System i

Sicherheit
System i und Internetsicherheit

Version 6 Release 1

System i

Sicherheit
System i und Internetsicherheit

Version 6 Release 1

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen", auf Seite 31 gelesen werden.

Diese Ausgabe bezieht sich auf Version 6, Release 1, Modifikation 0 von IBM i5/OS (Produktnummer 5761-SS1) und alle nachfolgenden Releases und Modifikationen, es sei denn, es erfolgen anders lautende Angaben in neuen Ausgaben. Diese Version kann nicht auf allen RISC-Modellen (RISC = Reduced Instruction Set Computer) ausgeführt werden. Auf CICS-Modellen ist sie nicht ausführbar.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM System i Security and Internet Security, Version 6 Release 1,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
SW TSC Germany
Kst. 2877
Februar 2008

Inhaltsverzeichnis

System i und Internetsicherheit

Die Internetanbindung des eigenen LAN verlangt von Ihnen eine erneute Bewertung Ihrer Sicherheitsanforderungen.

Mit den integrierten Softwarelösungen und der Sicherheitsarchitektur des Produkts IBM System i können Sie wirksame Abwehrmaßnahmen gegen potenzielle Sicherheitsfallen und Eindringlinge aus dem Internet errichten. Der Einsatz dieser Sicherheitsangebote garantiert, dass Ihre Kunden, Mitarbeiter und Geschäftspartner alle erforderlichen Geschäftsdaten in einer sicheren Umgebung abrufen können.

In der vorliegenden Themensammlung werden die allgemein bekannten Sicherheitsrisiken und der Zusammenhang zwischen diesen Risiken und Ihren Internetzielen und e-business Zielen erläutert. Hier erfahren Sie auch, wie die Risiken gegenüber den Vorteilen der verschiedenen Sicherheitsoptionen einzuschätzen sind, die vom System geboten werden, um diesen Risiken zu begegnen. Sie können selbst entscheiden, wie Sie diese Informationen für die Entwicklung eines für Ihr Unternehmen adäquaten Netzsicherheitsplans nutzen.

PDF-Datei für System i und Internetsicherheit

Sie können die vorliegenden Informationen über eine PDF-Datei anzeigen oder drucken.

Zum Anzeigen oder Herunterladen der PDF-Version dieses Dokuments wählen Sie System i und Internetsicherheit aus (ca. 456 KB).

Sie können auch die folgenden Referenzinformationen anzeigen oder herunterladen:
- Intrusion detection (ca. 285 KB). Sie können Richtlinien zur Erkennung von unbefugtem Zugriff erstellen, mit denen verdächtige Zugriffsereignisse (z. B. falsch erstellte IP-Pakete) geprüft werden, die über das TCP/IP-Netz übertragen werden. Sie können auch eine Anwendung erstellen, die die Prüfdaten analysiert und Berichte an den Sicherheitsadministrator sendet, wenn unbefugte Zugriffe über TCP/IP wahrscheinlich sind.
- Enterprise Identity Mapping (EIM) (ca. 1.954 KB). Enterprise Identity Mapping (EIM) ist ein Mechanismus für die Zuordnung von Personen oder Entitäten (z. B. Services) zu den entsprechenden Benutzeridentitäten in verschiedenen Benutzerregistern im gesamten Unternehmen.
- Einzelanmeldung (ca. 1.203 KB). Die Lösung für Einzelanmeldung reduziert die Anzahl der Anmeldungen, die ein Benutzer für den Zugriff auf mehrere Anwendungen und Systeme ausführen muss, sowie die Anzahl der Kennwörter.
- Planning and Setting Up System Security (ca. 3.992 KB). Planning and Setting Up System Security enthält Informationen zur effektiven und systematischen Planung der Sicherheit auf Systemebene.

PDF-Dateien speichern

So können Sie eine PDF-Datei auf Ihrer Workstation speichern, um diese anzuzeigen oder zu drucken:
1. Klicken Sie in Ihrem Browser mit der rechten Maustaste auf den PDF-Link.
2. Klicken Sie auf die Option zum lokalen Speichern der PDF-Datei.
3. Navigieren Sie zu dem Verzeichnis, in dem die PDF-Datei gespeichert werden soll.
4. Klicken Sie auf **Speichern**.

Adobe Reader herunterladen

Auf Ihrem System muss Adobe Reader installiert sein, damit Sie die PDF-Dateien anzeigen und drucken können. Sie können das Programm kostenlos von der Adobe-Website (www.adobe.com/products/acrobat/readstep.html)  herunterladen.

Zugehörige Konzepte
Intrusion detection
Enterprise Identity Mapping (EIM)
Einzelanmeldung
Planning and setting up system security

System i und Überlegungen zur Internetsicherheit

Die Sicherheitsprobleme im Zusammenhang mit dem Internet sind signifikant. Dieser Abschnitt bietet einen Überblick über die Sicherheitsfunktionen und -angebote von i5/OS.

Bei der Anbindung der System i-Plattform an das Internet betrifft normalerweise eine der ersten Fragen das Thema Sicherheit und Internet. Der vorliegende Abschnitt kann Ihnen bei der Beantwortung dieser Frage helfen.

Welche Informationen für Sie relevant sind, hängt davon ab, wie Sie das Internet nutzen möchten. Ihr erster Schritt besteht darin, den Benutzern Ihres internen Netzes den Zugriff auf das Web und Internet-E-Mail zu gewähren. Möglicherweise ziehen Sie ebenfalls in Erwägung, sensible Informationen von einem Standort an einen anderen zu übertragen. Schließlich planen Sie u. U. sogar, das Internet für E-Commerce zu nutzen oder ein Extranet zwischen Ihrem Unternehmen und Ihren Geschäftspartnern und Lieferanten aufzubauen.

Vor dem Einstieg ins Internet sollten Sie genau überlegen, was Sie tun möchten und wie Sie dabei vorgehen möchten. Die Entscheidungsfindung sowohl hinsichtlich Internetnutzung als auch Internetsicherheit kann eine komplizierte Angelegenheit sein.

Anmerkung: Wenn Sie mit der Terminologie zum Thema Sicherheit und Internet noch nicht vertraut sind, können Sie beim Durcharbeiten der vorliegenden Veröffentlichung die allgemeine Terminologie zum Thema Sicherheit hinzuziehen.

Sobald Sie sich darüber im Klaren sind, wie Sie das Internet für e-business nutzen möchten, und Sie die Sicherheitsprobleme sowie die verfügbaren Sicherheitstools, -funktionen und -angebote kennen, können Sie Ihre Sicherheitsrichtlinien und Sicherheitsziele entwickeln. Dabei spielen zahlreiche Faktoren eine Rolle. Wenn Sie mit Ihrem Unternehmen im Internet präsent sein möchten, spielen Ihre Sicherheitsrichtlinien eine entscheidende Rolle für die Wahrung der Sicherheit Ihrer Systeme und Ressourcen.

Sicherheitsmerkmale von i5/OS

Neben zahlreichen speziellen Sicherheitsangeboten zum Schutz Ihres Systems im Internet verfügt das Betriebssystem i5/OS über die folgenden Sicherheitsmerkmale:

- Integrierte Sicherheit, die im Vergleich zu Add-on-Sicherheitssoftwarepaketen anderer Systeme äußerst schwer zu umgehen ist.
- Objektbasierte Architektur, die das Erstellen und Verbreiten von Viren technisch schwierig macht. Auf einem Betriebssystem i5/OS kann eine Datei weder vorgeben, ein Programm zu sein, noch kann ein Programm ein anderes Programm ändern. Auf Grund der Integritätsmerkmale von i5/OS müssen für den Objektzugriff die vom System zur Verfügung gestellten Schnittstellen verwendet werden. Es besteht keine Möglichkeit, auf ein Objekt direkt über dessen Adresse im System zuzugreifen. Eine relative Adresse kann nicht in einen Zeiger verwandelt werden (d. h., es kann kein Zeiger konstruiert werden). Die Zeigermanipulation ist auf anderen Systemarchitekturen eine bei Hackern beliebte Methode.
- Flexibilität, die Ihnen ermöglicht, den Systemschutz so zu gestalten, dass er Ihren speziellen Anforderungen gerecht wird. Über den Security Planner können Sie feststellen, welche Sicherheitsempfehlungen für Ihre Sicherheitsbedürfnisse in Frage kommen.

Spezielle Sicherheitsangebote von i5/OS

Das Betriebssystem i5/OS hält auch zahlreiche spezielle Sicherheitsangebote bereit, mit denen Sie den Systemschutz bei der Internetanbindung verbessern können. Je nachdem, wie Sie das Internet nutzen, können Sie eines oder mehrere dieser Angebote nutzen:

- Virtuelles Privates Netzwerk (VPN) stellt eine Erweiterung des privaten Intranets eines Unternehmens auf ein öffentliches Netz wie das Internet dar. Ein VPN kann zur Herstellung einer sicheren privaten Verbindung genutzt werden, indem ein privater Tunnel über ein öffentliches Netz erstellt wird. VPN ist ein integriertes Feature des Betriebssystems i5/OS, das über die System i Navigator-Schnittstelle zugänglich ist.
- Paketregeln sind ein integriertes Feature des Betriebssystems i5/OS, das über die System i Navigator-Schnittstelle zugänglich ist. Sie können mit Hilfe dieses Features Regeln für IP-Paketfilter und die Netzwerkadresskonvertierung (Network Address Translation - NAT) konfigurieren, um den TCP/IP-Datenverkehr Ihres Systems zu steuern.
- Mit den SSL-Protokollen (Secure Sockets Layer) können Sie Anwendungen für SSL konfigurieren, um sichere Verbindungen zwischen Serveranwendungen und den entsprechenden Clients herzustellen. SSL wurde ursprünglich für sichere Web-Browser- und Serveranwendungen entwickelt, aber auch andere Anwendungen können für die Verwendung von SSL konfiguriert werden. Zahlreiche Anwendungen sind jetzt SSL-fähig, darunter der IBM HTTP-Server für i5/OS, System i Access für Windows, FTP (File Transfer Protocol), Telnet usw.

Zugehörige Konzepte

„Sicherheitsrichtlinien und Sicherheitsziele” auf Seite 6
Ihre Sicherheitsrichtlinien definieren, was Sie schützen möchten, und die Sicherheitsziele geben an, was von den Benutzern erwartet wird.

„Virtual Private Network für sichere private Kommunikation” auf Seite 28
Virtual Private Network (VPN), eine Erweiterung des Intranets eines Unternehmens auf das vorhandene Gerüst eines öffentlichen oder privaten Netzes, kann Ihnen helfen, vertraulich und sicher innerhalb Ihres Unternehmens zu kommunizieren.

„Szenario: e-business Pläne des Unternehmens JKL Toy” auf Seite 8
Das typische Szenario des Unternehmens JKL Toy, das beschlossen hat seine Unternehmensziele mit Hilfe des Internets zu erweitern, ist möglicherweise für Sie bei der Planung Ihres eigenen e-business sehr hilfreich.

Zugehörige Informationen

Verbindung zum Internet

eServer Security Planner

IP filtering and network address translation

Secure Sockets Layer

AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet

Internetsicherheit planen

Bei der Entwicklung Ihrer Internetnutzungspläne müssen Sie Ihren Sicherheitsbedürfnissen besondere Beachtung schenken.

Sie müssen detaillierte Informationen über Ihre Internetnutzungspläne zusammenstellen und Ihre interne Netzkonfiguration dokumentieren. Auf der Grundlage dieser Informationen können Sie Ihre Sicherheitsbedürfnisse genau ermitteln.

Sie müssen beispielsweise folgende Informationen dokumentieren und beschreiben:

- Ihre aktuelle Netzkonfiguration.
- Konfigurationsdaten für DNS (Domain Name System) und E-Mail-Server.

- Ihre Verbindung zum Internet-Service-Provider (ISP).
- Die Internetdienste, die Sie nutzen möchten.
- Die Internetdienste, die Sie anderen Internetbenutzern zur Verfügung stellen möchten.

