zu ICA-Browserdienst	1604 (UDP)	MetaFrame XP-Server antworten immer auf gerichtete UDP-Anfragen.
Gerichtete Server-zu-Server-UDP-Kommunikation	1604 (UDP)	Nicht konfigurierbar. Dieser Anschluss wird nur verwendet, wenn die Farm im gemischten Modus mit MetaFrame 1.8-Servern betrieben wird.
SNMP-Managementprotokoll	161	Nicht konfigurierbar
SNMP-Trap	162	Nicht konfigurierbar

Weitere IP-Ports sind entsprechend der Server-Rollen und eingesetzten Anwendungen auf den Systemen freizugeben und zu konfigurieren.

Aufspüren von Sicherheitslöchern

Die einzelnen Systemkomponenten gilt es auf folgende Aspekte zu prüfen:

- Offene Ports
- Verwundbarkeit der Dienste
- Passwörter

PortScan

Unnötig geöffnete Ports sind ein Sicherheitsrisiko. Ein Port-Scanner erkennt neben den Port-Nummern auch die dazugehörige Standard-Anwendung. Unerwartete offene IP-Ports sollten (z.B. mit TCPView von Sysinternals) nach Prozessen hin untersucht werden, die die entsprechenden Ports verwenden.

Unverwünschte oder unnötige Prozesse sollten durch Deinstallieren der dazugehörigen Programme oder durch deaktivieren der darüber laufenden Dienste beendet werden.

VulnerabilityScan

Vulnerability-Scanner untersuchen Systeme nicht nur nach offenen Ports, sondern ermitteln gleichzeitig eine Vielzahl zusätzlicher Informationen wie beispielsweise:

- Namen des Rechners (NetBIOS)
- Angemeldete Benutzer
- Gruppen und Benutzer
- Freigaben
- Offene Ports

Die gewonnenen Informationen zeigen die vermutlichen Schwachstellen inklusive einer Empfehlung, wie diese zu beheben sind.

Für ein System, das ohne gültige Anmeldung oder als NULL-Session erkannt wird gilt: Je weniger Informationen vom System gewonnen werden, desto besser.

PasswordAuditing

Password Auditing Tools versuchen schwache Passwörter mit verschieden Verfahren aufzuspüren. Mit einer Liste (Dictionary) von möglichen Passwörtern oder der Brute Force Methode werden Passwörter mit jeder Kombination von vorgegebenen Zeichen verglichen und bei Übereinstimmung ausgegeben. Schwache Passwörter sollte man durch starke Passwörter ersetzen.

Informationen über Sicherheitsprobleme enthält das Problem Alerts Archiv von Microsoft.

http://www.microsoft.com/germany/ms/ technet-servicedesk/paarchiv.htm

Schritt 3: Bewertung

Risikomanagement

Die Auswirkung von Sicherheitsrisiken gehört zu den deterministisch wenig bestimmbaren Größen in einem IT-System. Eine objektive Betrachtung und Analyse des Risikos kann zur Abschätzung dienen.

Vorgehensweise:
Qualitative Verfahren setzen die identifizierten Risiken durch eine verbale Beschreibung in Relation zueinander.

- Quantitative Ansätze liefern eine nach dem Schadensmaß geordnete Liste aller Schwachstellen.
- Die Schwachstellenanalyse zeigt auf, welche Sicherheitsvorkehrungen benötigt werden.

Eine Bestandsaufnahme lässt sich in verschiedene Kategorien gliedern, die aufzeigen, „was soll geschützt werden?“:

- Konfiguration- und Passwortdateien
- Datenbanken
- Kommunikationsdienste
- Logdateien
- Sicherheitskopien
- Überwachungsprogramme
- etc.

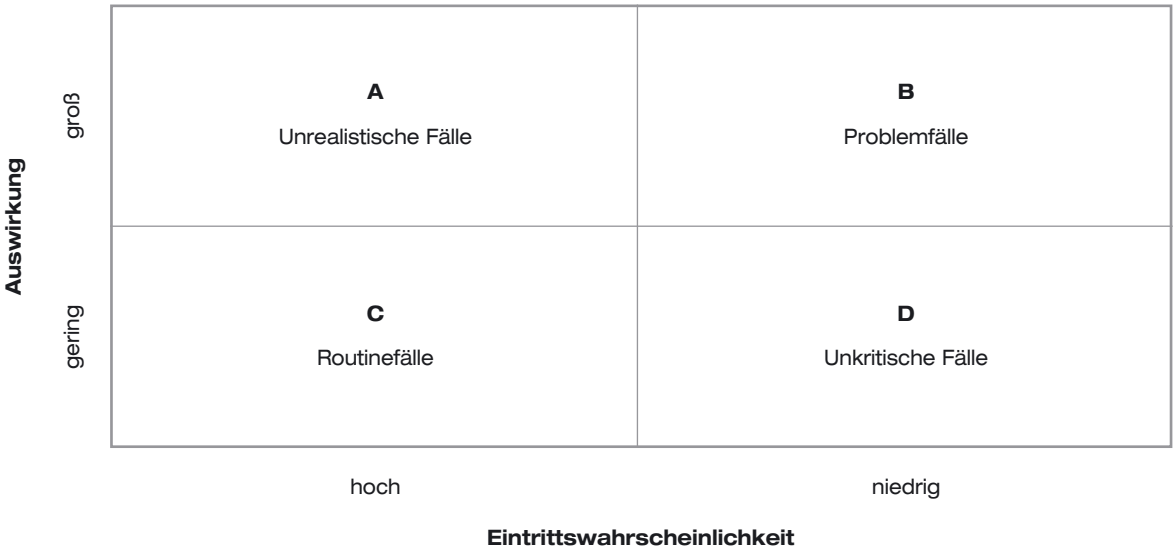
Risikoanalyse

Risiken haben eine ökonomische Wirkung auf das Projekt und das Unternehmen, und entstehen aus einem unzureichenden Informationsstand. Durch eine systematische Analyse in der Klärungsphase werden mögliche eintretende Risiken erkannt und können in einer Risikoanalyse bewertet werden. Eine detaillierte Beurteilung von Risiken wird durch einen bewerteten Kriterienkatalog erreicht.

Beispiel einer Bewertung

	Kriterien	Gewicht	Ausprägung					Risiko	
			1	2	3	4	5	derzeit ■	nach Beginn ●
Wirtschaftliches Risiko	Finanzrisiko (Existenz)	9,0			●	■		36	27
	Risiken aus der Zusammenarbeit mit dem Kunden	5,5		■	●			11	16,5
	Risiken aus der Zusammenarbeit mit Koop-Partnern	5,0		■	●			10	15
	Risiken im Projektmanagement	4,0		■●				8	8
	Risiken an Verfügbarkeit von qualifizierten Mitarbeitern	7,5		■	●			15	22,5
	Aufwand an Gegenmaßnahmen	3,0			■	●		9	12
Projektbedingte Risiken	Sind Sicherheitsziele und Aufgaben klar definiert	9,0		●		■		36	18
	Erfahrung an Sicherheitsthemen	4,0			●		■	20	12
	Komplexität des Projektes (Anzahl Module)	4,0		■●				8	8
	Projektdauer	3,0			■●			9	9
	Externe Lieferanten/Dienstleister	4,0				■	●	16	20
	Pufferzeiten ausreichend?	7,5		■	●			15	22,5
Technisches Risiko	Fehler im Entwurf	9,0		■			●	18	40
	Fehler in Umsetzung	8,0				■	●	24	40
	Reaktionszeit	2,0				■		8	6
	Störung der Angriffe	3,5		■			●	7	17,5
	Änderung	8,0			■		●	24	40
	Stabilität des Sicherheitssystems	4,0		■		●		8	12
		100	**unkritisch**		**normal**	**kritisch**		**282**	**346**

Die Kriterien der Einzelrisiken werden gewichtet und hinsichtlich ihrer Ausprägung bewertet. Die Auswertung ermöglicht eine Einordnung in festgelegte Risikoklassen und dient als eine Entscheidungshilfe zur Risikoanalyse.



- **Risikoklasse A:** *400 - 500* Gegenstandslos, da wirtschaftlich nicht vertretbar
- **Risikoklasse B:** *300 - 400* Können mit *üblichen* Maßnahmen nicht abgefangen werden, bedürfen besonderer Maßnahmen
- **Risikoklasse C:** *200 - 300* Typische Aufgabe eines Grundschutzes
- **Risikoklasse D:** *100 - 200* Bedürfen keiner besonderen Beachtung

Die Einzelrisiken werden systematisch bewertet – dennoch bleibt ein subjektiver Bewertungsspielraum. Die gewonnenen Informationen sollten zudem in eine Datenbasis einfließen, um spätere Projekte aus diesen Erfahrungen besser bewerten zu können.

Schritt 4: Umsetzung

MetaFrame XP

Die Citrix-Serverfarmen stellen eine flexible und stabile Methode zum Bereitstellen von Anwendungen dar.

Die Komponenten und Technologien, auf denen das serverbasierte Computingmodell von Citrix aufgebaut ist, umfassen die auf der Independent Management Architecture (IMA) basierende MetaFrame-XP Serverfamilie, die ICA-Clientsoftware und das ICA-Protokoll.

Windows 2000 Server

Der MetaFrame XP Server ist auf Windows 2000 installiert.

Die Windows 2000 Systemdienste wie Terminal Services (und Terminal Services Licensing) sind grundsätzlich Dienste, die bei Verwendung von MetaFrame XPe aktiviert sind.

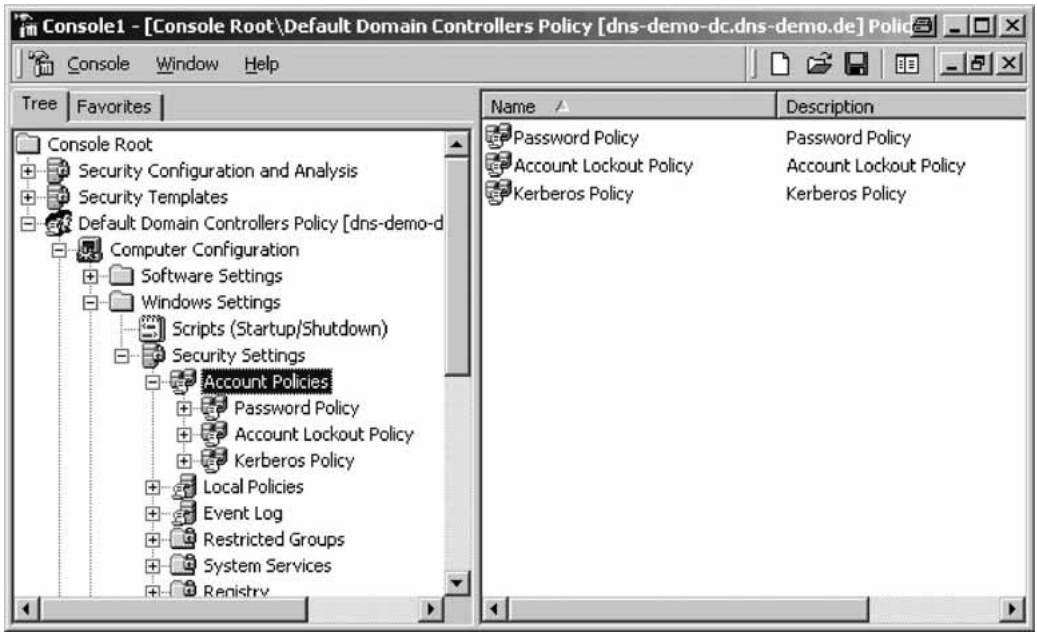
Das Betriebssystem stellt Funktionen zur Erhöhung der Sicherheit zur Verfügung. Mit der Microsoft Management Console (MMC) lassen sich alle wichtigen Sicherheitsfunktionen einstellen.

Die Zugriffsrechte auf die verschiedenen Objekte (Ordner und Dateien des Dateisystems, Freigaben des Server-Dienstes, Schlüssel der Registry und Objekte des Active Directory) kann man anhand der Sicherheitsrichtlinien für Benutzer und Gruppen festlegen. Die Gruppenrichtlinien (GPO) ermöglichen im Active Directory die automatische Verteilung der Sicherheitsrichtlinien innerhalb eines Unternehmens. Ein Auditing (Überwachungsrichtlinien) ermöglicht das Überwachen der Aktionen (z.B. Objektzugriffe) durch Benutzer und Gruppen.

Sicherheit für die Konfiguration von Computern

Mit den Snap-In-Sicherheitsvorlagen für die Microsoft Management Console (MMC) bietet Windows 2000 ein zentrales Werkzeug zum Definieren von Systemsicherheit. Es verwaltet alle vorhandenen Sicherheitsattribute, die angezeigt, angepasst und auf einem lokalen Computer angewendet oder in ein Gruppenrichtlinienobjekt importiert werden können.