Die Dokumentation derartiger Informationen hilft Ihnen dabei festzustellen, wo die Sicherheitsrisiken liegen und welche Maßnahmen Sie ergreifen müssen, um diese Risiken zu minimieren.

Beispiel: Sie möchten Ihren internen Benutzern gestatten, Telnet für die Verbindung zu den Hosts an einem bestimmten Forschungsstandort zu verwenden. Die internen Benutzer benötigen diesen Dienst für die Entwicklung neuer Produkte für Ihr Unternehmen. Sie haben jedoch eventuell Bedenken hinsichtlich vertraulicher Daten, die ungeschützt über das Internet transportiert werden. Das Abfangen und Benutzen dieser Daten durch die Konkurrenz könnte ein finanzielles Risiko für Ihr Unternehmen bedeuten. Nachdem Sie Ihre Anforderungen (Telnet) und die damit verbundenen Risiken (Preisgabe vertraulicher Informationen) festgestellt haben, können Sie entscheiden, welche zusätzlichen Sicherheitsmaßnahmen Sie implementieren müssen, um die Vertraulichkeit der Daten zu gewährleisten (wie Aktivierung von SSL (Secure Sockets Layer)).

Sicherheit durch mehrfache Abwehrstufen

Ihre Sicherheitsrichtlinien definieren, was Sie schützen möchten und was Sie von den Systembenutzern erwarten.

Ihre Sicherheitsrichtlinien bilden eine Basis für die Sicherheitsplanung beim Entwurf neuer Anwendungen oder der Erweiterung Ihres aktuellen Netzes. Sie beschreiben die Zuständigkeiten der Benutzer wie beispielsweise den Schutz vertraulicher Informationen und das Erstellen sicherer Kennwörter.

Anmerkung: Sie müssen für Ihr Unternehmen Sicherheitsrichtlinien erstellen, die die Risiken für Ihr internes Netz auf ein Minimum beschränken. Zahlreiche Risiken können mit Hilfe der internen Sicherheitseinrichtungen des Betriebssystems i5/OS minimiert werden, sofern diese richtig konfiguriert sind. Bei der Anbindung Ihres Systems an das Internet müssen Sie jedoch zusätzliche Maßnahmen ergreifen, um die Sicherheit Ihres internen Netzes auch weiterhin zu gewährleisten.

Der Internetzugriff zwecks Durchführung geschäftlicher Aktivitäten birgt zahlreiche Risiken. Beim Erstellen der Sicherheitsrichtlinien gilt es, zwischen dem Angebot an Diensten und der Kontrolle des Zugriffs auf Funktionen und Daten abzuwägen. Bei netzfähigen Computern ist die Wahrung der Sicherheit schwieriger, da der Übertragungskanal selbst bereits möglichen Attacken ausgesetzt ist.

Einige Internetdienste sind anfälliger für bestimmte Arten von Attacken als andere. Daher ist es besonders wichtig, dass Sie sich der Risiken eines jeden Dienstes, den Sie nutzen oder anbieten möchten, bewusst sind. Außerdem hilft Ihnen die Kenntnis möglicher Sicherheitsrisiken dabei, klare Sicherheitsziele festzulegen.

Das Internet bietet den verschiedensten Individuen die Gelegenheit, die Sicherheit der Kommunikation über das Internet zu bedrohen. In der folgenden Liste finden Sie einige der typischen Sicherheitsrisiken, denen auch Sie ausgesetzt sein können:

- **Passive Attacken**

  Bei einer passiven Attacke überwacht der Angreifer Ihren Datenaustausch auf dem Netz, um an geheime Informationen heranzukommen. Derartige Attacken können netzbasiert (Aufzeichnung der DFV-Verbindung) oder systembasiert (Ersetzen einer Systemkomponente durch ein trojanisches Pferd, das heimlich Daten erfasst) sein. Passive Attacken sind die Attacken, die am schwierigsten aufzudecken sind. Daher müssen Sie davon ausgehen, dass immer irgendjemand alles abhört, was Sie über das Internet senden.

- **Aktive Attacken**

  Bei einer aktiven Attacke versucht der Angreifer, Ihre Abwehrmaßnahmen zu durchbrechen und in Ihre Netzsysteme einzudringen. Es gibt zahlreiche Arten von aktiven Attacken:
  - Bei **Systemzugriffsversuchen** versucht der Angreifer, Sicherheitslücken zu finden, um Zugriff auf und Kontrolle über ein Client- oder ein Serversystem zu erhalten.
  - Beim **Spoofing** versucht der Angreifer, Ihre Abwehrmaßnahmen zu durchbrechen, indem er sich als vertrauenswürdiges System tarnt, oder Sie werden von einem Benutzer dazu überredet, ihm vertrauliche Informationen zu schicken.
  - Bei **Denial-of-Service-Attacken** versucht der Angreifer, Ihren Arbeitsablauf zu stören oder zu stoppen, indem er den Datenverkehr umleitet oder Ihr System mit Junk-Nachrichten bombardiert.
  - Bei **verschlüsselten Attacken** versucht der Angreifer, Ihre Kennwörter zu erraten oder zu stehlen, oder er verwendet spezielle Tools, mit denen er versucht, verschlüsselte Daten zu entschlüsseln.

Mehrfache Abwehrstufen

Da es potenzielle Internetsicherheitsrisiken auf verschiedenen Ebenen geben kann, müssen Sie Sicherheitsmaßnahmen ergreifen, die mehrfache Abwehrstufen umfassen. Im Allgemeinen sollten Sie sich vor der Internetanbindung nicht fragen, ob Sie Störversuchen oder Denial-of-Service-Attacken ausgesetzt sein werden, sondern davon ausgehen, dass Sie auf ein Sicherheitsproblem stoßen werden. Daher besteht die beste Verteidigung in einer durchdachten und proaktiven Offensive. Wenn Sie bei der Planung der Internetsicherheit den mehrstufigen Ansatz verwenden, ist sichergestellt, dass ein Angreifer, der eine Abwehrstufe überwunden hat, von einer nachfolgenden gestoppt wird.

Ihre Sicherheitsrichtlinien müssen Maßnahmen beinhalten, die Schutz auf den folgenden Ebenen des traditionellen Network-Computing-Modells bieten. Ganz allgemein ist bei der Planung der Sicherheitsmaßnahmen von unten (Sicherheit auf Systemebene) nach oben (Sicherheit auf Transaktionsebene) vorzugehen.

Sicherheit auf Systemebene
: Ihre Maßnahmen zum Systemschutz bilden die letzte Verteidigungslinie gegen ein internetbasiertes Sicherheitsproblem. Daher muss der erste Schritt beim Aufbau einer umfassenden Internetsicherheitsstrategie darin bestehen, einen wirksamen Basissystemschutz zu konfigurieren.

Sicherheit auf Netzebene
: Maßnahmen zur Netzsicherheit steuern Ihren Zugriff auf das Betriebssytem i5/OS und andere Systeme im Netz. Wenn Sie Ihr Netz mit dem Internet verbinden, müssen Sie sich vergewissern, dass Ihnen adäquate Sicherheitsmaßnahmen auf Netzebene zur Verfügung stehen, um die internen Netzressourcen vor unbefugtem Zugriff und Eindringen zu schützen. Eine Firewall ist die am weitesten verbreitete Methode zur Gewährleistung der Netzsicherheit. Ihr Internet-Service-Provider (ISP) kann ein wichtiger Bestandteil Ihres Netzsicherheitsplans sein. Ihre Methode zur Netzsicherung muss die vom ISP gebotenen Sicherheitsmaßnahmen umreißen, wie beispielsweise Filterregeln für die ISP-Routerverbindung sowie Sicherheitsvorkehrungen für das allgemein zugängliche Domain Name System (DNS).

Sicherheit auf Anwendungsebene
: Sicherheitsmaßnahmen auf Anwendungsebene steuern, wie Benutzer mit bestimmten Anwendungen interagieren können. Generell sollten Sie für alle benutzten Anwendungen Sicherheitseinstellungen konfigurieren. Besondere Aufmerksamkeit hinsichtlich der Sicherheit sollten Sie jedoch denjenigen Anwendungen und Diensten widmen, die Sie über das Internet nutzen oder selbst im Internet zur Verfügung stellen möchten. Diese Anwendungen und Dienste können besonders leicht von Unbefugten missbraucht werden, die eine Möglichkeit suchen, sich Zugriff auf Ihre Netzsysteme zu verschaffen. Die Sicherheitsmaßnahmen, für die Sie sich entscheiden, müssen sowohl die Sicherheitsrisiken auf der Serverseite als auch die auf der Clientseite abdecken.

Sicherheit auf Übertragungsebene
: Sicherheitsmaßnahmen auf Übertragungsebene schützen die Datenübertragung innerhalb eines Netzes und zwischen verschiedenen Netzen. Wenn Sie Daten über ein ungesichertes Netz wie das Internet übertragen, können Sie den Datenfluss zwischen Quelle und Ziel nicht steuern. Der

Datenverkehr fließt durch viele verschiedene Systeme, auf die Sie keinen Einfluss haben. Sofern Sie keine Sicherheitsmaßnahmen treffen, beispielsweise indem Sie Ihre Anwendungen für die Verwendung von SSL (Secure Sockets Layer) konfigurieren, kann jeder Ihre weitergeleiteten Daten einsehen und verwenden. Sicherheitsmaßnahmen auf Übertragungsebene schützen Ihre Daten, während sie zwischen den anderen geschützten Bereichen hin und her fließen.

Wenn Sie Ihre umfassenden Internetsicherheitsrichtlinien entwickeln, sollten Sie für jede einzelne Ebene eine Sicherheitsstrategie erstellen. Außerdem sollten Sie beschreiben, wie die einzelnen Strategien zusammenwirken, um so ein umfassendes Sicherheitsnetz für Ihre Geschäftsabläufe zur Verfügung zu stellen.

Zugehörige Konzepte

„Sicherheitsstufen als Voraussetzung für Internetzugang" auf Seite 10
Vor der Anbindung an das Internet sollten Sie entscheiden, welche Sicherheitsstufe Sie zum Schutz Ihres Systems benötigen.

„Optionen für Netzsicherheit" auf Seite 11
Wählen Sie zum Schutz der internen Ressourcen die geeigneten Sicherheitsmaßnahmen auf Netzebene aus.

„Optionen für Anwendungssicherheit" auf Seite 18
Ihnen stehen einige Optionen zur Verfügung, um den Internetsicherheitsrisiken für zahlreiche populäre Internetanwendungen und -dienste zu begegnen.

„Optionen für Übertragungssicherheit" auf Seite 24
Wenn die Daten über ein ungesichertes Netz wie das Internet übertragen werden, sollten Sie zum Schutz Ihrer Daten die geeigneten Sicherheitsmaßnahmen implementieren. Zu diesen Maßnahmen gehören SSL (Secure Sockets Layer), System i Access für Windows und VPN-Verbindungen (VPN - Virtual Private Network).

„Sicherheitsrichtlinien und Sicherheitsziele"
Ihre Sicherheitsrichtlinien definieren, was Sie schützen möchten, und die Sicherheitsziele geben an, was von den Benutzern erwartet wird.

„E-Mail-Sicherheit" auf Seite 21
Die Verwendung von E-Mail im Internet oder anderen ungesicherten Netzen birgt Sicherheitsrisiken, auch wenn das System über eine Firewall geschützt ist.

Zugehörige Verweise

 System i Security Guide for IBM i5/OS Version 5 Release 4

Sicherheitsrichtlinien und Sicherheitsziele

Ihre Sicherheitsrichtlinien definieren, was Sie schützen möchten, und die Sicherheitsziele geben an, was von den Benutzern erwartet wird.

Ihre Sicherheitsrichtlinien

Jeder Internetdienst, den Sie nutzen oder anbieten, birgt Risiken für Ihr System und das Netz, mit dem es verbunden ist. Sicherheitsrichtlinien bestehen aus einer Reihe von Regeln, die für das Arbeiten mit den Computer- und DFV-Ressourcen eines Unternehmens gelten. Diese Regeln umfassen Bereiche wie physische Sicherheit, Mitarbeitersicherheit, Verwaltungssicherheit und Netzsicherheit.