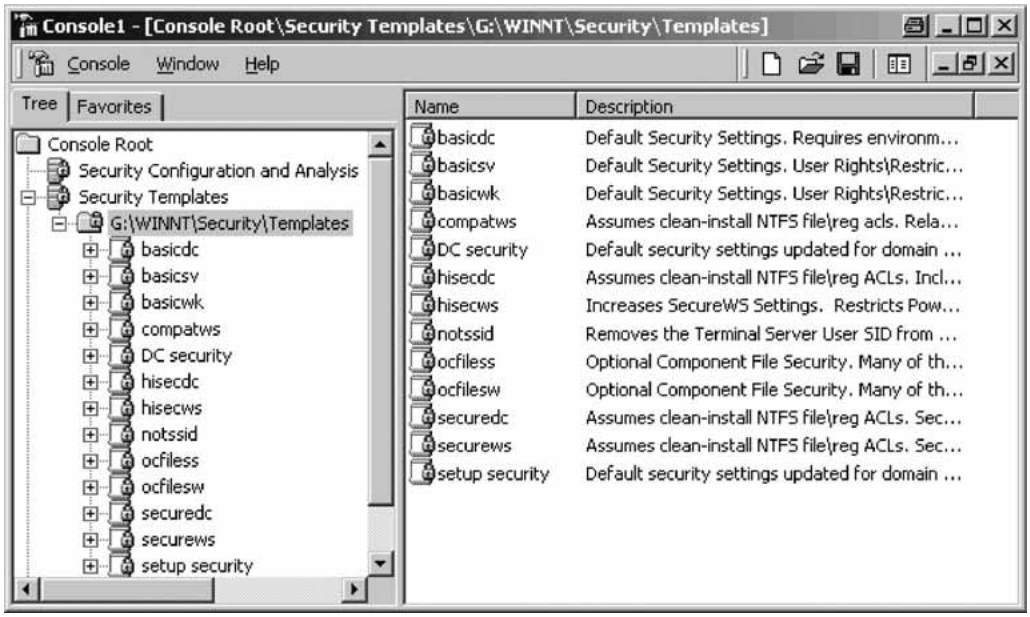
Sicherheitsvorlagen können außerdem als Basiskonfiguration für Sicherheitsanalysen dienen, wenn sie zusammen mit den Snap-InSicherheitskonfiguration und -analyse verwendet werden.



Die Tabelle zeigt die Einstellmöglichkeiten für Sicherheitsrichtlinien und Schablonen:

Bereich	Bedeutung
Kontenrichtlinien	Konfiguration von Kennwort-, Konten- und Kerberos-Richtlinien
Lokale Richtlinien	Konfiguration der Überwachung von Benutzerrechten und Sicherheitsoptionen
Ereignisprotokoll	Einstellungen für Anwendungs-, Sicherheits- und Systemprotokoll
Eingeschränkte Gruppen	Konfiguration der Gruppenmitgliedschaft für sicherheitssensible Gruppen
Systemdienste	Einstellungen für das Startverhalten und die Sicherheit von Diensten
Registry	Sicherheitsrelevante Einstellungen für Registry-Schlüssel
Dateisystem	Konfiguration für einzelne Freigaben, Ordner und Dateien

Der **Security Configuration Editor** (SCE) erlaubt die Definition von Schablonen in Form von .inf-Dateien, in denen entsprechende Einstellungen zusammengefasst sind.



Die in einer Schablone hinterlegten Einstellungen können anschließend in den **Security Configuration Manager (SCM)** eingelesen werden, um diese mit den aktuellen Einstellungen des Computers vergleichen zu können.

Der *Security Guide Scripts Download* für Windows 2000 Server bietet unter anderen folgende Sicherheitsvorlagen an:

- Baseline Security
- Baseline Security für Domain Controller
- File and Print Server
- Internet Information Server
- Infrastructure

http://download.microsoft.com/download/win2000adserv/secops/RTM/NT5/EN-US/ SecOps.exe

Inhalt der SecOps.exe:

```
eventcomb\eventcombmt.chm
eventcomb\eventcombmt.exe

\patchmgmt\hfnetchk
\patchmgmt\logs
\patchmgmt\movelog.vbs
\patchmgmt\readme.txt
\patchmgmt\serverlists
\patchmgmt\hfnetchk\readme.txt
\patchmgmt\serverlists\servers.txt

\templates\baseline.inf
\templates\baselinedc.inf
\templates\exchange backend incremental.inf
\templates\exchange dc incremental.inf
\templates\file and print incremental.inf
\templates\iis incremental.inf
\templates\infrastructure incremental.inf
\templates\owa frontend incremental.inf
```

NSA (NATIONAL SECURITY AGENCY)

Die National Security Agency (www.nsa.org) bietet zusätzlich sehr nützliche und den Anforderungen entsprechend verschiedene Security Recommendation Guides unter http://nsa1.www.conxion.com an:

- Microsoft Windows 2000 Network Architecture Guide
- Guide to Securing Microsoft Windows 2000 Group Policy
- Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set
- Group Policy Reference
- Guide to Securing Microsoft Windows 2000 Active Directory
- Guide to Securing Microsoft Windows 2000 DNS
- Guide to Securing Microsoft Windows 2000 Encrypting File System
- Guide to Securing Microsoft Windows 2000 File and Disk Resources
- Guide to Securing Microsoft Windows 2000 Schema
- Guide to Securing Windows NT/9x Clients in a Windows 2000 Network
- Guide to Secure Configuration and Administration of Microsoft ISA Server 2000
- Guide to the Secure Configuration and Administration of Microsoft Windows 2000 Certificate Services
- Guide to the Secure Configuration and Administration of Microsoft Windows 2000 Certificate Services (Checklist Format)
- Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0
- Guide to Using DoD PKI Certificates in Outlook 2000
- Guide to Windows 2000 Kerberos Settings
- Microsoft Windows 2000 Router Configuration Guide
- Guide to Securing Microsoft Windows 2000 DHCP
- Guide to Securing Microsoft Windows 2000 Terminal Services
- Microsoft Windows 2000 IPsec Guide
- Guide to the Secure Configuration and Administration of Microsoft Exchange 2000

Außerdem sind dazugehörige Security Configuration Templates für den Security Configuration Editor (SCE) im ASCII-Text-Format (Windows 2000 „INF“ Files) erhältlich:

- SCERegVl.INF
- W2KDC.INF
- W2K Domain Policy.INF
- W2K Server.INF
- W2K Workstation.INF
- ISA.INF

DAS DIENSTPROGRAMM SECEDIT

Das Befehlszeilenprogramm *Secedit.exe* kann manuell, über eine Stapelverarbeitungsdatei oder über den Taskplaner aufgeführt werden, um Sicherheitsvorlagen automatisch zu erstellen, anzuwenden oder die Systemsicherheit zu analysieren.

Dieses Programm ist besonders hilfreich, wenn die Sicherheit für mehrere Computer zu analysieren oder zu konfigurieren ist.

Analysieren der Systemsicherheit	**secedit /analyze**	Mit diesem Befehl kann man die Systemsicherheit analysieren.
Konfigurieren der Systemsicherheit	**secedit /configure**	Mit diesem Befehl wird die Systemsicherheit konfiguriert, indem eine gespeicherte Vorlage angewendet wird.
Aktualisieren der Sicherheitseinstellungen	**secedit /refreshpolicy**	Mit diesem Befehl wird die Systemsicherheit aktualisiert, indem die Sicherheitseinstellungen erneut auf das Objekt Gruppenrichtlinie angewendet werden.
Exportieren von Sicherheitseinstellungen	**secedit /export**	Mit diesem Befehl kann man eine gespeicherte Vorlage aus einer Sicherheitsdatenbank in eine Vorlagendatei für Sicherheit exportieren.
Überprüfen einer Konfigurationsdatei für Sicherheit	**secedit /validate**	Mit diesem Befehl lässt sich die Syntax einer Vorlage für Sicherheit überprüfen, bevor sie zur Analyse in eine Datenbank importiert oder auf ein System angewendet wird.

Beispiel mit secedit.exe zum Analysieren der Systemsicherheit:

```
Secedit /analyze
/DB         Gibt den Pfad zu der Datenbank an
/CFG        Parameter gibt den Pfad zu der Vorlage für die
            Sicherheit an, die zur Analyse in die Datenbank
            importiert werden soll
/log        Pfad zur Protokolldatei
/verbose    Informationen bei der Ausführung werden angezeigt
/quiet      Unterdrückt Ausgaben auf dem Bildschirm bzw. in die
            Protokolldatei
```

NFuse Classic und Secure Gateway Service

Internet Information Server
NFuse Classic und Secure Ticket Authority (STA) des Citrix Secure Gateway nutzen den Internet Information Service (IIS) als Web-Server auf Basis von Windows 2000.

Die Rechte des Web-Publishingdienstes regeln den Zugriff über das HTTP (Hypertext Transfer Protocol):

- Scriptzugriff (Script Source Access)
- Lesen (Read)
- Schreiben (Write)
- Verzeichnis durchsuchen (Directory Browsing)
- Ausführungsberechtigungen (Execute Permission): Keine, Nur Skripts, Skripts und ausführbare Dateien
- Anwendungsschutz (Application Protection): niedrig, mittel, hoch

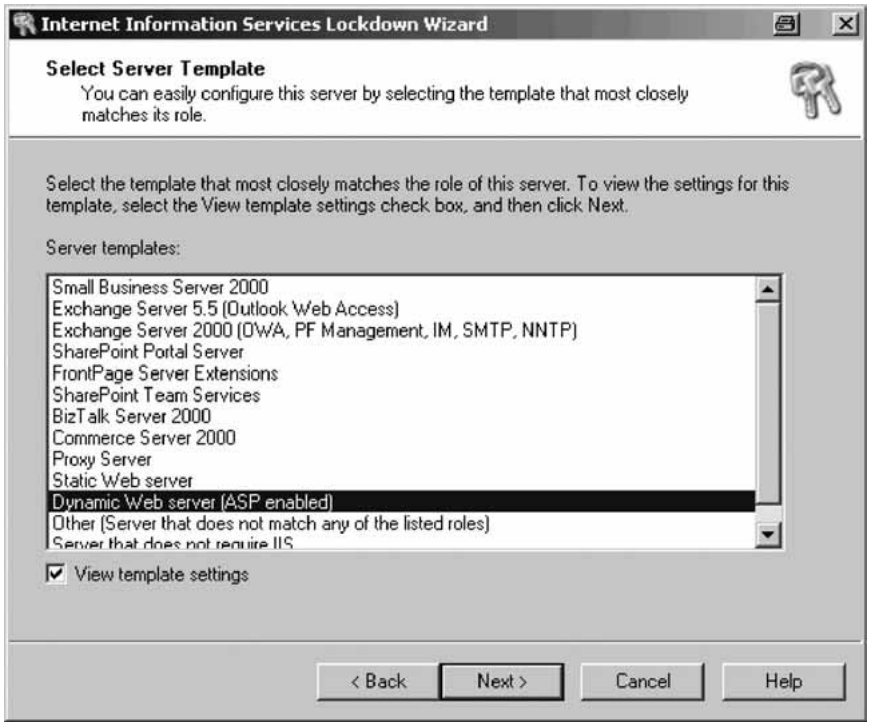
TIPP
Die Installation eines Web-Servers auf einem anderen Laufwerk bzw. Pfad für das WWW-Root kann nur in der Unattended Installation durchgeführt werden (siehe Knowledge-Base-Artikel Q261002). Dazu wird folgender Eintrag in der unattended.txt oder winnt.sif eingefügt:

[InternetServer]
PathWWWRoot = „Pfad“

IIS LOCKDOWN TOOL
Für den Schutz des Internet Information Services stehen das IIS Lockdown Tool (Version 2.1) und der URLScan (ein Bestandteil des IIS Lockdown Tools) von Microsoft zur Verfügung.

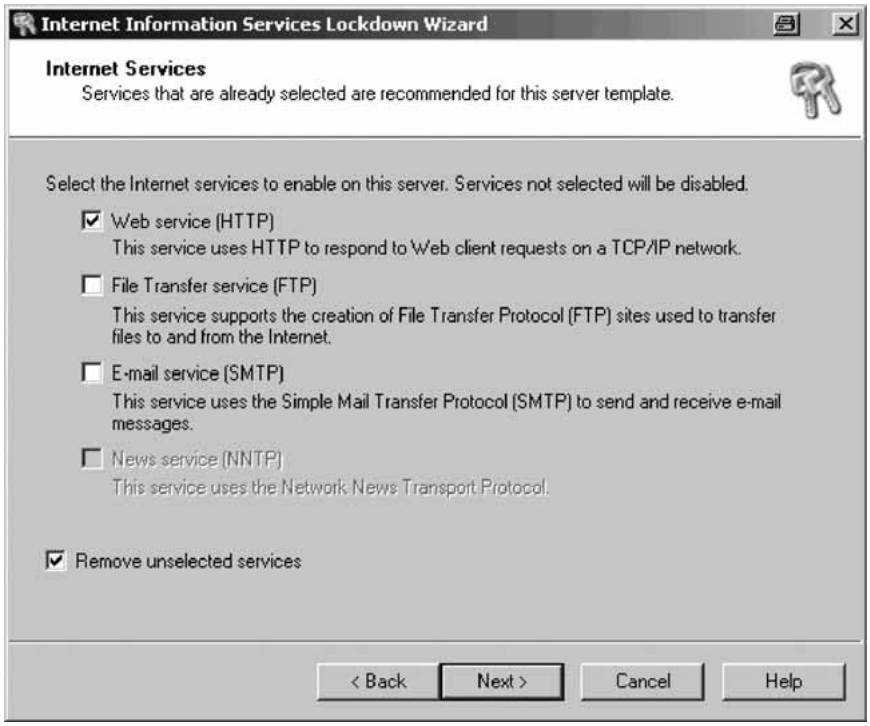
http://www.microsoft.com/technet/security/tools/locktool.asp

Mit Auswahl eines Templates des IIS Lockdown-Tools können in Abhängigkeit von der Serverrolle einzelne Dienste des IIS aktiviert, deaktiviert oder deinstalliert werden. Das Entfernen von diversen Komponenten, wie beispielsweise das WebDAV Protokoll, erhöht die Sicherheit ebenso wie verschärfte Berechtigungen und das Deaktivieren des Script Mappings.



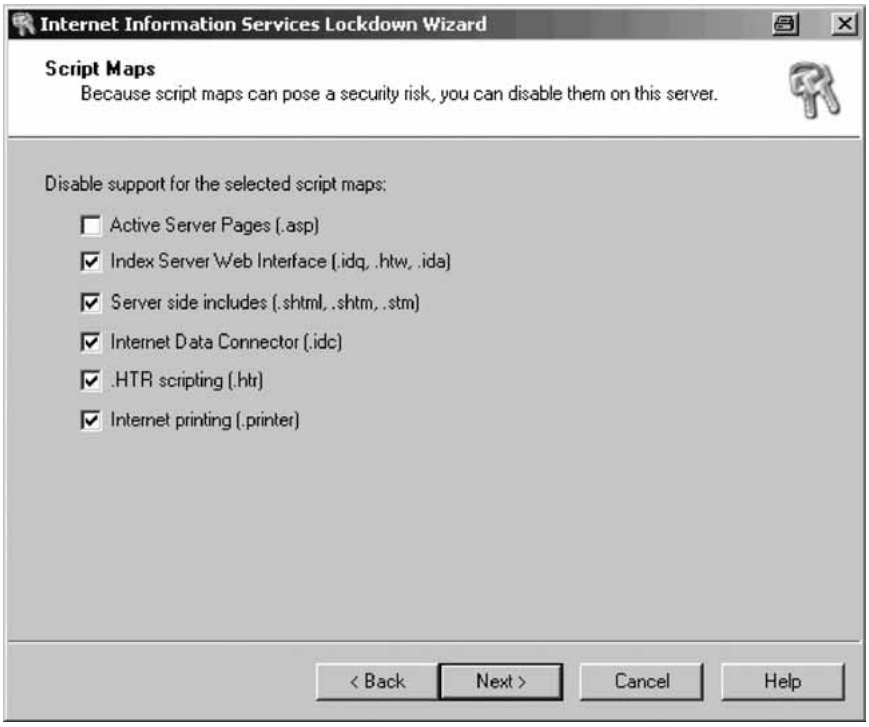
SCHRITT 1:
Auswahl der Server-Rolle

Die Auswahl der Serverrolle dient dem Erteilen von Anweisungen zum Konfigurieren der grundlegenden Sicherheit auf Servern mit IIS 5.



SCHRITT 2:
Welche Dienste sollen verwendet werden?

Dienste wie FTP, SMNT, NNTP, IIS Admin Service sind auf einem dedizierten IIS für NFuse und Secure Gateway im Internet nicht im Einsatz und daher zu deaktivieren. Ein Entfernen der Dienste erhöht die Sicherheit vor unerlaubtem Zugriff auf diese Dienste.



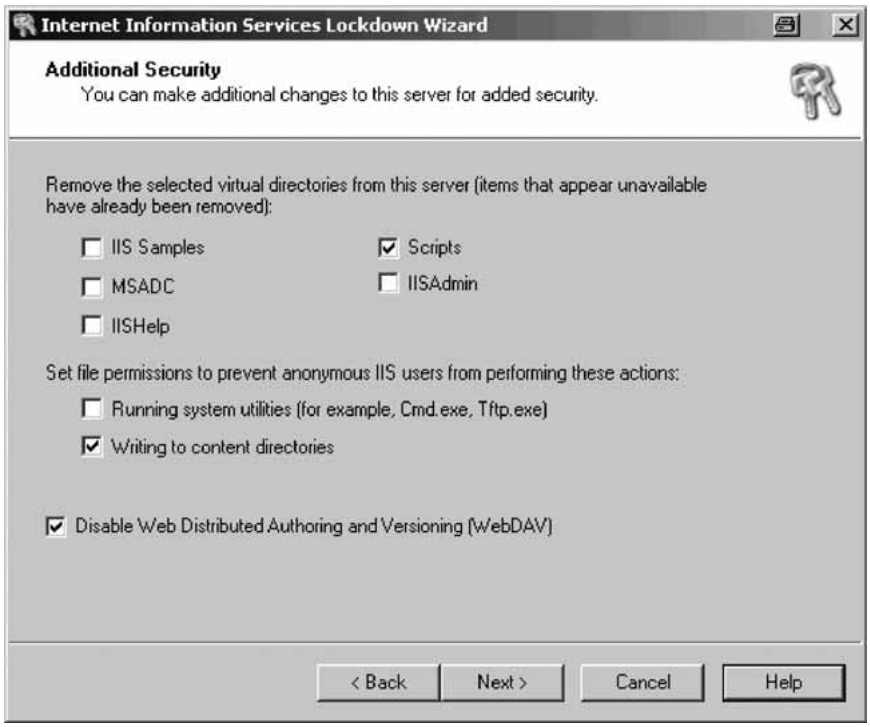
SCHRITT 3: Script-Zuordnungen deaktivieren?

Wenn IIS eine Anforderung für eine Datei eines Typs (z.B. ASP und SHTM) erhält, wird der Aufruf von einer DLL verarbeitet. Werden Erweiterungen oder Funktionen nicht verwendet, sollte man die entsprechenden Zuordnungen entfernen.

Entfernen von:	Wenn Folgendes nicht verwendet wird:
.htr	Webbasiertes Zurücksetzen von Kennwörtern
.idc	Internet-Datenbank-Connector (alle IIS 5-Websites sollten ADO oder eine ähnliche Technologie verwenden)
.shtm, .stm und .shtml	Serverseitige Includedateien
.printer	Internetdrucken
.htw, .ida und .idq	Index Server

Das Festlegen geeigneter Access Control Lists (ACLs) für virtuelle Verzeichnisse ist ebenfalls anwendungsabhängig und kann manuell erfolgen.

Dateityp	Zugriffssteuerungslisten
CGI (EXE, DLL, CMD, PL)	Jeder (Ausführen) Administratoren (Vollzugriff) System (Vollzugriff)
Skriptdateien (ASP)	Jeder (Ausführen) Administratoren (Vollzugriff) System (Vollzugriff)
Includedateien (INC, SHTM, SHTML)	Jeder (Ausführen) Administratoren (Vollzugriff) System (Vollzugriff)
Statische Inhalte (TXT, GIF, JPG, HTML)	Jeder (Lesen) Administratoren (Vollzugriff) System (Vollzugriff)



SCHRITT 4:
Entfernen von virtuellen Verzeichnissen

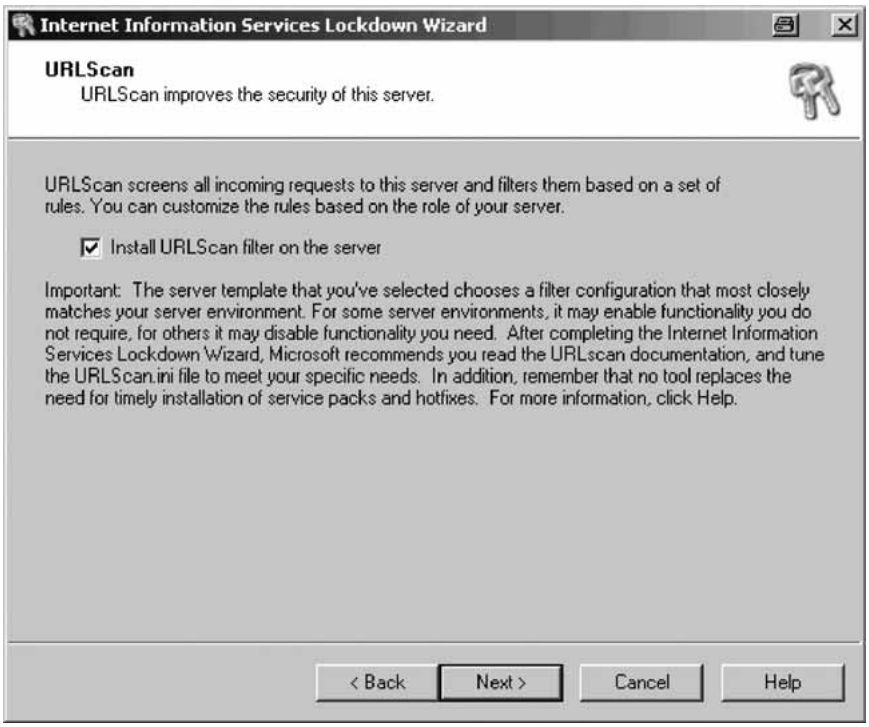
Statt ACLs für jede Datei festzulegen, lassen sich auch neue virtuelle Verzeichnisse für jeden Dateityp anlegen. Für jedes Verzeichnis wird die ACL festgelegt und die Vererbung an die Dateien zugelassen.

Beispielsweise kann eine Verzeichnisstruktur folgendermaßen aussehen:

- C:\inetpub\wwwroot\NFuse\statisch (HTML)
- C:\inetpub\wwwroot\NFuse\include (INC)
- C:\inetpub\wwwroot\NFuse\skript (ASP)
- C:\inetpub\wwwroot\NFuse\programme (DLL)
- C:\inetpub\wwwroot\NFuse\grafiken (GIF, JPEG)

HINWEIS

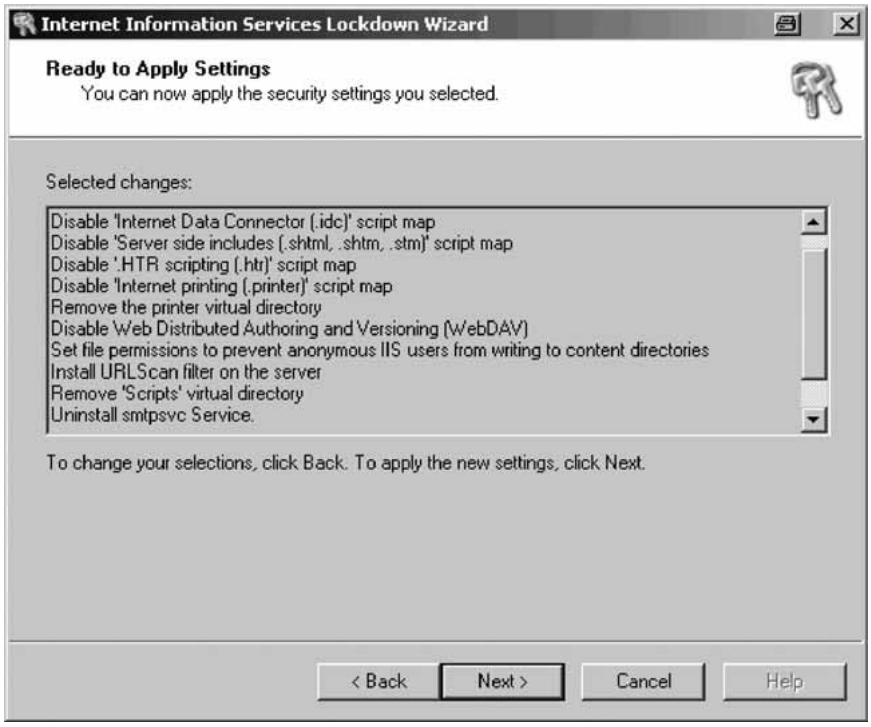
Das virtuelle Verzeichnis **iisadmpwd** ermöglicht das Zurücksetzen von Windows-NT- und Windows-2000-Kennwörtern. Es ist hauptsächlich im Intranet vorgesehen und wird im Rahmen von IIS 5 nicht installiert, jedoch auch nicht entfernt, wenn eine Aktualisierung eines Servers mit IIS 4 auf IIS 5 durchgeführt wird. Das Verzeichnis sollte entfernt werden, sofern es nicht benötigt wird. Weitere Informationen zur Funktionsweise sind im Microsoft Knowledge-Base-Artikel Q184619 zu finden.



SCHRITT 5:
Soll der URLScan installiert werden?