Ihre Sicherheitsrichtlinien definieren, was Sie schützen möchten und was Sie von den Systembenutzern erwarten. Sie bilden eine Basis für die Sicherheitsplanung beim Entwurf neuer Anwendungen oder der Erweiterung Ihres aktuellen Netzes. Sie beschreiben die Zuständigkeiten der Benutzer wie beispielsweise den Schutz vertraulicher Informationen und das Erstellen sicherer Kennwörter. Sie sollten ebenfalls beschreiben, wie die Effektivität der Sicherheitsmaßnahmen überwacht werden soll. Mit einer derartigen Überwachung können Sie feststellen, ob jemand versucht, Ihre Sicherheitsvorkehrungen zu umgehen.

Zur Entwicklung der Sicherheitsrichtlinien gehört, dass Sie Ihre Sicherheitsziele klar definieren. Nach der Erstellung von Sicherheitsrichtlinien müssen Sie entsprechende Maßnahmen ergreifen, um die enthaltenen

Regeln zur Anwendung zu bringen. Zu diesen Maßnahmen gehören die Mitarbeiterschulung und das Bereitstellen der erforderlichen Software und Hardware zur Durchsetzung der Regeln. Wenn Sie Änderungen an Ihrer Systemumgebung vornehmen, müssen Sie auch Ihre Sicherheitsrichtlinien aktualisieren. Dadurch ist sichergestellt, dass Sie alle neuen Risiken erfassen, die sich durch die Änderungen ergeben.

Ihre Sicherheitsziele

Wenn Sie Sicherheitsrichtlinien erstellen, müssen Sie klare Ziele vor Augen haben. Sicherheitsziele können einer oder mehreren der folgenden Kategorien angehören:

Ressourcenschutz
Ihre Ressourcenschutzmethode garantiert, dass nur berechtigte Benutzer auf Objekte im System zugreifen können. Die Fähigkeit, alle Arten von Systemressourcen zu schützen, gehört zu den Stärken des System i. Sie müssen die verschiedenen Kategorien von Benutzern, die auf Ihr System zugreifen können, sorgfältig definieren. Als Bestandteil Ihrer Sicherheitsrichtlinien müssen Sie ebenfalls definieren, welche Zugriffsberechtigungen Sie diesen Benutzergruppen erteilen möchten.

Authentifizierung
Die Gewissheit oder Prüfung, dass die Ressource (Mensch oder Maschine) am anderen Ende der Sitzung tatsächlich die ist, die zu sein sie vorgibt. Eine gründliche Authentifizierung schützt ein System vor dem Sicherheitsrisiko des betrügerischen Auftretens, wobei ein Absender oder Empfänger eine falsche Identität verwendet, um auf ein System zuzugreifen. Traditionell werden auf Systemen Kennwörter und Benutzernamen für die Authentifizierung verwendet; digitale Zertifikate können eine noch sicherere Authentifizierungsmethode darstellen, während sie außerdem zusätzliche Sicherheitsleistungen bieten. Wenn Sie Ihr System mit einem öffentlichen Netz wie dem Internet verbinden, gelten für die Benutzerauthentifizierung ganz neue Maßstäbe. Ein wichtiger Unterschied zwischen dem Internet und Ihrem Intranet besteht darin, dass Sie beim Intranet der Identität eines Benutzers, der sich anmeldet, eher trauen können. Daher sollten Sie ernstlich in Betracht ziehen, striktere Authentifizierungsmethoden als beim traditionellen Anmeldeverfahren mit Benutzername und Kennwort anzuwenden. Authentifizierte Benutzer können je nach Berechtigungsstufe unterschiedliche Zugangsberechtigungen haben.

Berechtigung
Die Gewissheit, dass eine Person oder ein Computer am anderen Ende der Sitzung berechtigt ist, die Anforderung auszuführen. Beim Erteilen einer Berechtigung wird festgelegt, wer oder was auf Systemressourcen zugreifen oder bestimmte Aktivitäten auf einem System ausführen darf. In der Regel erfolgt die Erteilung der Berechtigung im Zuge der Authentifizierung.

Integrität
Die Gewissheit, dass die ankommenden Informationen dieselben Informationen sind, die gesendet wurden. Damit Sie die Integrität verstehen, müssen Sie die Konzepte der Datenintegrität und Systemintegrität verstehen.

- **Datenintegrität**: Daten werden vor unbefugten Änderungen oder dem Vortäuschen einer anderen Identität geschützt. Datenintegrität schützt vor dem Sicherheitsrisiko der Manipulation, wobei jemand Informationen abfängt und ändert, für die er nicht berechtigt ist. Neben dem Schutz der Daten, die innerhalb Ihres Netzes gespeichert sind, sind möglicherweise zusätzliche Sicherheitsvorkehrungen erforderlich, um die Datenintegrität auch dann zu garantieren, wenn Daten aus ungesicherten Quellen auf Ihr System gelangen. Für Daten, die aus einem öffentlichen Netz auf Ihrem System ankommen, sind Sicherheitsvorkehrungen erforderlich, damit Sie die folgende Aufgaben erfüllen können:
  - Die Daten gegen Ausspionieren (Sniffing) und Interpretieren schützen, normalerweise durch Verschlüsselung.
  - Sicherstellen, dass die Übertragung nicht verändert wurde (Datenintegrität).
  - Beweisen, dass die Übertragung erfolgt ist (Unbestreitbarkeit). In Zukunft könnte das elektronische Äquivalent zu registrierter oder zertifizierter Mail erforderlich sein.
- **Systemintegrität**: Ihr System liefert konsistente und erwartete Ergebnisse mit erwartetem Durchsatz. Bei dem Betriebssystem i5/OS wird die Systemintegrität als Sicherheitskomponente

meist übersehen, da sie ein wesentlicher Bestandteil der i5/OS-Architektur ist. Die i5/OS-Architektur macht es beispielsweise einem Hacker extrem schwer, ein Betriebssystemprogramm zu imitieren oder zu ändern, wenn Sicherheitsstufe 40 oder 50 verwendet wird.

Unbestreitbarkeit
Der Beweis dafür, dass eine Transaktion stattgefunden hat oder dass Sie eine Nachricht gesendet oder empfangen haben. Die Unbestreitbarkeit wird unterstützt durch die Verwendung digitaler Zertifikate und der Kryptografie mit einem öffentlichen Schlüssel, um Transaktionen, Nachrichten und Dokumente zu signieren. Absender und Empfänger stimmen überein, dass der Austausch stattfindet. Die digitale Signatur auf den Daten bietet den erforderlichen Beweis.

Vertraulichkeit
Die Gewissheit, dass sensible Informationen vertraulich bleiben und für einen Lauscher unsichtbar sind. Vertraulichkeit ist entscheidend für die gesamte Datensicherheit. Das Verschlüsseln von Daten mit Hilfe digitaler Zertifikate und des Secure Socket Layer (SSL) oder einer VPN-Verbindung (VPN) unterstützt die Wahrung der Vertraulichkeit, wenn Daten über ungesicherte Netze übertragen werden. Ihre Sicherheitsrichtlinien sollten beschreiben, wie Sie die Vertraulichkeit sowohl für Informationen innerhalb Ihres Netzes als auch für Informationen, die Ihr Netz verlassen, gewährleisten möchten.

Prüfung sicherheitsrelevanter Aktivitäten
Die Überwachung sicherheitsrelevanter Ereignisse zur Erstellung eines Protokolls über erfolgreiche und nicht erfolgreiche (verweigerte) Zugriffe. Einträge über erfolgreiche Zugriffe geben Auskunft darüber, wer was auf Ihren Systemen tut. Einträge über nicht erfolgreiche (verweigerte) Zugriffe geben Auskunft darüber, dass entweder jemand versucht, Ihre Sicherheitsvorkehrungen zu durchbrechen oder jemand Probleme beim Zugriff auf Ihr System hat.

Zugehörige Konzepte

„System i und Überlegungen zur Internetsicherheit" auf Seite 2
Die Sicherheitsprobleme im Zusammenhang mit dem Internet sind signifikant. Dieser Abschnitt bietet einen Überblick über die Sicherheitsfunktionen und -angebote von i5/OS.

„Sicherheit durch mehrfache Abwehrstufen" auf Seite 4
Ihre Sicherheitsrichtlinien definieren, was Sie schützen möchten und was Sie von den Systembenutzern erwarten.

Digital Certificate Manager konfigurieren

Secure Socket Layer (SSL)

„Szenario: e-business Pläne des Unternehmens JKL Toy"
Das typische Szenario des Unternehmens JKL Toy, das beschlossen hat seine Unternehmensziele mit Hilfe des Internets zu erweitern, ist möglicherweise für Sie bei der Planung Ihres eigenen e-business sehr hilfreich.

Szenario: e-business Pläne des Unternehmens JKL Toy

Das typische Szenario des Unternehmens JKL Toy, das beschlossen hat seine Unternehmensziele mit Hilfe des Internets zu erweitern, ist möglicherweise für Sie bei der Planung Ihres eigenen e-business sehr hilfreich.

Das Unternehmen JKL Toy ist ein zwar kleiner, jedoch rasch wachsender Spielwarenhersteller. Der Firmenchef zeigt sich begeistert über das Wachstum des Unternehmens und darüber, wie die dadurch verursachten Gemeinkosten durch das neue Betriebssystem i5/OS in Grenzen gehalten werden können. Sharon Jones, Leiterin des Rechnungswesens, ist für die Systemverwaltung und -sicherheit verantwortlich.

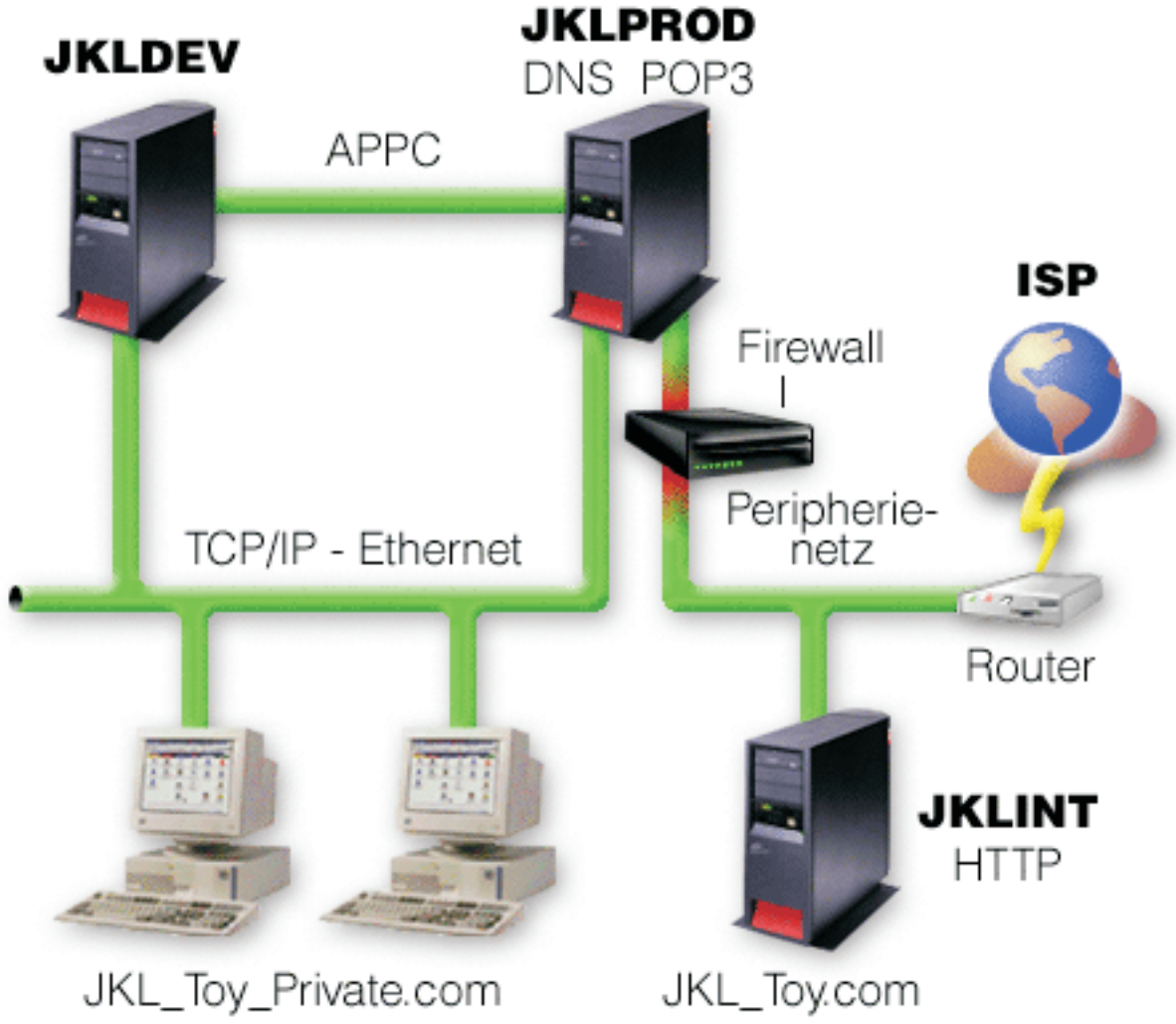
JKL Toy wendet seine Sicherheitsrichtlinien seit über einem Jahr erfolgreich auf die internen Anwendungen an. Das Unternehmen plant derzeit den Aufbau eines Intranets, um die gemeinsame Benutzung interner Informationen effektiver gestalten zu können. Es ist außerdem geplant, das Internet zur Förderung der Unternehmensziele einzusetzen. Zu diesen Zielen gehören auch Pläne, dem Unternehmen eine Marketingpräsenz im Internet zu verschaffen, einschließlich Onlinekatalog. Das Internet soll auch zur