URLScan filtert alle ankommenden Requests für den Server. Die Regeln für die Filterung legen Sie als Administrator fest. URLScan schützt vor Vulnerabilities, die im Microsoft Security Bulletin 02-018 beschrieben sind. Der MS02-018 ist ein kumulatives Update vom April 2002 für die Internet-Informationsdienste. Die Informationen in diesem Artikel beziehen sich auf den Microsoft Internet Information Services (IIS), Version 4.0, 5.0 und 5.1.

HINWEIS
Für den IIS 5.1 steht die Datei Q319733_WXP_SP1_x86_DEU.exe und für den IIS 5.0 die Datei Q319733_ W2K_SP3_X86_DE.exe im Microsoft Download Center zum Download zur Verfügung.



SCHRITT 6:
Abschließende Konfiguration

Zusammenfassung der getroffenen *IIS Lock Down* Einstellungen und abschließende Konfiguration.

Deaktivieren nicht benötigter System-Dienste
Welche Dienste deaktiviert werden können, hängt von der Rolle des Servers ab. Eine minimale Konfiguration des IIS als Mitgliedsserver reduziert die annähernd 100 Systemdienste auf rund zwanzig. Somit werden die möglichen Sicherheitsrisiken durch nicht genutzte (und überwachte) Systemdienste reduziert.

Dienste	Servicename	Empfohlene Startart
COM+ Event System	EVENTSYSTEM	Manual
DHCP Client	DHCP	Automatic
Distributed Link Tracking Client	TRKWKS	Automatic
DNS Client	DNSCACHE	Automatic
Event Log	EVENTLOG	Automatic
Logical Disk Manager	DMSERVER	Automatic
Logical Disk Manager Administrative Service	DMADMIN	Manual
Net Logon	NETLOGON	Automatic
Network Connections	NETMAN	Manual
Performance Logs and Alerts	SYSMONLOG	Manual
Plug and Play	PLUGPLAY	Automatic
Protected Storage	PROTECTEDSTORAGE	Automatic
Remote Procedure Call (RPC)	RPCSS	Automatic
Remote Registry Service	REMOTEREGISTRY	Automatic
Security Accounts Manager	SAMSS	Automatic
Server	LANMANSERVER	Automatic
System Event Notification	SENS	Automatic
TCP/IP NetBIOS Helper Service	LMHOSTS	Automatic
Windows Management Instrumentation Driver Extension	WMI	Manual
Windows Time	W32TIME	Automatic
Workstation	LANMANWORKSTATION	Automatic
World Wide Web Publishing Service	W3SVC	Automatic

Citrix-Verwaltungswerkzeuge

Citrix Data Store
Der Data Store einer MetaFrame-XP-Serverfarm kann auf einer SQL-basierenden Datenbank installiert werden. Microsoft SQL Server ist eine Client-/Server-Datenbank, die stabile und skalierbare Unterstützung für den Datenzugriff durch mehrere Server bietet. Sie eignet sich für die Anwendung in MetaFrame Serverfarmen beliebiger Größe.

Beim Betrieb einer SQL-Server-Umgebung sind die Aspekte der Benutzer- und Kontenverwaltung innerhalb einer Failover-Cluster-Unterstützung, hinsichtlich dem Protokollversand sowie für lokale Administratoren, Domänen-Admins und integrierte Administratoren zu betrachten.

MetaFrame XP verwendet beim Zugriff auf den Microsoft SQL-Datenbank-Server die Authentifizierungsmethode Server-Authentifizierung. Der administrative Standardbenutzername von Microsoft SQL ist „SA“ und sollte mit einem Kennwort versehen sein oder durch einen anderen Account ersetzt werden.

Um die Anmeldeüberwachung sowohl für erfolgreiche als auch für fehlgeschlagene Anmeldeversuche auf dem SQL-Server zu aktivieren, kann der Datenbank-Administrator (DBA) im Dialogfeld SQL-Server-Eigenschaften auf der Registerkarte Sicherheit unter Überwachungsebene auf die entsprechende Option klicken. Diese überwachten Anmeldeversuche werden sowohl in das Windows-2000-Anwendungsereignisprotokoll als auch in das SQL-Server-Ereignisprotokoll geschrieben. Damit die Änderung wirksam wird, muss der SQL-Server-Dienst angehalten und neu gestartet werden.

Ein C2-Überwachungsmodus zeichnet alle Ereignisse der Ereignisklassen für die Sicherheitsüberwachung und aller Datenspalten auf.

In der SQL-Server-2000-Onlinedokumentation finden sich weiter gehende Informationen zu „Sicherheitsüberwachung-Ereigniskategorie“ und „c2 audit mode (Option)“.

Das Microsoft Security Bulletin MS02-30 (Unchecked Buffer in SQLXML Could Lead to Code Execution – Q321911) beschreibt einen Patch gegen Sicherheitslücken in Microsoft SQL Server 2000.

Citrix Management Console
Die Citrix Management Console und IMA ermöglichen die Verwaltung von MetaFrame-XP-Servern und darunter betriebenen Serverfarmen von einem beliebigen Standort aus. Die Konsole kommuniziert über das IMA-Protokoll über TCP/IP mit MetaFrame-XP-Servern und anderen IMA-basierten Citrix-Servern.

Citrix Web Console
Mit der Citrix Web Console können MetaFrame-XP-Serverfarmen mit einem Webbrowser überwacht werden.

Mit der Webkonsole können folgende Informationen zu einer Serverfarm anzeigt und verwaltet werden: Aktive Sitzungen, veröffentlichte Anwendungen, Server und Benutzer, Abmelden von Sitzungen, Spiegelung, Trennen und Senden von Nachrichten wie mit der Citrix Management Console.

WICHTIG!
Die Citrix Web Console verschlüsselt die Informationen nicht, die an Webbrowser gesendet werden. Wenn sich ein Benutzer an der Konsole anmeldet, werden die Anmeldeinformationen des Benutzers als unverschlüsselter Text an die Webkonsole gesendet. Um maximale Sicherheit zu gewährleisten, ist der Webbrowser und IIS für die Verwendung von SSL-Verschlüsselung zu konfigurieren.

Citrix Network Manager
Citrix Network Manager ist eine in MetaFrame XPe enthaltene Komponente, die Systemverwaltungsfunktionen über SNMP-Verwaltungskonsolen von Drittanbietern zur Verfügung stellt. Network Manager setzt sich aus einem SNMP-Agent, der mit MetaFrame XPe installiert wird, und Plug-Ins für die unterstützten SNMP-Managementkonsolen zusammen.

TIPP
Der SNMP Service (und SNMP Trap) werden nur bei Einsatz von MetaFrame XPe und Network Management benötigt. Eine Deaktivierung des SNMP-Dienstes verhindert, dass durch SNMP-Attacken die Management Information Base (MIB) durch einen SNMP-Walk auslesen und Informationen für weitere Attacken verwendet werden können.

Sicherheitseinstellungen für die SNMP-Community
Da alle SNMP-Implementierungen die SNMP-Version 1 (RFC 1157) unterstützen müssen, ist eine Prüfung der Produkte hinsichtlich der Angriffsgefahren notwendig. Sehr viele Hersteller geben Aussagen und Hinweise über ihre Produkte. Eine Hilfestellung ist in der Knowledgebase des CERT Coordination Center verfügbar. Unter http://www.kb.cert.org/vuls/id/107186 finden sich Lösungen für zusätzliche und geeignete Gegenmaßnahmen.

Die SNMP-Version 2 (RFC 1902) kommt am häufigsten zum Einsatz. Die Datenübertragung wird durch einen Community-Namen geschützt. Unter Umständen können die SNMP-Passwörter in Erfahrung gebracht werden: Sind die SNMP-Schlüssel als „public" definiert, so sind sie mit SNMP-Kommandos remote einsehbar. Daher ist eine mehrstufige Vergabe von Community-Namen für Schreib- und Lese-Vorgänge unerlässlich. Eine SNMP Brute Force Attack (mit SNMP-Walk) versucht mit jeder möglichen Zeichenkette die SNMP Read-Only and Read-Write Community Strings festzustellen.

Wenn eine SNMP-Community auf dem MetaFrame-Server mit Lese- und Schreibberechtigungen konfiguriert ist und der Citrix SNMP-Agent aktiviert ist, können Angreifer remote potentiell gefährliche Vorgänge ausführen. Für die folgenden Network-Manager-Funktionen ist Lese- und Schreibzugriff erforderlich:

- Neustarten eines MetaFrame-Servers
- Abmelden eines Benutzers von einem MetaFrame-Server
- Trennen eines Benutzers von einem MetaFrame-Server
- Senden einer Meldung an einen Benutzer
- Beenden eines Prozesses
- Herunterfahren eines MetaFrame-Servers

TIPP
Um zu verhindern, dass unbefugte Benutzer administrative Vorgänge über SNMP ausführen, ist der SNMP-Dienst auf den MetaFrame-Servern so zu konfigurieren, dass nur SNMP-Pakete von bekannten Computern mit SNMP-Managementkonsolen angenommen werden. Wenn Sie eine Firewall haben, können Sie „Spoofing" verhindern, indem die Firewall so konfiguriert wird, dass Pakete abgeblockt werden, die von außerhalb der Firewall kommen, aber eine Quell-IP-Adresse haben, die bekanntermaßen innerhalb der Firewall liegt.

Alternativ dazu können diese Funktionen komplett deaktiviert werden, indem die Lese- und Schreibberechtigungen für alle SNMP-Communities auf allen MetaFrame-Servern entfernt werden. Statt Network Manager mit Lese- und Schreibzugriff zu verwenden, kann auch die Citrix Management Console einsetzt werden. Die Citrix Management Console verwendet die domänenbasierte Benutzerauthentifizierung von Windows NT und ist daher eine sicherere Methode für den Zugriff auf diese Funktionen. Die Citrix Management Console kann direkt von Network Manager aus gestartet werden.

Sichere Server-zu-Server-Verbindungen
Windows 2000 stellt mit IPSec die Verschlüsselung des Netzwerkverkehrs auf IP-Ebene (OSI-Ebene 3) zur Verfügung. Damit kann eine Verschlüsselung auch für die Protokolle (z.B. telnet, ftp etc.) eingerichtet werden, die selbst keine Verschlüsselung anbieten und Klartextauthentifikation verwenden. Mit Hilfe der IPSec-Richtlinien lassen sich Paketfilter für IPSec-Datenpakete, wie auch NonIPSec-Datenpakete einrichten, die jeglichen IP-Verkehr bearbeiten.

Schritt 5: Prüfen und überwachen

Festlegen geeigneter ACLS für die ILS-Protokolldateien

Die von IIS generierten Protokolldateien werden in %systemroot%\system32\LogFiles abgelegt und sollten folgende ACL aufweisen:

- Administratoren (Vollzugriff)
- System (Vollzugriff)
- Jeder (Lesen, Schreiben, Erstellen)

Aktivieren von Protokollierung

Um zu ermitteln, ob ein Web-Server Angriffen ausgesetzt ist, ist eine Protokollierung unabdingbar.

Die Protokollierung ist im **Internetdienste-Manager** zu aktivieren.

Das *erweiterte W3C-Protokollformat* legt folgende Eigenschaften fest:

- Client-IP-Adresse
- Benutzername
- Methode
- URI-Stamm
- Protokollstatus
- Win32-Status
- Benutzer-Agent
- Server-IP-Adresse
- Serveranschluss

TIPP
Die Bedeutung von Win32-Fehlern kann mit der Befehlszeile **net helpmsg <Fehlernummer>** ermittelt werden.

Schritt 6: Reaktion und Anpassungen

Die Datensicherheit befasst sich mit der Verfügbarkeit wie auch mit der Wiederherstellung von Daten.

Wichtig sind erprobte Strategien für Erhalt und Verfügbarkeit der Daten und die Kommunikationsverbindungen. Die Kontinuitäts- und Wiederanlaufplanungen sind wichtig, um schnell die Geschäftstätigkeit im Notfall wieder herzustellen. Tritt ein Notfall ein, hängt das Business Continuity oder Disaster Recovery des Unternehmens von der Güte dieser Planungen und der Verfügbarkeit der Notfall-Ressourcen ab.

Vorgehensweise:

- Entwickeln von Aktionsplänen
- Kommunikationspläne
- Notfallpläne
- Backup-Systeme für Systeme
- Pflegen von Beziehungen
- Testläufe
- Review
- Abstimmungen

Verbesserung und Gewährleistung der Betriebsqualität:

- Durch standardisiertes Vorgehen wird die Vollständigkeit der zu liefernden Ergebnisse am besten gewährleistet.
- Definierte Zwischenergebnisse ermöglichen frühzeitige Prüfmaßnahmen.
- Einheitliche Maßnahmen dienen der Durchführung von schnellen Prüfmaßnahmen.
- Die begleitenden sicherheitsrelevanten Tätigkeiten dienen u.a. der Qualitätssicherung, dem Konfigurationsmanagement und technischen Projektmanagement und unterstützen die Anforderungen der IT-Sicherheitskriterien.