Übertragung von sensiblen Informationen zwischen den Niederlassungen und der Firmenzentrale genutzt werden. Außerdem möchte das Unternehmen Mitarbeitern des Entwicklungslabors den Internetzugriff zu Forschungs- und Entwicklungszwecken gestatten. Schließlich sollen Kunden die Möglichkeit erhalten, die Website des Unternehmens für direkte Onlinebestellungen zu nutzen. Sharon Jones erstellt gerade einen Bericht über die potenziellen Sicherheitsrisiken derartiger Vorgänge und darüber, welche Sicherheitsmaßnahmen das Unternehmen ergreifen sollte, um diese Risiken zu minimieren. Frau Jones ist für die Aktualisierung der Sicherheitsrichtlinien und die Umsetzung der geplanten Sicherheitsmaßnahmen verantwortlich.

Dies sind die Ziele der verstärkten Internetpräsenz:

- Förderung des Firmenimages und der Firmenpräsenz im Rahmen einer umfassenden Werbekampagne
- Bereitstellung eines Onlineproduktkatalogs für Kunden und Vertriebsmitarbeiter
- Verbesserung des Kundendienstes
- Bereitstellung von E-Mail und Zugriff auf das World Wide Web für Mitarbeiter

Nachdem man sich davon überzeugt hat, dass das System über einen wirksamen Basissystemschutz verfügt, entscheidet sich JKL Toy dafür, ein Firewallprodukt für die Sicherheit auf Netzebene einzusetzen. Die Firewall schirmt das interne Netz vor zahlreichen potenziellen Internetrisiken ab. In der folgenden Abbildung ist die Internet- oder Netzkonfiguration des Unternehmens dargestellt.



Wie aus der Abbildung hervorgeht, verfügt das Unternehmen JKL Toy über zwei primäre Systeme. Ein System für Entwicklungsanwendungen (JKLDEV), das andere für Produktionsanwendungen (JKLPROD). Auf beiden Systemen werden unternehmenskritische Daten und Anwendungen verarbeitet. Daher gibt es Bedenken, die Internetanwendungen ebenfalls auf diesen Systemen auszuführen. Das Unternehmen hat entschieden, ein neues System (JKLINT) für die Ausführung dieser Anwendungen hinzuzufügen.

Das Unternehmen hat das neue System in ein Peripherienetz eingebunden und verwendet eine Firewall zwischen diesem und dem internen Hauptnetz, um das Unternehmensnetz und das Internet besser voneinander trennen zu können. Diese Trennung senkt die Internetrisiken, denen die internen Systeme ausgesetzt sind. Da das neue System ausschließlich als Internetserver fungiert, gestaltet sich außerdem die Verwaltung der gesamten Netzsicherheit weniger kompliziert.

Das Unternehmen führt zu diesem Zeitpunkt keine unternehmenskritischen Anwendungen auf dem neuen System aus. Während dieser Phase der e-business Planung stellt das neue System lediglich eine statische öffentliche Website zur Verfügung. Das Unternehmen möchte jedoch Sicherheitsmaßnahmen zum Schutz des Systems und der öffentlichen Website implementieren, um auf diese Weise Dienstunterbrechungen und andere mögliche Angriffe zu verhindern. Aus diesem Grund schützt das Unternehmen das System sowohl mit Regeln zur Paketfilterung und Netzwerkadresskonvertierung als auch mit strengen allgemeinen Sicherheitsmaßnahmen.

Je mehr anspruchsvollere allgemeine Anwendungen das Unternehmen in Zukunft entwickeln wird (beispielsweise eine E-Commerce-Website oder Extranetzugriff), desto ausgefeiltere Sicherheitsmaßnahmen wird es implementieren.

Zugehörige Konzepte

„Sicherheitsrichtlinien und Sicherheitsziele" auf Seite 6
Ihre Sicherheitsrichtlinien definieren, was Sie schützen möchten, und die Sicherheitsziele geben an, was von den Benutzern erwartet wird.

„System i und Überlegungen zur Internetsicherheit" auf Seite 2
Die Sicherheitsprobleme im Zusammenhang mit dem Internet sind signifikant. Dieser Abschnitt bietet einen Überblick über die Sicherheitsfunktionen und -angebote von i5/OS.

„Optionen für Netzsicherheit" auf Seite 11
Wählen Sie zum Schutz der internen Ressourcen die geeigneten Sicherheitsmaßnahmen auf Netzebene aus.

„Optionen für Übertragungssicherheit" auf Seite 24
Wenn die Daten über ein ungesichertes Netz wie das Internet übertragen werden, sollten Sie zum Schutz Ihrer Daten die geeigneten Sicherheitsmaßnahmen implementieren. Zu diesen Maßnahmen gehören SSL (Secure Sockets Layer), System i Access für Windows und VPN-Verbindungen (VPN - Virtual Private Network).

Sicherheitsstufen als Voraussetzung für Internetzugang

Vor der Anbindung an das Internet sollten Sie entscheiden, welche Sicherheitsstufe Sie zum Schutz Ihres Systems benötigen.

Ihre Maßnahmen zum Systemschutz bilden die letzte Verteidigungslinie gegen ein internetbasiertes Sicherheitsproblem. Der erste Schritt beim Aufbau einer umfassenden Internetsicherheitsstrategie muss darin bestehen, die grundlegenden i5/OS-Sicherheitseinstellungen sorgfältig zu konfigurieren. Gehen Sie folgendermaßen vor, um sicherzustellen, dass Ihr Systemschutz die Mindestanforderungen erfüllt:

- Setzen Sie die Sicherheitsstufe (Systemwert QSECURITY) auf 50. 50 ist die höchste Stufe des Integritätsschutzes, die für ein System in risikoreichen Umgebungen wie dem Internet empfohlen wird.

Anmerkung: Wenn Sie momentan mit einer niedrigeren Sicherheitsstufe als 50 arbeiten, müssen Sie Ihre Systemverwaltungsprozeduren oder Anwendungen möglicherweise aktualisieren. Lesen Sie die Informationen im Handbuch System i Security Reference, bevor Sie auf eine höhere Sicherheitsstufe wechseln.

- Setzen Sie Ihre sicherheitsrelevanten Systemwerte auf Werte, die mindestens den empfohlenen Einstellungen entsprechen. Mit dem System i Navigator-Sicherheitsassistenten können Sie die empfohlenen Sicherheitseinstellungen konfigurieren.
- Vergewissern Sie sich, dass keine Benutzerprofile - auch nicht die von IBM gelieferten - Standardkennwörter haben. Sie können dies mit dem Befehl ANZDFTPWD (Standardkennwörter analysieren) überprüfen.
- Verwenden Sie die Objektberechtigung, um Ihre wichtigen Systemressourcen zu schützen. Schränken Sie den Zugriff auf Ihr System ein, d. h., verweigern Sie standardmäßig jedem (PUBLIC *EXCLUDE) den Zugriff auf Systemressourcen wie Bibliotheken und Verzeichnisse. Gestatten Sie nur wenigen Benutzern Zugriff auf diese eingeschränkten Ressourcen. Die Zugriffsbeschränkung über Menüs reicht in einer Internetumgebung nicht aus.
- Sie müssen die Objektberechtigung auf Ihrem System definieren.

Zur Konfiguration dieser Mindestanforderungen an den Systemschutz können Sie entweder den eServer Security Planner oder den Sicherheitsassistenten, der über die System i Navigator-Schnittstelle verfügbar ist, verwenden. Der Security Planner gibt Ihnen, ausgehend von Ihren Antworten auf eine Reihe von Fragen, mehrere Sicherheitsempfehlungen. Anhand dieser Empfehlungen können Sie dann die Systemsicherheitseinstellungen konfigurieren, die Sie benötigen. Im Unterschied zum Security Planner konfiguriert der Assistent anhand dieser Empfehlungen die Systemsicherheitseinstellungen für Sie.

Zahlreiche Risiken können mit Hilfe der internen Sicherheitseinrichtungen von i5/OS minimiert werden, sofern diese richtig konfiguriert und verwaltet werden. Bei der Anbindung Ihres Systems an das Internet müssen Sie jedoch zusätzliche Maßnahmen ergreifen, um die Sicherheit Ihres internen Netzes auch weiterhin zu gewährleisten. Nachdem Sie sichergestellt haben, dass Sie einen allgemeinen Systemschutz installiert haben, können Sie mit der Konfiguration zusätzlicher Sicherheitsmaßnahmen als Bestandteil Ihres umfassenden Sicherheitsplans für die Internetnutzung beginnen.

Zugehörige Konzepte

„Sicherheit durch mehrfache Abwehrstufen" auf Seite 4
Ihre Sicherheitsrichtlinien definieren, was Sie schützen möchten und was Sie von den Systembenutzern erwarten.

Zugehörige Verweise

Security level system value

Security reference

Optionen für Netzsicherheit

Wählen Sie zum Schutz der internen Ressourcen die geeigneten Sicherheitsmaßnahmen auf Netzebene aus.

Für Verbindungen mit ungesicherten Netzen müssen Ihre Sicherheitsrichtlinien eine umfassende Schutzmethode beschreiben, die auch die Sicherheitsmaßnahmen beinhaltet, die Sie auf Netzebene implementieren werden. Die Installation einer Firewall gehört zu den besten Methoden, umfassende Sicherheitsmaßnahmen zu implementieren.

Ihr Internet-Service-Provider (ISP) kann ein wichtiger Bestandteil Ihres Netzsicherheitsplans sein. Ihre Methode zur Netzsicherung sollte die vom ISP gebotenen Sicherheitsmaßnahmen umreißen, wie beispielsweise Filterregeln für die ISP-Routerverbindung sowie Sicherheitsvorkehrungen für das allgemein zugängliche Domain Name System (DNS).

Obwohl eine Firewall sicherlich eine der wichtigsten Abwehrmaßnahmen innerhalb Ihres gesamten Sicherheitsplans darstellt, sollte sie doch nicht Ihre einzige Abwehrmaßnahme sein. Da es potenzielle Internetsicherheitsrisiken auf verschiedenen Ebenen geben kann, müssen Sie Sicherheitsmaßnahmen ergreifen, die mehrfache Abwehrstufen umfassen.