Schritt 7: Reaktion und Anpassungen

Zur Installation von Service Packs und Hotfixes in großen Infrastrukturen ist der Systems Management Server (SMS) für die einwandfreie Softwareverteilung geeignet. Zukünftig wird ein Add-On zur Verfügung stehen, mit dem auch eine kombinierte Hotfix-Analyse und -Verteilung möglich ist.

Active Directory stellt zwar einen Mechanismus zur Softwareverteilung von MSI-Paketen bereit, die aber zur Verteilung von Service Packs und Hotfixes ungeeignet ist, da diese nur bedingt in diesem Format vorliegen.

Die manuelle Installation einer größeren Anzahl von Hotfixes kostet viel Zeit und erfordert üblicherweise einen Systemneustart. Mit Hilfe von QChain können mehrere Hotfixes auf einmal, ohne Reboot, installiert werden; allerdings ist diese Vorgehensweise nicht für jede Kombination von Hotfixes geeignet.

Einzelne Systeme oder eine kleine Anzahl von Systemen lassen sich mit Windows Update sehr einfach analysieren und aktualisieren. Windows Update erhält von einer Microsoft Website die aktuelle Liste von Hotfixes und lädt bei Bedarf die Updates herunter. Die fehlenden Hotfixes und Updates werden dem Benutzer zur Installation angeboten, der die gewünschten Updates auswählt. Diese werden heruntergeladen und installiert.

Der Software Update Service (SUS) bietet einen zentralisierten Softwareverteilungsansatz. Ein SUS-Server lädt die verfügbaren Updates für Windows 2000 aus dem Internet herunter, um sie lokal vorzuhalten. Nach dem Download müssen die Updates noch vom Administrator verifiziert und freigegeben werden. Dies ermöglicht, dass Systeme eines Netzwerks über den SUS-Client ihre Software-Updates nur noch vom lokalen SUS-Server installieren müssen. Der Software Update Service Client bietet verschiedene Operationsstufen an. Die Updates lassen sich manuell oder automatisch (nach einem eingestellten Zeitplan) installieren.

Die Möglichkeiten, Citrix-Hotfixes zu installieren, ist in den Dokumenten CTX761623 (Unattended Installation) und CTX678340 (Silent Installation) beschrieben. Die Hinweise für Service Packs von Citrix sind im Dokument CTX096380 (Feature Release 2 / Service Pack 2) erläutert.

Softwaremanagement

Das Management von Service Packs und Hotfixes ist ein wichtiger Teil des Systemmanagements, mit dem sichergestellt werden kann, dass eine sichere Infrastruktur auch sicher bleibt.

Das **Strategic Technology Protection Program** (**STPP**) von Microsoft ist ein Programm, das Informationen, Services und Tools bereitstellt, um die Systeme zu schützen. Update-Services, Tools und weitere Informationsquellen zum Thema Sicherheit bei Microsoft sind unter ***http://www.microsoft.com/germany/themen/security/tools.htm*** abrufbar.

Mit der Microsoft Sicherheits-Benachrichtigung können unter ***http://www.microsoft.com/securitynotification*** auch proaktiv Informationen über neue Gefahren und mögliche Sicherheitslücken bezogen werden.

Allgemeine Vorgehensweise

Im ersten Schritt des STPP werden mit entsprechenden Maßnahmen die bestehenden Systeme sicherer gemacht, um diese vor etwaigen Gefahren zu schützen. Mit dem zweiten Schritt wird der erreichte Standard gehalten und mit Hilfe von regelmäßigen Updates sowie anderer Maßnahmen weiter erhöht.

Windows Update-Funktionen helfen, Systeme automatisch auf dem neuesten Sicherheitsstand zu halten. Security Notification Services informieren automatisch über die aktuellen Sicherheitsmeldungen zu Microsoft Produkten. Das Microsoft Security Tool Kit erhöht die IT-Sicherheit vorhandener und neuer Systeme. Und Security-Partner unterstützen bei der zuverlässigen Planung, Ausarbeitung und Umsetzung von spezifischen Unternehmens-Lösungen.

Baseline Analyse

Das Tool ***QFECheck.exe*** (beschrieben im Microsoft Knowledge-Base-Artikel-Q282784) listet die Hotfixes auf Windows 2000 auf:

```
C:\>qfecheck
Windows 2000 Hotfix Validation Report for \\SERVER
Report Date: 8/8/2002  12:00am
Current Service Pack Level:  Service Pack 2
Hotfixes Identified:
Q282784: Current on system.
Q282522: Current on system.
SP2SRP1: Current on system.
```

Unter ***http://www.microsoft.com/downloads*** ist das Tool QFECheck.exe (Q282784_W2K_spl_X86_EN.exe) für Windows 2000 verfügbar.

Der Microsoft Knowledge-Base-Artikel Q260910 gibt Informationen über die letzten Versionen der Service Packs, und der Artikel Q311401 beschreibt das Windows 2000 Security Rollup Package 1 (SRP1) vom Januar 2002. Bei dem Security Rollup Package für Windows 2000 handelt es sich um ein kumulatives Rollup aller Sicherheits-Updates, die seit der Veröffentlichung von Windows 2000 Service Pack 2 (SP2) angeboten wurden.

Download von Service Pack und Security Rollup Package für Windows 2000: http://www.microsoft.com/windows2000/downloads/servicepacks

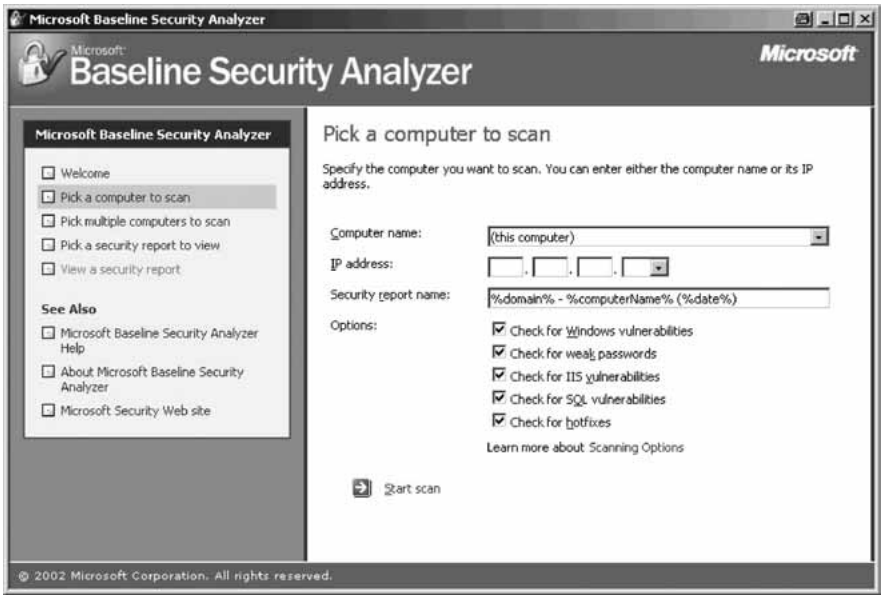
MICROSOFT BASELINE SECURITY ANALYZER (GUI)

Der Microsoft Baseline Security Analyzer (MBSA) ist ein grafisches Tool, mit dem Systeme auf Sicherheitslöcher und fehlende Service Packs und Hotfixes untersucht werden können.



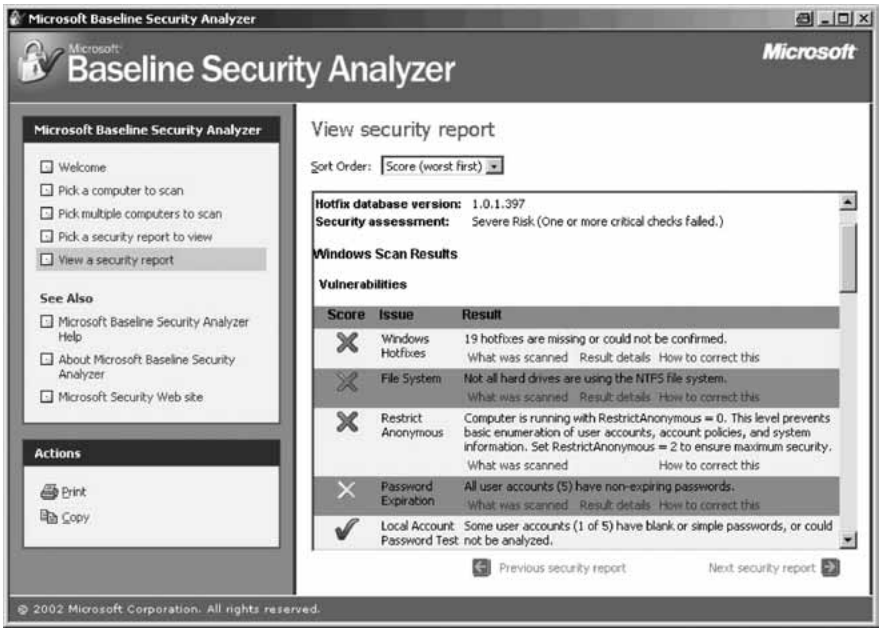
Folgende Aspekte werden analysiert:

- Windows und IIS Vulnerabilities
- Schwache Passwörter
- Überprüfen des Software Standes



Folgende Tool Scanning Options lassen sich wählen:

- IIS Checks
- SQL Checks
- Hotfix Checks
- Password Checks



Nach erfolgter Analyse des Systems wird ein Report mit Anzeige der Ergebnisse und Empfehlungen ausgegeben.

HINWEIS

Der Microsoft Baseline Security Analyzer (MBSA) Version 1.0 wird im Microsoft Knowledge-Base-Artikel Q320454 beschrieben.

MICROSOFT BASELINE SECURITY ANALYZER (CMD)

Das Programm ***MBSAcli.exe*** ist der Microsoft Baseline Security Analyzer als befehlszeilenorientierte Anwendung.

Optionen von MBSAcli.exe:

```
mbsacli.exe
Parameter List:
/c       domain\computer       Scan named computer.
/i       IP                    Scan named IP address.
/r       IP-IP                 Scan named IP addresses range.
/d       domain                Scan named domain.
/n       option                Select which scans to NOT
                               perform.
All checks are performed by default.
Valid values: "OS", "SQL", "IIS", "HotFix", "Password".
Can be concatenated with "+" (no spaces).
/o       filename              Output XML file name template.
Default: %domain% - %computername% (%date%).
/f       filename              Redirect output to a file.
/qp                            Don't display scan progress.
/qe                            Don't display  error list.
/qr                            Don't display  report list.
/e                             List errors from latest scan.
/l                             List all reports available.
/ls                            List reports from the latest scan.
/lr      filename              Display overview report.
/ld      filename              Display detailed report.
/?                             Display this help/usage.
```

Beispiele:

```
MBSACLI /n Password
MBSACLI /c MyDomain\MyComputer /n Password+Hotfix+SQL
MBSACLI /d MyDomain
MBSACLI /i 200.0.0.1
MBSACLI /r "200.0.0.1-200.0.0.50"
MBSACLI /l
MBSACLI /ld "Domain - Computer (03-01-2002 12-00 AM)"
MBSACLI /f "C:\results.txt"
```

Die Ausführung von MBSAcli.exe ohne Parameter prüft den lokalen Computer.

```
C:\Programme\Microsoft Baseline Security Analyzer>mbsacli
Microsoft Baseline Security Analyzer © 2002, Microsoft
Corporation. All rights reserved. Developed for Microsoft
Corporation by Shavlik Technologies, LLC www.shavlik.com
Version 1.0
Engine version 3.6.0.7
Hotfix version 3.65.0.1

Attempting to download the CAB from:
http://download.microsoft.com/download/xml/security/1.0/NT5/EN-
US/mssecure.cab
File was successfully downloaded.
Attempting to load .\mssecure.xml.
Using XML data version = 1.0.1.360  Last modified on 8/8/2002.
Scan performed Mon Aug 12 12:20:19 2002
Shavlik Network Security Hotfix Checker, Enterprise Edition,
3.70
Using XML data version = 1.0.1.360  Last modified on 8/8/2002.

Scanning...
[          ][..........] 1 of 1 computer scan(s) complete.
Scan Complete.

Computer Name,  IP Address,  Assessment,  Report Name
-----------------------------------------------------
Domain\SERVER, 10.1.1.1, Severe Risk, Domain-SERVER (08-08-2002
12-00 PM)
```

Das Tool sucht am lokalen Computer bzw. bei Servern im Netzwerk nach installierten Patches. Die Datei mssecure.xml (hier gekürzt) ist eine Informationsdatei im XML-Format für die Überprüfung des Systems:

```
<?xml version="1.0" ?>
<BulletinDatastore DataVersion="1.0.1.360"
LastDataUpdate="8/8/2002" SchemaVersion="1.0.0.11"
LastSchemaUpdate="6/6/2001" ToolVersion="3.32"
MBSAToolVer="1.0"
    MBSAToolURL="http://www.microsoft.com/technet/security/too
ls/Tools/MBSAhome.asp" RevisionHistory=".298 includes
various sqnumber updates">
<!--
Built for Microsoft by Shavlik Technologies. On the web at:
www.shavlik.com/security
    -->
<Bulletins>
  <Bulletin BulletinID="MS98-001" BulletinLocationID="73"
FAQLocationID="73" FAQPageName="FQ98-001"
    Title="Disabling Creation of Local Groups on a
    Domain by Non-Administrative Users"
DatePosted="1998/06/01" DateRevised="1999/03/24"
Supported="Yes" Summary="The ability for non-
    administrative users to create aliases on the
    domain could be abused if they create a large
    number of local groups in the domain and cause the
    size of the account database to grow without
    restrictions. Unlimited local group creation could
    crash the domain controller and lead to excessive
    network traffic due to the replication of local
    group information to backup domain controllers."
Issue="" ImpactSeverityID="0" PreReqSeverityID="0"
MitigationSeverityID="0" PopularitySeverityID="0">
    <BulletinComments />
<QNumbers>
      <QNumber QNumber="Q169556" />
    </QNumbers>
<Patches>
    <Patch PatchName="CREATALS_x86.exe"
PatchLocationID="619" SBID="0"
      SQNumber="Q169556" NoReboot="0">
        <gekürzt>
```

Die Tools *MBSAcli.exe* und *HFNetChk.exe* vergleichen die gefundenen Patches mit der XML-Datei mssecure.xml, die erstmals aus dem Internet geladen wird und dort ständig aktualisiert vorliegt. Diese XML-Datei enthält neben den aktuellen Versionsnummern der Patches auch ihre Prüfsummen, um so unzulässige Veränderungen zu erkennen.

http://www.aspheute.com/artikel/20010928.htm

MICROSOFT NETWORK SECURITY HOTFIX CHECKER

Das Programm HFNetChk.exe ist ein Kommandozeilen-orientiertes Tool zu Analyse von Hotfixes. Zahlreiche Parameter ermöglichen eine angepasste Analyse der Systeme.

Der Microsoft Knowledge-Base-Artikel Q303215 beschreibt das Microsoft Network Security Hotfix Checker Tool (HFNetChk.exe) und stellt den Download (Nshc332.exe) zur Verfügung. Zusätzliche Informationen sind in dem Artikel Q305385 (Frequently Asked Questions for Microsoft Network Security Hotfix Checker Tool) und Q306460 (HFNetChk.exe Returns NOTE Messages for Installed Patches) veröffentlicht.

Optionen von HFNetChk.exe:

```
hfnetchk.exe
[-h hostname]       NetBIOS Name
[-fh Hostfile]      NetBIOS Names in Datei
[-i ipaddress]      IP Adresse
[-fip ipfile]       IP Adressen in Datei
[-r range]          IP Adressen Bereich
[-d domainname]     Prüft eine ganze Domäne
[-n]                Prüft ein ganzes Subnetz
[-b]                Minimale Sicherheit (Baseline)
[-t threads]        Anzahl gleichzeitiger Prüfungen
[-o output]         Outputformat: wrap|tab
[-x datasource]     Pfad zur XML-Datei
[-z]                Keine Registry-Checks
[-v]                Verbose-Modus
[-s suppression]    1=NOTES  2=NOTES+WARNING
[-nosum]            Keine Checksummen-Prüfung
[-u username]       Anmeldebenutzername
[-p password]       Anmeldekennwort
[-f outfile]        Ausgabedatei
```

Beispiel: htnetchk.exe –nosum -f <ouputfile> -o tab

Die Checksummenüberprüfung wird abgeschaltet, um das Problem der Lokalisierung zu umgehen (eine Funktion die der MBSA nicht unterstützt!). Die Analyseergebnisse werden in eine Tabulator-getrennte Datei umgeleitet, die für den Import in eine Datenbank geeignet ist.

Beispiel einer Ausgabe von HFNetChk.exe:

```
C:\hfnetchk.exe
Microsoft Network Security Hotfix Checker, 3.32
Attempting to download the CAB from:
http://download.microsoft.com/download/xml/security/1.0/NT5/EN-
US/mssecure.cab
File was successfully downloaded.
Attempting to load U:\mssecure.xml.
Using XML data version = 1.0.1.360  Last modified on 8/8/2002.

Scanning SERVER
............
Done scanning SERVER
SERVER (10.1.1.1)

WINDOWS 2000 SP2

Warning
        The latest service pack for this product is not
installed.
Currently SP2 is installed. The latest service pack is SP3.
        Note            MS01-022        Q296441
        Patch NOT Found MS02-001        Q311401
        Patch NOT Found MS02-006        Q314147
        Patch NOT Found MS02-008        Q318203
        Patch NOT Found MS02-013        Q300845
        Patch NOT Found MS02-014        Q313829
        Patch NOT Found MS02-017        Q311967
        Patch NOT Found MS02-024        Q320206
        Patch NOT Found MS02-029        Q318138

INTERNET EXPLORER 6 GOLD

        Patch NOT Found MS02-009        Q318089
        Patch NOT Found MS02-023        Q321232
        Note           MS02-027     Q323889
```

Manuelles Updaten von Windows

Das Programm QChain.exe ermöglicht es, mehrere Hotfixes zu installieren und erfordert nur einen Reboot. Der Microsoft Knowledge-Base-Artikel Q296861 beschreibt die Funktionalität.

Optionen von QChain.exe :

```
qchain.exe
[logfilename]
[-z]                          Kein Reboot nach der Installation
[-m]                          Quiet mode
```

Beispiel einer Qchain.exe Ausgabe:

```
---- Old Information In The Registry ------
Source:C:\WINNT\inf\acpi.inf
Version: 5.0.2183.1
Destination:d:\ntsust\testregchech\1394.inf
Version: 5.0.2183.1

Source:C:\WINNT\inf\adm_mult.inf
Version: 5.0.2184.1
Destination:d:\ntsust\testregchech\1394.inf
Version: 5.0.2183.1

Source:C:\WINNT\inf\banshee.inf
Version: 5.0.2080.1
Destination:d:\ntsust\testregchech\1394.inf
Version: 5.0.2183.1

---- New Information In The Registry ------
Source:C:\WINNT\inf\adm_mult.inf
Version: 5.0.2184.1
Destination:d:\ntsust\testregchech\1394.inf
Version: 5.0.2183.1
```

Die Installation kann mit einer Stapeldatei ausgeführt werden:

```
@echo off
setlocal
set PATHTOFIXES= some path

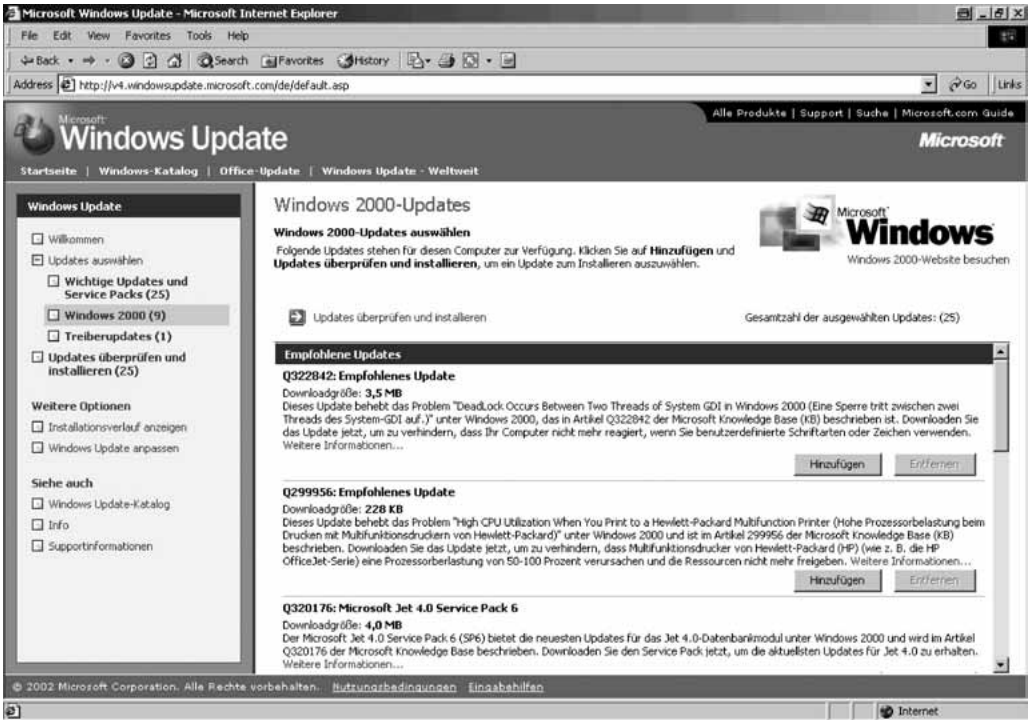
%PATHTOFIXES%\Q123456_w2k_sp2_x86.exe -z -m
%PATHTOFIXES%\Q123321_w2k_sp2_x86.exe -z -m
%PATHTOFIXES%\Q123789_w2k_sp2_x86.exe -z -m
%PATHTOFIXES%\qchain.exe
```

Nachdem alle Hotfixes installiert sind wird QChain.exe ausgeführt und ein Reboot des Computers durchgeführt.

Der Hotfix Installer kann ein Self-Extracting Package Program File (z.B. Qnnnnnn_w2k_spx_x86_en.exe) sein, oder eine Hotfix.exe (wenn alle Dateien eines Paketes entpackt sind).

Automatisches Updaten von Windows

Windows Update ist die Onlineerweiterung von Windows, dessen Inhalt regelmäßig aktualisiert wird. Dadurch können Systeme automatisch mit den aktuellsten Updates und Erweiterungen versorgt werden, und das Betriebssystem ist somit immer auf dem neuesten Stand.



Die Kategorien für Windows-Betriebssystemupdates enthalten unter anderem:

- **Wichtige Updates –** Sicherheitspatches und andere wichtige Updates, um Computer auf dem neuesten Stand zu halten und die Netzwerksicherheit zu gewährleisten.
- **Empfohlene Downloads –** aktuellste Windows und Internet Explorer Service-Packs und andere wichtige Updates.
- **Windows-Systemprogramme –** Programme, die die Leistung erhöhen, Upgrades vereinfachen und die Arbeit von Systemadministratoren erleichtern

Es besteht jederzeit die Möglichkeit, bestimmte Updates von der Windows Update-Website (***http://windowsupdate.microsoft.com***) zu installieren.

Systems Management Server
Der Systems Management Server (SMS) 2.0 ist eine zentralisierte, skalierbare Change- und Konfigurations-Managementlösung für Windows-basierende Desktops und Server. Die Funktionsmerkmale des zentralen Tools für die Softwaredistribution umfassen Hardware-Inventarisierung, Software-Inventarisierung und Software-Metering, Software-Verteilung und -Installation sowie Tools für die Problembehandlung auf Remotecomputern.

Das Programm **Systems Management Server Installer** ist Bestandteil des SMS und stellt eine grundlegende Paketierungs-Technologie und Mitschnittfunktionen zur Verfügung, mit der sich die Vorbereitungszeit für die Softwareverteilung verkürzen lässt.

SMS 2.0 Deploy Security Tool Kit Fixes:

http://www.microsoft.com/smserver/techinfo/deployment/20/deployosapps/smsseckit.asp

Deployment Guide:

http://www.microsoft.com/smserver/docs/sst2D.doc

SMS ermittelt die benötigten Security Fixes auf den Systemen. Im Systems Management Server 2.0 Administrator Handbuch im Kapiel 4 „Creating Your SMS Security Strategy" (***http://www.microsoft.com/technet/prodtechnol/sms/proddocs/smsadm/part1/smsad04.asp***) wird eingehend die Sicherung der SMS-Umgebung beschrieben.