Wann immer Sie Ihr System oder Ihr internes Netz mit dem Internet verbinden, müssen Sie den Einsatz eines Firewallprodukts als wichtigste Abwehrmaßnahme in Betracht ziehen. Das Produkt IBM Firewall ist zwar nicht mehr für das Produkt i5/OS lieferbar, und und es gibt auch keine Produktunterstützung mehr, aber es stehen zahlreiche andere Produkte zur Auswahl.

Da kommerzielle Firewallprodukte eine breite Palette von Technologien für die Netzsicherheit bieten, entscheidet sich das Unternehmen JKL Toy für ein solches Produkt zum Schutz des Netzes. Weil die ausgewählte Firewall das Betriebssystem nicht schützt, entscheiden sie sich für die zusätzliche Sicherheitseinrichtung, die durch die Verwendung der i5/OS-Paketregeln bereitgestellt wird. Dadurch können Filter- und NAT-Regeln zur Steuerung des Datenverkehrs für den Internet-Server erstellt werden.

Zugehörige Konzepte

„Sicherheit durch mehrfache Abwehrstufen" auf Seite 4
Ihre Sicherheitsrichtlinien definieren, was Sie schützen möchten und was Sie von den Systembenutzern erwarten.

„Szenario: e-business Pläne des Unternehmens JKL Toy" auf Seite 8
Das typische Szenario des Unternehmens JKL Toy, das beschlossen hat seine Unternehmensziele mit Hilfe des Internets zu erweitern, ist möglicherweise für Sie bei der Planung Ihres eigenen e-business sehr hilfreich.

Intrusion detection

Zugehörige Informationen

Redbook: All You Need to Know When Migrating from IBM Firewall for AS/400

Firewalls

Eine Firewall ist eine Blockade zwischen einem sicheren internen Netz und einem ungesicherten Netz wie beispielsweise dem Internet.

Die meisten Unternehmen verwenden eine Firewall, um ein internes Netz sicher mit dem Internet zu verbinden, obwohl auch interne Netze untereinander mit Firewalls geschützt werden können.

Eine Firewall stellt einen kontrollierten einzelnen Berührungspunkt (einen sog. *Chokepoint*) zwischen Ihrem sicheren internen Netz und dem ungesicherten Netz dar. Die Firewall verfügt über folgende Funktionen:

- Benutzern in Ihrem internen Netz kann der Zugriff auf ausgewählte Ressourcen, die sich in dem externen Netz befinden, ermöglicht werden.
- Unbefugten Benutzern im externen Netz kann der Zugriff auf Ressourcen, die sich in Ihrem internen Netz befinden, verweigert werden.

Wenn Sie eine Firewall als Gateway zum Internet (oder einem anderen Netz) verwenden, verringern Sie das Risiko für Ihr internes Netz. Die Verwendung einer Firewall erleichtert außerdem die Verwaltung der Netzsicherheit, da Firewallfunktionen zahlreiche Direktiven Ihrer Sicherheitsrichtlinien ausführen.

Funktionsweise einer Firewall

Um sich die Funktionsweise einer Firewall zu veranschaulichen, stellen Sie sich vor, Ihr Netz sei ein Gebäude, zu dem Sie den Zutritt kontrollieren möchten. Ihr Gebäude kann ausschließlich über ein Foyer betreten werden. In diesem Foyer befinden sich eine Empfangsdame zur Begrüßung und Sicherheitspersonal zur Beobachtung von Besuchern, Videokameras zur Überwachung des Besucherverhaltens sowie Ausweisleser zur Authentifizierung der Besucher, die das Gebäude betreten.

Die genannten Maßnahmen können alle zusammen u. U. eine wirksame Zutrittskontrolle zu Ihrem Gebäude darstellen. Wenn es jedoch einer unbefugten Person gelingt, sich Zutritt zu verschaffen, haben Sie keine Möglichkeit, das Gebäude vor möglichen Taten dieses Eindringlings zu schützen. Wenn Sie jedoch die Bewegungen des Eindringlings überwachen, haben Sie die Chance, alle verdächtigen Handlungen festzustellen.

Komponenten einer Firewall

Eine Firewall ist ein Verbund aus Hardware und Software, die gemeinsam den unbefugten Zugriff auf einen Teil eines Netzes verhindern. Eine Firewall besteht aus den folgenden Komponenten:

- **Hardware**

  Die Firewall-Hardware besteht normalerweise aus einem separaten Computer oder einer dedizierten Einheit zur Ausführung der Softwarefunktionen für die Firewall.
- **Software**

  Die Firewall-Software stellt diverse Anwendungen zur Verfügung. Hinsichtlich der Netzsicherheit bietet eine Firewall Schutz mit Hilfe der folgenden Verfahren:
  - IP-Paketfilterung (Internet Protocol)
  - Netzwerkadresskonvertierung (NAT)
  - SOCKS-Server
  - Proxy-Server für diverse Dienste, wie z. B. HTTP, Telnet, FTP usw.
  - Mail Relay Services
  - Split Domain Name System (DNS)
  - Protokollierung
  - Echtzeitüberwachung

  Anmerkung: Einige Firewalls stellen VPN-Dienste (Virtual Private Network) zur Verfügung, so dass Sie verschlüsselte Sitzungen zwischen Ihrer Firewall und anderen kompatiblen Firewalls einrichten können.

Firewallverfahren verwenden

Sie können die Proxy-Server, SOCKS-Server oder NAT-Regeln der Firewall verwenden, um internen Benutzern den sicheren Zugriff auf Dienste im Internet zu gewährleisten. Die Proxy- und SOCKS-Server unterbrechen TCP/IP-Verbindungen an der Firewall, um interne Netzinformationen vor dem ungesicherten Netz zu verbergen. Die Server stellen ebenfalls zusätzliche Protokollierungsmöglichkeiten zur Verfügung.

Sie können NAT verwenden, um Internetbenutzern problemlosen Zugriff auf ein öffentliches System hinter der Firewall zu gewähren. Die Firewall schützt Ihr Netz insofern, als NAT Ihre internen IP-Adressen verbirgt.

Eine Firewall kann interne Informationen auch durch Bereitstellen eines eigenen DNS-Servers schützen. Tatsächlich gibt es in diesem Fall zwei DNS-Server: einer wird für Informationen über das interne Netz verwendet, und der andere auf der Firewall wird für Informationen über externe Netze und die Firewall selbst verwendet. Auf diese Weise können Sie den externen Zugriff auf Informationen auf Ihren internen Systemen steuern.

Bei der Definition einer Firewallstrategie könnte man davon ausgehen, dass es ausreicht, alles, was ein Risiko für das Unternehmen darstellt, zu verbieten, und alles andere zu erlauben. Da sich aber kriminelle Hacker ständig neue Angriffsmethoden ausdenken, müssen Sie bereits im Vorgriff Möglichkeiten schaffen, diese Angriffe zu verhindern. Wie in dem Gebäudebeispiel müssen Sie auch hier durch entsprechende Überwachung darauf achten, ob es Hinweise gibt, dass jemand einen Weg gefunden hat, Ihre Abwehr-

maßnahmen zu durchbrechen. Im Allgemeinen bringt die nachträgliche Schadensbeseitigung mehr Nachteile und Kosten mit sich als das vorsorgliche Verhindern eines Einbruchs.

Beim Einsatz einer Firewall besteht die beste Strategie darin, nur jene Anwendungen zuzulassen, die von Ihnen getestet wurden und die Sie für vertrauenswürdig erachten. Wenn Sie diese Strategie verfolgen, müssen Sie die Liste der Dienste, die auf Ihrer Firewall ausgeführt werden sollen, bis ins Kleinste definieren. Sie können jeden Dienst durch die Verbindungsrichtung (von innen nach außen oder von außen nach innen) charakterisieren. Sie sollten ebenfalls die Benutzer auflisten, die Sie für die einzelnen Dienste berechtigen möchten, sowie die Maschinen, die eine Verbindung für den jeweiligen Dienst herstellen können.

Welchen Schutz kann eine Firewall bieten?

Eine Firewall wird zwischen dem eigenen Netz und dem Verbindungspunkt zum Internet (oder zu einem anderen ungesicherten Netz) installiert. Anschließend können Sie die Anzahl der Eingangspunkte in Ihr Netz beschränken. Eine Firewall stellt einen einzelnen Berührungspunkt (einen sog. Chokepoint) zwischen Ihrem Netz und dem Internet dar. Da Sie nur einen Berührungspunkt haben, können Sie besser kontrollieren, welche Daten Sie ins Netz hineinlassen und welche heraus.

Eine Firewall erscheint nach außen mit einer einzelnen Adresse. Den Zugriff auf das ungesicherte Netz stellt die Firewall über Proxy- oder SOCKS-Server oder Netzwerkadresskonvertierung (NAT) zur Verfügung, wobei sie Ihre internen Netzwerkadressen verdeckt. Daher wird die Vertraulichkeit Ihres internen Netzes durch die Firewall gewahrt. Das vertrauliche Behandeln von Informationen über Ihr Netz ist eine Methode, mit der die Firewall einen Angriff in Form eines betrügerischen Auftretens (Spoofing) erschwert.

Eine Firewall ermöglicht Ihnen die Kontrolle des ein- und ausgehenden Datenverkehs, so dass die Gefahr einer Netzattacke minimiert wird. Eine Firewall filtert zuverlässig alle Daten, die an Ihrem Netz ankommen, so dass nur bestimmte Arten von Daten für bestimmte Ziele in das Netz eingeleitet werden. Auf diese Weise wird die Gefahr, dass jemand Telnet oder FTP (File Transfer Protocol) benutzt, um Zugriff auf Ihre internen Systeme zu erlangen, auf ein Minimum reduziert.

Welchen Schutz kann eine Firewall nicht bieten?

Wenn auch eine Firewall ganz erheblichen Schutz vor bestimmten Angriffen bietet, ist sie doch nur ein Teil Ihrer gesamten Sicherheitslösung. Eine Firewall kann beispielsweise nicht den notwendigen Schutz für Daten liefern, die Sie mittels Anwendungen wie SMTP-Mail (Simple Mail Transfer Protocol), FTP und Telnet über das Internet senden. Sofern Sie diese Daten nicht verschlüsseln, sind sie auf Ihrem Weg zum Empfänger für jedermann im Internet zugänglich.

i5/OS-Paketregeln

Mit den i5/OS-Paketregeln können Sie Ihr System schützen. Bei den Paketregeln handelt es sich um Funktionen des Betriebssystems i5/OS, auf die über die System i Navigator-Schnittstelle zugegriffen werden kann.

Mit den Paketregeln können Sie zwei der wichtigsten Netzsicherheitstechnologien konfigurieren, um den TCP/IP-Datenverkehr zu steuern:

- Netzwerkadresskonvertierung (NAT)
- IP-Paketfilterung

Da NAT und IP-Filterung integrierte Bestandteile Ihres Betriebssystems i5/OS sind, bieten sie Ihnen eine wirtschaftliche Möglichkeit zum Schutz Ihres Systems. In einigen Fällen reichen diese Sicherheitstechnologien völlig aus, so dass der Erwerb zusätzlicher Einrichtungen nicht notwendig ist. Diese Technologien bilden jedoch keine echte, funktionsfähige Firewall. Je nach Sicherheitsbedürfnissen und -zielen kann der IP-Paketschutz allein oder zusammen mit einer Firewall verwendet werden.

Anmerkung: Die absolute Sicherheit Ihres Systems sollte Vorrang vor den Kosten haben. Um sicherzugehen, dass Sie Ihrem Produktionssystem den maximal möglichen Schutz bieten, ist der Einsatz einer Firewall in Betracht zu ziehen.

Netzwerkadresskonvertierung und IP-Paketfilterung

Bei der Netzwerkadresskonvertierung (NAT) werden die IP-Quellen- oder die IP-Zieladressen von Paketen geändert, die durch das System transportiert werden. NAT ist eine Alternative zu den Proxy- und SOCKS-Servern einer Firewall, die stärkere Transparenz bietet. Außerdem kann NAT die Netzkonfiguration dadurch vereinfachen, dass auch Netze mit nicht kompatiblen Adressierungsstrukturen miteinander verbunden werden können. Folglich können NAT-Regeln so angewendet werden, dass ein Betriebssystem i5/OS als Gateway zwischen zwei Netzen fungieren kann, deren Adressierungsmethoden sich widersprechen oder nicht kompatibel sind. NAT kann auch eingesetzt werden, um die realen IP-Adressen eines Netzes zu verdecken, indem sie durch eine oder mehrere andere Adressen ersetzt werden. Da sich die IP-Paketfilterung und NAT gegenseitig ergänzen, werden sie häufig gemeinsam verwendet, um die Netzsicherheit zu erhöhen.

Die Verwendung von NAT kann auch den Betrieb eines öffentlichen Web-Servers hinter einer Firewall erleichtern. Öffentliche IP-Adressen für den Web-Server werden in persönliche interne IP-Adressen übersetzt. Dies verringert die Anzahl der erforderlichen registrierten IP-Adressen und minimiert die Auswirkungen auf das vorhandene Netz. NAT bietet internen Benutzern außerdem eine Möglichkeit, auf das Internet zuzugreifen, ohne ihre persönlichen internen IP-Adressen preiszugeben.

IP-Paketfilterung bietet die Möglichkeit, den IP-Datenverkehr anhand von Informationen in den Paketheadern selektiv zu blockieren oder zu schützen. Mit Hilfe des Internet-Setup-Assistenten im System i Navigator können Sie schnell und einfach Grundregeln für das Filtern konfigurieren, um unerwünschten Datenaustausch auf dem Netz zu blockieren.

IP-Paketfilterung kann für folgende Aufgaben eingesetzt werden:

- Erstellen einer Reihe von Filterregeln, um festzulegen, welchen IP-Paketen der Zugang zu Ihrem Netz gewährt und welchen er verweigert wird. Wenn Filterregeln erstellt werden, werden sie auf eine physische Schnittstelle (z. B. eine Token-Ring- oder Ethernet-Leitung) angewendet. Es besteht die Möglichkeit, die Regeln auf mehrere physische Schnittstellen oder unterschiedliche Regeln auf jede einzelne Schnittstelle anzuwenden.
- Erstellen von Regeln, um bestimmte Pakete zuzulassen oder abzulehnen, die auf den folgenden Headerdaten basieren:
  - IP-Zieladresse
  - Protokoll der IP-Quellenadresse (z. B. TCP und UDP)
  - Zielport (z. B. Port 80 für HTTP)
  - Quellenport
  - IP-Datagrammrichtung (ankommend oder abgehend)
  - Weitergeleitet oder lokal
- Verhindern, dass unerwünschter oder unnötiger Datenverkehr Anwendungen auf dem System erreicht. Sie können auch verhindern, dass Daten an andere Systeme weitergeleitet werden. Dies schließt ICMP-Pakete (Internet Control Message Protocol) der unteren Ebene (z. B. PING-Pakete) ein, für die kein spezieller Anwendungsserver erforderlich ist.
- Angeben, ob eine Filterregel, die einer Regel in einem Systemjournal entspricht, einen Protokolleintrag mit Informationen über Pakete erstellen soll. Nach Aufnahme der Informationen in ein Systemjournal kann der Protokolleintrag nicht mehr geändert werden. Das Protokoll ist ein ideales Tool zur Überwachung der Netzaktivität.

Mit Paketfilterregeln können Sie Ihre Computersysteme schützen, indem sie IP-Pakete entsprechend der von Ihnen definierten Kriterien ablehnen oder annehmen. Mit Hilfe von NAT-Regeln können Sie interne

Systeminformationen vor externen Benutzern verdecken, indem eine öffentliche IP-Adresse für Ihre interne IP-Adressinformationen eingesetzt wird. Obwohl IP-Paketfilter- und NAT-Regeln zu den wichtigsten Netzsicherheitstechnologien gehören, bieten sie dennoch nicht das Maß an Sicherheit, das ein voll funktionsfähiges Firewallprodukt bieten kann. Sie sollten Ihre Sicherheitsanforderungen und Sicherheitsziele sorgfältig analysieren, wenn es darum geht, sich zwischen einem vollständigen Firewallprodukt und den i5/OS-Feature Paketregeln zu entscheiden.

Zugehörige Konzepte

Network address translation (NAT)

IP packet filtering

Erkennung von unbefugtem Zugriff

Erkennung von unbefugtem Zugriff bedeutet, dass Informationen über unbefugte Zugriffsversuche und Angriffe vom TCP/IP-Netz aus zusammengestellt werden. In Ihren allgemeinen Sicherheitsrichtlinien wird es einen Abschnitt zur Erkennung von unbefugtem Zugriff geben.

Der Begriff *Erkennung von unbefugtem Zugriff* wird in der i5/OS-Dokumentation mit zwei Bedeutungen verwendet. Bei der ersten Bedeutung bezieht sich die Erkennung von unbefugtem Zugriff auf die Verhinderung und Erkennung von Sicherheitsrisiken. Es könnte, z. B., sein, dass ein Hacker versucht, unter Verwendung einer ungültigen Benutzer-ID in das System einzudringen, oder dass ein unerfahrener Besucher mit einer zu hohen Berechtigungsstufe wichtige Objekte in den Systembibliotheken ändert.

Bei der zweiten Bedeutung bezieht sich dieser Begriff auf die neue Funktion zur Erkennung von unbefugtem Zugriff, die anhand bestimmter Richtlinien verdächtigen Datenverkehr auf dem System überwacht. Sie können Richtlinien zur Erkennung von unbefugtem Zugriff erstellen, mit denen verdächtige Zugriffsereignisse geprüft werden, die über das TCP/IP-Netz übertragen werden.

i5/OS-Netzsicherheitsoptionen auswählen

Sie müssen die Optionen für Netzsicherheit entsprechend Ihrer Internetnutzungspläne auswählen.

Lösungen für die Netzsicherheit, die vor unbefugtem Zugriff schützen, basieren in der Regel auf Firewalls. Sie können sich für ein mit allen Funktionen ausgestattetes Firewallprodukt als Schutz für Ihr System entscheiden oder spezielle Netzsicherheitstechnologien als Bestandteil der TCP/IP-Implementierung von i5/OS aktivieren. Diese Implementierung besteht aus dem Feature Paketregeln (enthält IP-Filterung und NAT) und dem Feature HTTP für i5/OS, ein Lizenzprogramm für Proxy-Server.

Ob Sie sich für das Feature Paketregeln oder eine Firewall entscheiden, hängt von Ihrer Netzumgebung, Ihren Zugriffsbedürfnissen und Sicherheitsbedürfnissen ab. Wann immer Sie Ihr System oder Ihr internes Netz mit dem Internet oder einem anderen nicht gesicherten Netz verbinden, müssen Sie den Einsatz eines Firewallprodukts als wichtigste Abwehrmaßnahme in Betracht ziehen.

Eine Firewall ist in diesem Fall deshalb vorzuziehen, weil es sich bei einer Firewall normalerweise um eine dedizierte Hardware- und Softwareeinheit mit einer begrenzten Anzahl von Schnittstellen für den externen Zugriff handelt. Wenn Sie die TCP/IP-Technologien von i5/OS für den Internetzugriffsschutz einsetzen, verwenden Sie eine gängige Datenverarbeitungsumgebung mit unzähligen Schnittstellen und Anwendungen, die für den externen Zugriff offen sind.

Anmerkung: Möglicherweise möchten Sie eine Firewall und die integrierten i5/OS-Netzsicherheitstechnologien verwenden. Diese Maßnahme schützt Ihr System vor internen Attacken (hinter der Firewall) und vor Attacken, die eventuell Ihre Firewall aufgrund fehlerhafter Konfiguration oder aus anderen Gründen überwinden.

Der Unterschied ist aus zahlreichen Gründen von Bedeutung. Beispiel: Ein dediziertes Firewallprodukt stellt keinerlei weitere Funktionen oder Anwendungen außer den von der Firewall selbst benötigten zur Verfügung.

Folglich kann ein Angreifer, der die Firewall erfolgreich umgeht und somit auf sie zugreifen kann, nicht viel ausrichten. Wenn ein Angreifer jedoch die TCP/IP-Sicherheitsfunktionen auf Ihrem System umgeht, hat er potenziell Zugriff auf eine Vielzahl nützlicher Anwendungen, Dienste und Daten. Der Angreifer kann diese dann benutzen, um das System selbst zu zerstören oder Zugriff auf andere Systeme in Ihrem internen Netz zu erlangen.

Wie bei allen anderen die Sicherheit betreffenden Entscheidungen, müssen Sie auch hier Kosten und Nutzen gegeneinander abwägen. Sie müssen Ihre Unternehmensziele analysieren und sich zwischen den Risiken, die Sie eingehen möchten, und den Kosten, die die Schutzmaßnahmen zur Minimierung dieser Risiken verursachen, entscheiden.

Die folgende Tabelle enthält Informationen darüber, wann die TCP/IP-Sicherheitseinrichtungen angebracht sind und wann eine mit allen Funktionen ausgestattete Firewalleinheit vorzuziehen ist. Mit Hilfe dieser Tabelle können Sie feststellen, ob Sie zum Schutz Ihres Netzes und Ihrer Systeme eine Firewall, die TCP/IP-Sicherheitseinrichtungen oder eine Kombination aus beiden verwenden müssen.

Sicherheitstechnologie	Verwendung der TCP/IP-Technologie von i5/OS	Verwendung einer mit allen Funktionen ausgestatteten Firewall
IP-Paketfilterung	• Zusätzlicher Schutz für ein einzelnes Betriebssystem i5/OS, z. B. ein allgemein zugänglicher Web-Server oder ein Intranetsystem mit sensiblen Daten. • Schutz für ein Teilnetz eines unternehmensweiten Intranets, wenn das Betriebssystem i5/OS als Gateway (gewöhnlicher Router) für das restliche Netz fungiert. • Steuerung der Kommunikation mit einem vertrauenswürdigen Partner über ein privates Netz oder ein Extranet, wobei das Betriebssystem i5/OS als Gateway fungiert.	• Schutz eines unternehmensweiten Netzes vor dem Internet oder anderen ungesicherten Netzen, mit denen das eigene Netz verbunden ist. • Schutz eines großen Teilnetzes mit starkem Netzverkehr vor dem restlichen unternehmensweiten Netz.
Netzwerkadresskonvertierung (NAT)	• Möglichkeit, zwei private Netze zu verbinden, deren Adressierungsstrukturen nicht kompatibel sind. • Verbergen von Adressen in einem Teilnetz gegenüber einem weniger vertrauenswürdigen Netz.	• Verbergen der Adressen von Clients, die auf das Internet oder ein anderes ungesichertes Netz zugreifen. Verwendung als Alternative zu Proxy- und SOCKS-Servern. • Bereitstellung von Diensten eines Systems in einem privaten Netz für Clients im Internet.
Proxy-Server	• Weiterleitung für ferne Standorte in einem unternehmensweiten Netz, wenn eine zentrale Firewall Zugriff auf das Internet bietet.	• Weiterleitung für ein vollständiges unternehmensweites Netz beim Zugriff auf das Internet.

Zugehörige Verweise

IP filtering and network address translation

HTTP-Server für i5/OS

Zugehörige Informationen

AS/400 Internet Scenarios: A Practical Approach

Optionen für Anwendungssicherheit

Ihnen stehen einige Optionen zur Verfügung, um den Internetsicherheitsrisiken für zahlreiche populäre Internetanwendungen und -dienste zu begegnen.