Das **Microsoft Security Tool Kit** (http://www.microsoft.com/smserver/downloads/20/ tools/sectoolkit.asp) unterstützt die Sicherung einer Windows-Umgebung vor externen Attacken. Mit dem Systems Management Server 2.0 lassen sich die aktuellen Security Fixes verteilen.

http://www.microsoft.com/download/sms20/Install/2.1.1.0/NT45/EN-US/MSTImport.EXE

Checklisten

Windows 2000 Systemtools

Tools	Beschreibung	Quelle
WINVER.EXE	Zeigt als Pop-Up die Windows-version, Service Pack, etc.	Im Betriebssystem
OFECHECK.EXE	Listet die installierten Hotfixes	http://www.microsoft.com/downloads: Q282784_W2K_spl_X86_EN.exe für Windows 2000
HFNETCHK.EXE	Prüft und vergleicht Hotfixes	http://download.microsoft.com/download/win2000platform/Utility/3.3/NT45/EN-US/Nshc332.exe
MBSA.EXE und MBSACLI.EXE	Analysetool prüft Hotfixes und Servicepacks	http://download.microsoft.com/download/win2000platform/Install/1.0/NT5XP/EN-US/mbsasetup.msi
IISLOCK.EXE URLSCAN.EXE	Sichert den IIS	http://www.microsoft.com/technet/security/tools/locktool.asp
SECEDIT.EXE	Analyse und Konfiguration von Sicherheitseinstellungen	Im Betriebssystem
QCHAIN.EXE	Installation mehrer Hotfixes	http://download.microsoft.com/download/win2000platform/Utility/Q296861/NT45/EN-US/q296861_W2k_spl_x86_en.exe
WUAU22.MSI	Software Update Services Client	http://www.microsoft.com/windows2000/windowsupdate/sus/susdownload.asp
SUSSETUP.MSI	Software Update Services Server	http://www.microsoft.com/Windows2000/downloads/recommended/susserver/default.asp

Citrix Security Bulletin

Dateityp	Zugriffssteuerungslisten
CTX022138	HotFix CSGE100W001_MSI - Citrix Secure Gateway - Secure Ticket Authority v1_01 maintenance update to correct ticket validation weakness
CTX141262	Citrix Security Bulletin - Citrix NFuse Vulnerabilities
CTX204218	MetaFrame XP Advanced Concepts - Troubleshooting
CTX362806	Citrix Security Bulletin - Citrix Secure Gateway STA v1_00 ticket validation weakness
CTX403859	Security Attack Information
CTX448824	Citrix Security Bulletin - Citrix NFuse Vulnerabilities
CTX604940	Installing and Implementing WatchGuard ServerLock
CTX654124	Citrix Security Bulletin - Citrix MetaFrame Denial of Service Attack Vulnerabilities

Weitere Informationen zum Thema Security bei Citrix finden sich unter: ***http://knowledgebase.citrix.com***

IP-Ports

IP-Ports		Windows 2000 Dienst
21	TCP	FTP und FTP-Data (20)
23	TCP	Telnet
25	TCP	SMTP
42	TCP	WINS-Replikation
50		IPSEC (ESP)
51		IPSEC (AH)
53	UDP	DNS-Auflösung
53	TCP	DNS-Registrierung DNS-Zonentransfer
67	UDP	DHCP Lease (Server)
68	UDP	DHCP Lease (Client)
80		HTTP Citrix XML-Dienst
88	TCP + UDP	Kerberos
102	TCP	X.400 over TCP/IP
110	TCP	POP3
113	TCP	NNTP
135	TCP	[und Port > 1024] RPC (over IP) [und Port > 1024] Benutzerverwaltung [und Port > 1024] DHCP/DNS/WINS-Verwaltung [und Port > 1024] Systemmanager [und Port > 1024] Outlook
137	UDP	Windows-Anmeldung Computerbrowser Drucken WINS-Auflösung
137	TCP	WINS-Registrierung
138	UDP	Windows-Anmeldung Computerbrowser Dateireplikationsdienst Drucken
139	TCP	Windows-Anmeldung Dateizugriff Dateireplikationsdienst Benutzerverwaltung (SAM) Computerverwaltung Drucken Registrierungseditor Systemmonitor

143	TCP	IMAP
161		SNMP-Managementprotokoll
162		SNMP-Trap
359	TCP	Active Directory (LDAP)
443		HTTP-SSL Citrix SSL-Relay
445	TCP	Dateizugriff (Direct Host)
465	TCP	SMTP-SSL
500	UDP	IPSEC (IKE)
563	TCP	NNTP-SSL
631	TCP	Drucken (IPP)
636	TCP	Active Directory (LDAP-SSL)
993	TCP	IMAP-SSL
995	TCP	POP3-SSL
1433		SQL Server over TCP/IP MetaFrame XP-Server-Kommunikation mit Microsoft SQL
1494		ICA-Sitzungen
1604	UDP	ICA-Clients zu ICA-Browserdienst Gerichtete Server-zu-Server-UDP-Kommunikation
1701	UDP	VPN (L2TP)
1723	TCP	VPN (PPTP) und IP-Protokoll (47)
2512		Gerichtete MetaFrame XP-Server-zu-Server-UDP-Kommunikation
2513		Citrix Management Console zu MetaFrame XP-Server-Kommunikation
3268	TCP	Global Catalog (LDAP)
3269	TCP	Global Catalog (LDAP-SSL)
3389	TCP	RDP
9824	TCP	IIS-Administration

Betriebskonzept

Beispiel anhand einer Auswahl von System-Komponenten in einem Betriebskonzept

		Überprüfungs-prozess	Überwachungs-prozess	Aktualisierungs-prozess
➜	**Unternehmens-Router**			
	Betriebssystem-Version	❑	❑	❑
	Firmware-Version	❑	❑	❑
	Zugangskonfiguration für Administration	❑	❑	
	Zugangskonfiguration für externe Wartung	❑	❑	
	Sicherung der Zugangsart: Telnet/SNMP/SSH	❑	❑	
	Logging (syslog, propiritär)	❑	❑	
➜	**Unternehmens-Firewall**			
	Betriebssystem-Version	❑	❑	❑
	Firmware-Version	❑	❑	❑
	Zugangskonfiguration für Administration	❑	❑	
	Zugangskonfiguration für externe Wartung	❑	❑	
	Sicherung der Zugangsart: Telnet/SNMP/SSH	❑	❑	
	Logging (syslog, proprietär)	❑	❑	
	Port-Scan	❑	❑	
	IDS (Kopplung/Konfiguration/Messaging)	❑	❑	
➜	**Netzwerkkomponenten**			
	Betriebssystem-Version	❑	❑	❑
	Firmware-Version	❑	❑	❑
	Zugangskonfiguration für Administration	❑	❑	
	Zugangskonfiguration für externe Wartung	❑	❑	
	Sicherung der Zugangsart: Telnet/SNMP/SSH	❑	❑	
	Logging (syslog, proprietär)	❑	❑	
	Port-Scan	❑	❑	

➜	**Windows 2000**			
	Definition der Server-Rolle			
	Service Pack / Hotfixes / SRP	❑	❑	❑
	Passwörter	❑	❑	
	Services/Ports	❑		
	Virenscanner	❑	❑	❑
➜	**Terminal Services**			
	Security Template	❑	❑	
➜	**MetaFrame XP**		❑	❑
	XML-Service (Port: 80)			
	SNMP-Service (Port: 161/162)	❑	❑	
	Service Pack / Hotfixes	❑	❑	❑
	IMA-Service (Port: 2512/2513)	❑		
	Admin-Tools: CMC, Web-Console	❑		
➜	**Internet Information Service**			
	Service Pack / Hotfixes			
	Lock Down	❑	❑	
	Passwörter / Anmeldeprozess	❑	❑	❑
	Services/Ports	❑	❑	
➜	**SQL Server**			
	Passwörter / Anmeldeprozess	❑	❑	
➜	**Client-System**			
	Betriebssystemaktualisierung	❑	❑	❑
	Passwörter / Anmeldeprozess	❑	❑	
	Desktop/Personal-Firewall	❑	❑	❑
	ICA-Client Einstellung/Aktualisierung	❑	❑	❑
	Lokaler Virenscanner	❑	❑	❑

Windows-Dienste

Liste der Windows-Dienste (und Servicenamen).

Name des Dienstes	Servicename	Startart
Alerter	ALERTER	
Application Management	APPMGMT	
Boot Information Negotiation Layer	BINLSVC	
Certificate Services	CERTSVC	
ClipBook	CLIPSRV	
Cluster Service	CLUSSVC	
COM + Event System	EVENTSYSTEM	
Computer Browser	BROWSER	
DHCP Client	DHCP	
DHCP Server	DHCPSERVER	
Distributed File System	DFS	
Distributed Link Tracking Client	TRKWKS	
Distributed Link Tracking Server	TRKSVR	
Distributed Transaction Coordinator	MSDTC	
DNS Client	DNSCACHE	
DNS Server	DNS	
Event Log	EVENTLOG	
Fax Service	FAX	
File Replication	NTFRS	
File Server for Macintosh	MACFILE	
FTP Publishing Service	MSFTPSVC	
Gateway Service for Netware	NWCWORKSTATION	
IIS Admin Service	IISADMIN	
Indexing Service	CISVC	
Internet Authentication Service	IAS	
Internet Connection Sharing	SHAREDACCESS	
Intersite Messaging	ISMSERV	
IPSEC Policy Agent (IPSEC Service)	POLICYAGENT	
Kerberos Key Distribution Center	KDC	
Licence Logging Service	LICENSESERVICE	

Logical Disk Manager	DMSERVER	
Logical Disk Manager Administrative Service	DMADMIN	
Message Queuing	MSMQ	
Messanger	MESSENGER	
Net Logon	NETLOGON	
NetMeeting Remote Desktop Sharing	MNMSRVC	
Network Connections	NETMAN	
Network DDE	NETDDE	
Network DDE DSDM	NETDDEDSDM	
Network News Transfer Protocol (NNTP)	NNTPSVC	
NTLM Security Support Provider	NTLMSSP	
On-Line Presentation Broardcast	NSLSERVICE	
Performance Logs and Alerts	SYSMONLOG	
Plug and Play	PLUGPLAY	
Print Server for Macintosh	MACPRINT	
Print Spooler	SPOOLER	
Protected Storage	PROTECTEDSTORAGE	
QoS Admissin Control (RSVP)	RSVP	
QoS RSVP	RSVP	
Remote Access Auto Connection Manager	RASAUTO	
Remote Access Connection Manager	RASMAN	
Remote Procedure Call (RPC)	RPCSS	
Remote Procedure Call (RPC) Locator	RPCLOCATOR	
Remote Registry Service	REMOTEREGISTRY	
Remote Storage Engine	REMOTE_STORAGE_ENGINE	
Remote Storage File	REMOTE_STORAGE_FILE_SYSTEM _AGENT	
Remote Storage Media	REMOTE_STORAGE_SUBSYSTEM	
Remote Storage Notification	REMOTE_STORAGE_USER_LINK	
Removable Storage	NTMSSVC	
Routing and Remote Access	REMOTEACCESS	
RunAs Service	SECLOGON	
SAP Agent	NWSAPAGENT	

Security Accounts Manager	SAMSS	
Server	LANMANSERVER	
Simple Mail Transfer Protocol (SMTP)	SMTPSVC	
Simple TCP/IP Services	SIMPTCP	
Single Instance Groveler	GROVELER	
Site Server ILS Service	LDAPSVCX	
Smart Card	SCARDSVR	
Smart Card Helper	SCARDDRV	
SNMP Service	SNMP	
SNMP Trap Service	SNMPTRAP	
System Event Notification	SENS	
Task Scheduler	SCHEDULE	
TCP/IP NetBIOS Helper Service	LMHOSTS	
TCP/IP Print Server	LPDSVC	
Telephony	TAPISRV	
Telnet	TLNTSVR	
Terminal Services	TERMSERVICE	
Terminal Services Licensing	TERMSERVLICENSING	
Trivial FTP Deamon	TFTPD	
Uninterruptible Power Supply	UPS	
Utility Manager	UTILMAN	
Windows Installer	MSISERVER	
Windows Internet Name Service (WINS)	WINS	
Windows Management Instrumentation	WINMGMT	
Windows Management Instrumentation Driver Extension	WMI	
Windows Media Monitor Service	NSMONITOR	
Windows Media Program Service	NSPROGRAM	
Windows Media Station Service	NSSTATION	
Windows Media Unicast Service	NSUNICAST	
Windows Time	W32TIME	
Workstation	LANMANWORKSTATION	
World Wide Web Publishing Service	W3SVC	

Konfigurationsschritte (Windows 2000 Server)

Vorgehensschritte für die Konfiguration von Windows 2000 Server.