Sicherheitsmaßnahmen auf Anwendungsebene steuern, wie Benutzer mit bestimmten Anwendungen interagieren können. Generell müssen Sie für alle benutzten Anwendungen Sicherheitseinstellungen konfigurieren. Besondere Aufmerksamkeit hinsichtlich der Sicherheit müssen Sie jedoch denjenigen Anwendungen und Diensten widmen, die Sie über das Internet nutzen oder selbst im Internet zur Verfügung stellen möchten. Diese Anwendungen und Dienste können besonders leicht von Unbefugten missbraucht werden, die eine Möglichkeit suchen, sich Zugriff auf Ihre Netzsysteme zu verschaffen. Die Sicherheitsmaßnahmen, die Sie verwenden, müssen sowohl die Sicherheitsrisiken auf der Serverseite als auch die auf der Clientseite abdecken.

Es ist zwar wichtig, alle von Ihnen benutzten Anwendungen zu schützen, doch spielen die Sicherheitsmaßnahmen bei der Implementierung der Gesamtheit Ihrer Sicherheitsrichtlinien nur eine kleine Rolle.

Zugehörige Konzepte

„Sicherheit durch mehrfache Abwehrstufen" auf Seite 4
Ihre Sicherheitsrichtlinien definieren, was Sie schützen möchten und was Sie von den Systembenutzern erwarten.

Sicherheit für Web-Serving

Wenn Sie Besuchern Zugriff auf Ihre Website bieten, lassen Sie Informationen über den Aufbau der Site und die Codierung, mit der die Seite generiert wurde, außen vor. Der Besuch Ihrer Seite muss einfach, schnell und reibungslos erfolgen; die Verarbeitung, die dahinter steht, soll hinter den Kulissen ablaufen.

Als Administrator müssen Sie sicherstellen, dass Ihre Sicherheitsmaßnahmen keine negativen Auswirkungen auf die Website haben und dass über diese Sicherheitsmaßnahmen die gewählten Sicherheitsmodelle implementiert werden. Dazu müssen Sie die entsprechenden Sicherheitseinrichtungen, die in den IBM HTTP-Server für i5/OS integriert sind, auswählen.

Informationen dazu, wie mit Authentifizierung, Zugriffssteuerung und Verschlüsselung die Sicherheitseinrichtungen implementiert werden, finden Sie im Kapitel über das Einrichten von Sicherheit im IBM HTTP Server (powered by Apache) Redbook. 

HTTP (Hypertext Transfer Protocol) bietet Ihnen zwar die Möglichkeit, Daten anzuzeigen, aber nicht die Möglichkeit, Daten in einer Datenbankdatei zu ändern. U. U. müssen Sie jedoch einige Anwendungen erstellen müssen, für die eine Datenbankdatei aktualisiert werden muss. Es kann beispielsweise sein, dass Sie Formulare erstellen möchten, mit denen eine i5/OS-Datenbank aktualisiert wird, nachdem diese Formulare vom Benutzer ausgefüllt wurden. Dazu können Sie die CGI-Programme (Common Gateway Interface) verwenden.

Proxy-Server ist eine weitere Sicherheitseinrichtung, die verwendet werden kann. Der Proxy-Server empfängt Anforderungen, die an andere Server gerichtet sind, dann führt er die Anforderungen aus, leitet sie weiter, leitet sie um oder weist sie zurück.

Der HTTP-Server stellt ein Zugriffsprotokoll zur Verfügung, mit dessen Hilfe Sie sowohl Zugriffe als auch Zugriffsversuche auf den Server überwachen können.

Außer CGI-Programmen können Sie auch Java-Programmierung auf Ihren Webseiten verwenden. Bevor Sie auf Ihren Webseiten auch Java einsetzen, müssen Sie sich über die Java-Sicherheit im Klaren sein.

Zugehörige Konzepte

„Java-Internetsicherheit"
In den IT-Umgebungen von heute nimmt die Java-Programmierung mehr und mehr zu. Sie sollten sich auch auf die Handhabung der Sicherheitsprobleme vorbereiten, die im Zusammenhang mit Java auftreten können.

Zugehörige Informationen

Proxy server types and uses for HTTP Server (powered by Apache)

Security tips for HTTP Server

Common Gateway Interface

Java-Internetsicherheit

In den IT-Umgebungen von heute nimmt die Java-Programmierung mehr und mehr zu. Sie sollten sich auch auf die Handhabung der Sicherheitsprobleme vorbereiten, die im Zusammenhang mit Java auftreten können.

Obwohl eine Firewall vor den allgemeinen Internetsicherheitsrisiken schützt, bietet sie doch keinen Schutz vor zahlreichen Risiken, die die Verwendung von Java mit sich bringt. Ihre Sicherheitsrichtlinien sollten Einzelheiten darüber enthalten, wie das System in drei kritischen Bereichen geschützt werden kann, die für Java von Belang sind: Anwendungen, Applets und Servlets. Sie sollten auch mit dem Zusammenwirken von Java und Ressourcenschutz hinsichtlich der Authentifizierung und Berechtigung für Java-Programme vertraut sein.

Java-Anwendungen

Als Programmiersprache verfügt Java über einige Merkmale, die Java-Programmierer vor unbeabsichtigten Fehlern bewahren, die Integritätsprobleme verursachen können. (Andere Programmiersprachen, die normalerweise für PC-Anwendungen verwendet werden, wie C oder C++, bieten in dieser Hinsicht einen weniger starken Schutz als Java.) In Java müssen beispielsweise Eingaben ausnahmslos mit festgelegtem Datentyp erfolgen, was den Programmierer davor bewahrt, Objekte auf unbeabsichtigte Weise zu verwenden. Java lässt Zeigermanipulation nicht zu, was den Programmierer davor bewahrt, zufällig die Speichergrenzen des Programms zu überschreiten. Vom Standpunkt der Anwendungsentwicklung kann Java wie jede andere höhere Programmiersprache betrachtet werden. Sie müssen die gleichen Sicherheitsregeln für die Anwendungsentwicklung beachten, die auch für andere Sprachen auf Ihrem System gelten.

Java-Applets

Java-Applets sind kleine Java-Programme, die in HTML-Seiten integriert werden können, die auf dem Client ausgeführt werden, aber die Möglichkeit bieten auf Ihr Betriebssystem i5/OS zuzugreifen. Ein ODBC-Programm (Open Database Connectivity) oder ein APPC-Programm (Advanced Program-to-Program Communications), das auf einem PC in Ihrem Netz betrieben wird, kann ebenfalls auf Ihr System zugreifen, wenn Ihr System beispielsweise für die Bedienung von Anwendungen oder als Web-Server verwendet wird. Im Allgemeinen können Java-Applets nur mit dem System eine Sitzung aufbauen, von dem das Applet ursprünglich stammt. Deshalb kann ein Java-Applet von einem angeschlossenen PC nur dann auf Ihr Betriebssystem i5/OS zugreifen, wenn das Applet von diesem Betriebssystem i5/OS stammt.

Ein Applet kann versuchen, zu jedem TCP/IP-Port auf einem System eine Verbindung herzustellen. Es muss keinen Kontakt zu einem Software-Server aufnehmen, der in Java erstellt wurde. Bei Systemen, die mit der IBM Toolbox for Java erstellt wurden, muss das Applet jedoch eine Benutzer-ID und ein Kennwort zur Verfügung stellen, wenn es Verbindungen zurück zum System herstellt. Alle in dieser Veröffentlichung beschriebenen Systeme sind Betriebssysteme i5/OS. (Ein Java-Anwendungsserver muss die IBM Toolbox for Java nicht verwenden.) Normalerweise fordert die Klasse IBM Toolbox for Java den Benutzer zur Eingabe einer Benutzer-ID und eines Kennworts für die erste Verbindung auf.

Das Applet kann nur dann Funktionen auf dem Betriebssystem i5/OS ausführen, wenn das Benutzerprofil für die entsprechenden Funktionen berechtigt ist. Daher ist ein gute Ressourcenschutzmethode

unentbehrlich, wenn Sie vorhaben, Java-Applets für neue Anwendungsfunktionen einzusetzen. Wenn das System die Anforderungen von Applets verarbeitet, bleibt der Wert für die eingeschränkten Berechtigungsgruppen, der im Benutzerprofil angegeben ist, unbeachtet.

Mit Hilfe des Applet-Viewers können Sie ein Applet auf dem Betriebssystem i5/OS testen; er ist dabei jedoch nicht den Sicherheitsbeschränkungen eines Browsers unterworfen. Setzen Sie deshalb den Applet-Viewer nur zum Testen Ihrer eigenen Applets ein, und niemals, um Applets von externen Quellen auszuführen. Java-Applets schreiben häufig auf das PC-Laufwerk des Benutzers, wodurch das Applet möglicherweise die Gelegenheit erhält, eine destruktive Aktion auszuführen. Sie können jedoch ein digitales Zertifikat verwenden, um ein Java-Applet zu signieren und damit dessen Authentizität zu belegen. Das signierte Applet kann dann auch auf die lokalen Laufwerke des PCs schreiben, wenn die Standardeinstellung für den Browser dies nicht zulässt. Das signierte Applet kann ebenfalls auf zugeordnete Laufwerke Ihres Systems schreiben, da sich diese dem PC gegenüber wie lokale Laufwerke darstellen.

Für Java-Applets, die von Ihrem System stammen, müssen Sie möglicherweise signierte Applets einsetzen. Sie müssen die Benutzer jedoch anweisen, niemals signierte Applets von unbekannten Quellen zu akzeptieren.

Ab V4R4 können Sie mit der IBM Toolbox for Java eine SSL-Umgebung (Secure Sockets Layer) definieren. Außerdem können Sie das IBM Developer Toolkit for Java dazu verwenden, eine Java-Anwendung mit SSL zu sichern. Die Verwendung von SSL für Ihre Java-Anwendungen garantiert, dass die Daten verschlüsselt werden, einschließlich der zwischen Client und Server übergebenen Benutzer-IDs und Kennwörter. Sie können Digital Certificate Manager (DCM) verwenden, um registrierte Java-Programme für die Verwendung von SSL zu konfigurieren.

Java-Servlets

Servlets sind serverseitige, in Java erstellte Komponenten, die die Funktion eines Web-Servers dynamisch erweitern, ohne dessen Code zu ändern. Der IBM WebSphere Application Server, der zum Lieferumfang von IBM Web Enablement for i5/OS gehört, bietet Unterstützung für die Verwendung von Servlets auf den i5/OS-Betriebssystemen.

Auf Servlet-Objekte, die vom System verwendet werden, muss der Ressourcenschutz angewendet werden. Der Ressourcenschutz kann ein Servlet jedoch nicht ausreichend schützen. Wenn ein Web-Server ein Servlet lädt, verhindert der Ressourcenschutz nicht, dass andere dieses Servlet ebenfalls ausführen. Folglich müssen Sie den Ressourcenschutz zusätzlich zu den Sicherheitssteuerungselementen und -direktiven des HTTP-Servers anwenden. Lassen Sie es beispielsweise nicht zu, dass Servlets lediglich unter dem Profil des Web-Servers ausgeführt werden können. Sie müssen auch die Sicherheitseinrichtungen Ihrer Servlet-Entwicklungstools nutzen, wie sie beispielsweise im WebSphere Application Server for i5/OS enthalten sind.

Weitere Informationen über allgemeine Sicherheitsmaßnahmen für Java finden Sie in folgenden Quellen:

- IBM Developer Kit for Java: Java-Sicherheit.
- IBM Toolbox for Java: Sicherheitsklassen.
- Security considerations for Internet browsers.

Java-Authentifizierung und -Berechtigung für Ressourcen

Die IBM Toolbox for Java enthält Sicherheitsklassen, mit denen die Identität eines Benutzers geprüft und diese optional dem Betriebssystemthread für eine Anwendung oder ein Servlet, die bzw. das auf einem Betriebssystem i5/OS läuft, zugeordnet werden kann. Nachfolgende Ressourcenschutzüberprüfungen finden unter der zugeordneten Identität statt.