❑	Festplattenpartitionen mit NTFS formatieren
❑	Administratorkonto erhält ein starkes Kennwort
❑	Deaktivieren nicht benötigter Dienste
❑	Deaktivieren oder löschen nicht benötigter Konten
❑	Schützen von Dateien und Verzeichnissen
❑	Gastkonto deaktivieren
❑	Registrierung vor anonymem Zugriff schützen
❑	Anwenden entsprechender Registrierungs-ACLs
❑	Zugriff nur auf öffentliche LSA-Informationen (Local Security Authority)
❑	Richtlinien für stärkere Kennwörter
❑	Kontosperrungsrichtlinien festlegen
❑	Konfigurieren des Administratorkontos
❑	Entfernen aller nicht benötigten Dateifreigaben
❑	Festlegen der Dateifreigaben mit entsprechenden ACLs
❑	Installieren von Antivirensoftware und Antivirensoftware-Aktualisierungen
❑	Installieren des aktuellen Service Packs und Security Rollout Packs
❑	Installieren der entsprechenden Sicherheits-Hotfixes

Konfigurationsschritte (Internet Information Server)

Vorgehensschritte für die Konfiguration von IIS 5.0

❑	Festlegen geeigneter ACLs für virtuelle Verzeichnisse
❑	Festlegen geeigneter ACLs für die IIS-Protokolldateien
❑	Aktivieren der Protokollierung
❑	Deaktivieren oder Entfernen von Beispielanwendungen
❑	Entfernen des virtuellen Verzeichnisses „iisadmpwd"
❑	Entfernen nicht verwendeter Skriptzuordnungen

Citrix Web Server Debugging & Analysis Tool

Für die Ermittlung, ob das „Härten“ des Internet Information Server die Citrix- Komponenten beeinträchtigt, steht folgendes Tool zur Verfügung: Das *Citrix Web Server Debugging & Analysis Tool für NFuse Classic 1.7* ist in der Citrix Knowledge Base im Document CTX052061 beschrieben.

```
CITRIX® TECHNICAL SUPPORT
WEB SERVER DEBUGGING INFORMATION

This tool can be used to gather information about IIS web
servers in a Citrix environment serving any of the following
roles:
# NFuse Classic web server
# Citrix Secure Gateway Secure Ticket Authority
# MetaFrame XP server sharing XML Service port with IIS

The information reported below may be considered sensitive. To
protect the security of your web server, remove this file after
it has been used.
```

Das Tool ist ein Active Server Page (ASP) Script (debug.asp) und ermittelt die Einstellungen und Konfigurationen auf dem IIS (Internet Information Server) für folgende Komponenten:

- NFuse Classic Web Server
- Citrix Secure Gateway Secure Ticket Authority
- MetaFrame XP Server mit XML Service Port

Das ASP-Script wird in das NFuse-Verzeichnis des IIS kopiert und mit dem Web-Browser ausgeführt (z.B. http://WebServer/Citrix/NFuse17/debug.asp). Das Prüfungsergebnis wird in einer Webseite dargestellt. (Bekannte Probleme oder Fehlkonfigurationen werden in der Webseite als roter Text dargestellt!)

Folgende Einstellungen und Konfigurationen werden geprüft:

- Alle Webseiten, die Interfaces und die Dokument Root Directories
- Konfigurationsdetails von NFuse Classic
- Einstellungen der XML Services für IIS
- Einstellungen der CSG STA für IIS
- ASP Application Objekte und Variablen
- ASP Session Objekte und Variablen
- Client Web Browser Cookies (für den aktuellen Server)
- Alle IIS HTTP Server-Variablen

Auszug einer Systemprüfung und deren Ergebnisse:

CSG - SECURE TICKET AUTHORITY
Virtual directory /Scripts found at: c:\inetpub\scripts
CtxSta.dll: Found at c:\inetpub\scripts\CtxSta.dll
STA Configuration: c:\inetpub\scripts\CtxSta.config

```
[GlobalConfig]
UID=STA01
TicketVersion=10
TicketTimeout=100000
MaxTickets=100000
LogLevel=0
MaxLogCount=10
MaxLogSize=20
LogDir=C:\inetpub\scripts\
```

IIS settings analysis for /Scripts/CtxSta.dll:

- **Allow anonymous access:: False - Anonymous HTTP not allowed!** For the STA to operate, the /Scripts/CtxSta.dll URL must be available to anonymous users.
- **Script and executable permissions:: Execution not allowed!** For the STA to operate, the /Scripts folder must be granted "Scripts and executables" permission.
- **Require SSL:: True - SSL is required for the STA!** For the STA to operate, the /Scripts/CtxSta.dll URL must be available without requiring SSL (HTTPS) to the STA URL.
- **Require 128-bit SSL:: True - 128-bit SSL is required for the STA!** For the STA to operate, the /Scripts/CtxSta.dll URL must be available without requiring SSL (HTTPS) to the STA URL. WARNING: IIS may honor the 128-bit SSL option even when the above SSL option is set to false.

Cache ISAPI applications:: True - OK

HINWEIS
Nach dem Test und der Prüfung ist in jedem Fall das ASP-Skript (debug.asp) aus dem NFuse-Verzeichnis zu löschen – ein unberechtigter Zugriff auf dieses Tool gibt dem Angreifer sehr viele Systeminformationen!

Ressourcen

Weiterführende Literatur

Fuhrberg, K., Internet-Sicherheit, 2. akt. Auflage. Hanser Verlag, 2000

Gernert, C., Ahrend, N., IT-Management, System statt Chaos. Ein praxisorientiertes Vorgehensmodell. Oldenburg, 2001

Grundlegende Sicherheitscheckliste für Windows 2000 Server, Microsoft Corporation

Grundlegende Sicherheitscheckliste für Internet-Informationsdienste (IIS 5.0), Microsoft Corporation

Hegering, H.-G., Integriertes Management vernetzter Systeme. Konzepte, Architekturen und deren betrieblicher Einsatz. dpunkt-Verlag, 1999

IT-Security. IM – Fachzeitschrift für Information Management & Consulting, Heft 2. www.im-fachzeitschrift.de, Mai 2002

Network Management – Betriebshandbuch, Microsoft Corporation, Mai 2001

Microsoft SQL Server 2000-Betriebshandbuch, Kapitel 3, Security Administration, Microsoft Corporation

Microsoft Windows 2000 Sicherheit. Microsoft Press, 2000

Raepple M., Sicherheitskonzepte für das Internet, 2. überarb. Auflage. dpunkt Verlag 2001

Stephen A. Thomas, SSL & TLS Essentials: Securing the Web. Wiley, New York, March 2000

Strobel, S., Firewalls für das Netz der Netze. dpunkt Verlag, 1997

Windows 2000 Webserver – Empfohlene Vorgehensweisen für eine hohe Verfügbarkeit, von Tim Hodgkins. Microsoft Corporation, Oktober 2001

Weblinks

Microsoft

Microsoft Web Solution Plattform:
http://www.microsoft.com/germany/business
http://support.microsoft.com

MSDN Online:
http://www.microsoft.com/germany/msdn
http://msdn.microsoft.com

Microsoft TechNet Security:
http://www.microsoft.com/technet/security
http://www.microsoft.com/germany/themen/security

Microsoft SQL Server:
http://www.microsoft.com/technet/security

Citrix

Citrix Support:
http://www.citrix.com/support

Citrix Knowledge Base:
http://knowledgebase.citrix.com
http://www.knowledgecenter.citrix.com/ support/
security.asp

Software Downloads:
http://download.citrix.com

Project in a Box:
http://www.dabcc.com/projectinabox

Citrix Support Forum:
http://ctxex10.citrix.com/icaforum.nsf/($All)?OpenView

Sonstige

TheThin.net Support Portal:
http://www.thethin.net

SysInternals:
http://www.sysinternals.com

NTBugtraq:
http://www.ntbugtraq.com

Internet Security Systems:
http://www.iss.net

Artikel zu ASP:
http://www.aspheute.com/

SecurityFocus Online:
http://online.securityfocus.com

Institutionen zum Thema Sicherheit

TÜV Informationstechnik GmbH:
http://www.tuvit.de

ICSA ein Unternehmen der Gartner Group:
http://www.icsa.net

RFC (Request for Comments):
http://www.faqs.org/rfcs/index.html

IETF (Internet Engineering Task Force) IPsec:
http://www.ietf.org

IPv6/IPv4 Network Address and Protocol Translation:
http://trail.isi.edu/workshop2/fiuczynski/index.htm

CERT Coordination Center:
http://www.cert.org

Bundesamt für Sicherheit in der Informationstechnik:
http://www.bsi.de

IT-Sicherheitshandbuch
Handbuch für die sichere Anwendung der Informationstechnik
hrsgg. vom BSI, 1992
Bundesdruckerei
Zweigbetrieb Bonn, D-53175 Bonn
Tel.: (0228) 382020

IT-Grundschutzhandbuch
Standardsicherheitsmaßnahmen
Loseblattsammlung in drei Ordnern (inkl. CD-ROM)
ISBN 3-88784-915-9
Bundesanzeiger-Verlag
Postfach 10 05 34
D-50445 Köln
Tel.: (0221) 97668-200
Fax: (0221) 97668-278
E-Mail: bestellungen@bundesanzeiger.de

Inhalt

Einleitung und Überblick **3**

Was haben die Angreifer vor? 3
Die technische Ausgangslage 4
Was gilt es zu erreichen? 4
Sicherheitsanforderungen 4

Das Citrix-Gesamtsystem **6**

Citrix Systemkomponenten 6
MetaFrame XP 6
ICA-Client 6
NFuse Classic 6
Citrix Secure Gateway 7

Sicherheitsanforderungen an Citrix-Systeme 8
Kommunikation ICA-Clientgerät und NFuse Classic-Server 8
Risiken 9
Empfehlungen 9
Kommunikation NFuse Classic Server und MetaFrame-Server 10
Risiken 11
Empfehlungen 11
Kommunikation ICA-Client und MetaFrame-Server 11
Risiken 11
Empfehlungen 11

Sicherheitsprotokolle und Citrix Sicherheitskomponenten 12
SSL 12
TLS 17
Citrix SSL-Relay 17
ICA-Verschlüsselung (Citrix SecureICA) 18
Citrix Secure Gateway (CSG) 18

Sicherheitskonzeption **22**

SCHRITT 1: Planung 24
Sicherheitsstrategien, IT-Services und Security-Lösungen 24
Modelle 25
IT-Grundschutzhandbuch des BSI 25
ISO/IEC 17799 (BS 7799-1) 25
BS (British Standard) 7799-2 25
Common Body of Knowledge (CBK) General Model 25
IT Infrastructur Library (ITIL) 25
Microsoft Operations Framework (MOF) 26

SCHRITT 2: Analyse 27
Sicherheitsfaktoren 27
Mensch 27
Prozesse 27
Technologien 28
Aufspüren von Sicherheitslöchern 34
Port-Scan 34
Vulnerability-Scan 34
Password-Auditing 34

SCHRITT 3: Bewertung 35
Risikomanagement 35
Risikoanalyse 35

SCHRITT 4: Umsetzung 38
MetaFrame XP 38
Windows 2000 Server 38
Sicherheit für die Konfiguration von Computern 38
NFuse Classic und Secure Gateway Service 43
Internet Information Server 43
Deaktivieren nicht benötigter System-Dienste 49
Citrix Verwaltungswerkzeuge 50
Citrix Data Store 50
Citrix Management Console 50
Citrix Web Console 50
Citrix Network Manager 51
Sichere Server-zu-Server-Verbindungen 51

SCHRITT 5: Prüfen und überwachen 52

SCHRITT 6: Reaktion und Anpassungen 53

SCHRITT 7: Aktualisierung 54
Softwaremanagement 54
Allgemeine Vorgehensweise 54
Baseline Analyse 55
Manuelles Updaten von Windows 63
Automatisches Updaten von Windows 64
Systems Management Server 65

Checklisten **66**

Windows 2000 Systemtools 66
Citrix Security Bulletin 66
IP-Ports 67
Betriebskonzept 69
Windows-Dienste 71
Konfigurationsschritte (Windows 2000 Server) 74
Konfigurationsschritte (Internet Information Server) 74
Citrix Web Server Debugging & Analysis Tool 75

Ressourcen **77**

Weiterführende Literatur 77
Weblinks 78
Microsoft 78
Citrix 78
Sonstige 78



Worldwide Headquarters
Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309
USA
Tel: +1 (800) 393 1888
Tel: +1 (954) 267 3000
www.citrix.com

European Headquarters
Citrix Systems International GmbH
Rheinweg 9
8200 Schaffhausen,
Switzerland
Tel: +41 52 6 35 77-00
www.citrix.com

Citrix Systems GmbH
Airport Business Center
Am Söldnermoos 17
D-85399 Hallbergmoos
Munich, Germany
Tel: +49 (0)811 83-0000
www.citrix.de

Citrix Systèmes SARL
7, place de la Défense
92974 Paris la Défense 4 Cedex
France
Tel: +33 (0)1 49 00 33 00
www.citrix.fr

Northern European Headquarters
Citrix Systems UK Limited
Chalfont House
Chalfont Park, Gerrards Cross
Bucks SL9 6XA
United Kingdom
Tel: +44 (0) 1753 276 200
www.citrix.com

Asia Pacific Headquarters
Citrix Systems Australia Pty Ltd
State Forest Building
423 Pennant Hills Road
Pennant Hills NSW 2120
Sydney, Australia
Tel: +61 (0)2 9980 0800
www.citrix.com



© 2002 Citrix Systems, Inc. Alle Rechte vorbehalten. Citrix®, MetaFrame® und NFuse® sind Warenzeichen oder registrierte Warenzeichen von Citrix Systems, Inc. in den USA und/oder anderen Ländern. Windows®, Windows NT® und Active Directory® sind Warenzeichen oder registrierte Warenzeichen von Microsoft Corporation in den USA und anderen Ländern. Macintosh® ist registriertes Warenzeichen von Apple Computer, Inc. UNIX® ist registriertes Warenzeichen von The Open Group in den USA und anderen Ländern. Java™ ist Warenzeichen oder registriertes Warenzeichen von Sun Microsystems, Inc., in den USA und anderen Ländern. Alle übrigen Warenzeichen sind Eigentum ihrer jeweiligen Besitzer.

G-6095 09/02