Das IBM Developer Kit for Java unterstützt Java Authentication and Authorization Service (JAAS), eine Standarderweiterung des Java 2 Software Development Kit (J2SDK), Standard Edition. Derzeit bietet

J2SDK eine Zugriffssteuerung, die auf dem Ursprung und dem Unterzeichner des Codes basiert (Zugriffssteuerung auf der Basis der Codequelle).

Java-Anwendungen mit SSL sichern

Mit Hilfe von SSL (Secure Sockets Layer) kann die Übertragung für i5/OS-Anwendungen, die mit IBM Developer Kit for Java entwickelt wurden, gesichert werden. Clientanwendungen, die die IBM Toolbox for Java verwenden, können SSL ebenfalls nutzen. Die Aktivierung von SSL für Ihre eigenen Java-Anwendungen unterscheidet sich von der Aktivierung von SSL für andere Anwendungen.

Zugehörige Konzepte

„Sicherheit für Web-Serving" auf Seite 18
Wenn Sie Besuchern Zugriff auf Ihre Website bieten, lassen Sie Informationen über den Aufbau der Site und die Codierung, mit der die Seite generiert wurde, außen vor. Der Besuch Ihrer Seite muss einfach, schnell und reibungslos erfolgen; die Verarbeitung, die dahinter steht, soll hinter den Kulissen ablaufen.

Digital Certificate Manager konfigurieren

Authentication services

Zugehörige Informationen

Java Authentication and Authorization Service

Secure Sockets Layer (SSL)

E-Mail-Sicherheit

Die Verwendung von E-Mail im Internet oder anderen ungesicherten Netzen birgt Sicherheitsrisiken, auch wenn das System über eine Firewall geschützt ist.

Sie müssen diese Risiken kennen, damit Sie in Ihren Sicherheitsrichtlinien auch beschreiben können, wie diese Risiken minimiert werden sollen.

E-Mail ist eine Form der Kommunikation. Es ist wichtig, beim Versenden vertraulicher Informationen über E-Mail besonnen vorzugehen. Da eine E-Mail zahlreiche Systeme durchläuft, bevor Sie sie erhalten, besteht für Dritte die Gelegenheit, die Mail abzufangen und zu lesen. Daher besteht bei Ihnen möglicherweise der Wunsch, Sicherheitsmaßnahmen zu ergreifen, um die Vertraulichkeit Ihrer E-Mails zu schützen.

Allgemein bekannte E-Mail-Sicherheitsrisiken

Im Folgenden finden Sie einige Risiken im Zusammenhang mit der Verwendung von E-Mail:

- **Flooding (Überflutung)** (eine Art Denial-of-Service-Attacke) tritt auf, wenn ein System mit zahlreichen E-Mail-Nachrichten überlastet wird. Es ist für einen Angreifer relativ einfach, ein simples Programm zu erstellen, das Millionen von E-Mail-Nachrichten (einschließlich leerer Nachrichten) an einen einzelnen E-Mail-Server sendet, und so zu versuchen, den Server zu überlasten. Ohne entsprechende Sicherheitseinrichtungen kann auf dem Zielserver eine Dienstunterbrechung (Denial-of-Service) erfolgen, da die Speicherplatte des Servers mit unnützen Nachrichten gefüllt wird. Es kann auch sein, dass das System nicht mehr reagiert, da sämtliche Systemressourcen in die Verarbeitung der Mail aus der Attacke involviert werden.
- **Spamming** (Junk-E-Mail) ist ebenfalls ein häufiger Angriff mittels E-Mails. Mit der steigenden Zahl der Unternehmen, die E-Commerce über das Internet anbieten, kam es zu einer regelrechten Explosion unerwünschter oder unangeforderter E-Mails. Dies sind sog. Junk-Mails, die an eine riesige Verteilerliste von E-Mail-Benutzern gesendet werden und die Mailboxen der einzelnen Benutzer füllen.
- **Vertraulichkeit** stellt ein Risiko dar, wenn eine E-Mail über das Internet an eine andere Person gesendet wird. Diese E-Mail durchläuft zahlreiche Systeme, bevor sie den gewünschten Empfänger erreicht. Wenn Sie Ihre Nachricht nicht verschlüsselt haben, kann ein Hacker Ihre E-Mail an jedem Punkt entlang des Zustellungswegs abfangen und lesen.

Optionen für E-Mail-Sicherheit

Um sich vor den Gefahren des Flooding und Spamming zu schützen, müssen Sie Ihren E-Mail-Server entsprechend konfigurieren. Die meisten Serveranwendungen bieten Methoden an, um diese Angriffsformen abzuwehren. Sie können sich auch an Ihren Internet-Service-Provider (ISP) wenden, um sicherzustellen, dass er für zusätzlichen Schutz vor diesen Attacken sorgt.

Welche weiteren Sicherheitsmaßnahmen erforderlich sind, hängt sowohl davon ab, welches Maß an Vertraulichkeit Sie benötigen, als auch davon, welche Sicherheitseinrichtungen Ihre E-Mail-Anwendungen bieten. Reicht es beispielsweise aus, den Inhalt der E-Mail-Nachrichten vertraulich zu behandeln? Oder sollen sämtliche Informationen im Zusammenhang mit der E-Mail, wie beispielsweise IP-Quellen- und IP-Zieladresse, vertraulich behandelt werden?

Einige Anwendungen verfügen über integrierte Sicherheitseinrichtungen, die eventuell den Schutz bieten, den Sie benötigen. Beispielsweise bietet Lotus Notes Domino zahlreiche integrierte Sicherheitseinrichtungen, darunter die Verschlüsselung eines gesamten Dokuments oder einzelner Felder in einem Dokument.

Zur Verschlüsselung von Mails erstellt Lotus Notes Domino für jeden Benutzer einen eindeutigen öffentlichen und privaten Schlüssel. Mit dem privaten Schlüssel wird die Nachricht verschlüsselt, so dass sie nur von denjenigen Benutzern gelesen werden kann, die über den entsprechenden öffentlichen Schlüssel verfügen. Ihren öffentlichen Schlüssel müssen Sie an die vorgesehenen Empfänger schicken, damit diese Ihre verschlüsselten Mitteilungen entschlüsseln können. Wenn Sie eine verschlüsselte E-Mail erhalten, verwendet Lotus Notes Domino den öffentlichen Schlüssel des Absenders, um die Mitteilung für Sie zu entschlüsseln.

Informationen über die Verwendung dieser Notes-Verschlüsselungseinrichtungen finden Sie in der Onlinehilfefunktion für das Programm.

Sie haben mehrere Möglichkeiten, das Maß an Vertraulichkeit für E-Mails oder andere Informationen, die zwischen Geschäftsstellen, fernen Clients oder Geschäftspartnern ausgetauscht werden, zu erhöhen.

Wenn Ihre E-Mail-Serveranwendung SSL (Secure Sockets Layer) unterstützt, können Sie eine sichere Kommunikationssitzung zwischen dem Server und E-Mail-Clients einrichten. SSL bietet ebenfalls Unterstützung für die optionale Authentifizierung auf der Clientseite, sofern die Clientanwendung für deren Verwendung erstellt wurde. Da die gesamte Sitzung verschlüsselt wird, garantiert SSL auch die Datenintegrität während der Übertragung.

Sie haben weiterhin die Möglichkeit, eine VPN-Verbindung (Virtual Private Network) zu konfigurieren. Mit Ihrem System können Sie verschiedene VPN-Verbindungen konfigurieren, zu denen auch Verbindungen zwischen fernen Clients und Ihrem System gehören. Wenn Sie ein VPN verwenden, wird der gesamte Datenverkehr zwischen den kommunizierenden Endpunkten verschlüsselt, was sowohl die Vertraulichkeit als auch die Integrität der Daten garantiert.

Zugehörige Konzepte

„FTP-Sicherheit" auf Seite 23
Mit Hilfe von FTP (File Transfer Protocol) können Dateien zwischen einem Client (einem Benutzer auf einem anderen System) und Ihrem Server übertragen werden. Sie müssen die Sicherheitsrisiken kennen, die bei Verwendung von FTP auftreten können, damit in Ihren Sicherheitsrichtlinien auch beschrieben wird, wie diese Risiken minimiert werden sollen.

„Sicherheit durch mehrfache Abwehrstufen" auf Seite 4
Ihre Sicherheitsrichtlinien definieren, was Sie schützen möchten und was Sie von den Systembenutzern erwarten.

Virtual private network (VPN)

Zugehörige Verweise

Terminologie zum Thema Sicherheit

Zugehörige Informationen

Lotus Domino Reference Library

Lotus Documentation

Lotus Notes and Domino R5.0 Security Infrastructure Revealed Redbook

Lotus Domino for AS/400 Internet Mail and More Redbook

FTP-Sicherheit

Mit Hilfe von FTP (File Transfer Protocol) können Dateien zwischen einem Client (einem Benutzer auf einem anderen System) und Ihrem Server übertragen werden. Sie müssen die Sicherheitsrisiken kennen, die bei Verwendung von FTP auftreten können, damit in Ihren Sicherheitsrichtlinien auch beschrieben wird, wie diese Risiken minimiert werden sollen.

Sie können außerdem die Funktion für ferne Befehle (Remote Command) verwenden, um Befehle an den Server zu übergeben. Aus diesem Grund bietet sich FTP für die Arbeit mit fernen Systemen oder der Übertragung von Dateien zwischen Systemen an. Die Verwendung von FTP im Internet oder anderen ungesicherten Netzen stellt jedoch ein gewisses Sicherheitsrisiko für Sie dar. Die Kenntnis dieser Risiken hilft Ihnen beim Sichern des Systems.

- Ihre Objektberechtigungsmethode bietet möglicherweise keinen ausreichenden Schutz, wenn Sie FTP auf Ihrem System zulassen.

  Beispiel: Die allgemeine Berechtigung für Ihre Objekte könnte *USE sein, aber heute wird den meisten Benutzern der Zugriff auf diese Objekte verwehrt, weil Menüschutz verwendet wird. (Menüschutz verwehrt Benutzern alle Aktivitäten, die nicht zu ihren Menüauswahlmöglichkeiten gehören.) Da FTP-Benutzer nicht auf die Verwendung von Menüs beschränkt sind, können Sie alle Objekte auf Ihrem System lesen.

  Im Folgenden finden Sie einige Optionen, um dieses Sicherheitsrisiko in den Griff zu bekommen:

  – Aktivieren Sie die vollständige i5/OS-Objektsicherheit auf dem System (mit anderen Worten: Ändern Sie das Sicherheitsmodell des Systems von Menüschutz in Objektschutz). Dies ist die beste und sicherste Option.
  – Schreiben Sie Exitprogramme für FTP, um den Zugriff auf Dateien zu beschränken, die über FTP übertragen werden könnten. Diese Exitprogramme müssen mindestens das gleiche Maß an Schutz bieten wie das Menüprogramm. Möglicherweise wünschen Sie eine noch restriktivere FTP-Zugriffssteuerung. Diese Maßnahme gilt nur für FTP, nicht für andere Schnittstellen wie ODBC (Open Database Connectivity), DDM (Distributed Data Management oder DRDA (Distributed Relational Database Architecture).

    Anmerkung: Mit der Berechtigung *USE für eine Datei kann der Benutzer die Datei herunterladen. Mit der Berechtigung *CHANGE für eine Datei kann der Benutzer die Datei hochladen.

- Ein Hacker kann eine Denial-Of-Service-Attacke gegen Ihren FTP-Server richten, um Benutzerprofile auf dem System zu inaktivieren. Dies geschieht, indem wiederholt versucht wird, sich so lange mit einem falschen Kennwort für ein Benutzerprofil anzumelden, bis das Benutzerprofil inaktiviert wird. Bei dieser Art von Attacke wird das Profil nach drei unzulässigen Anmeldeversuchen inaktiviert.

  Was Sie zur Vermeidung dieses Risikos unternehmen können, hängt davon ab, zu welchen Kompromissen Sie bereit sind, wenn Sie einerseits die Sicherheit erhöhen müssen, um die Gefahr einer solchen Attacke zu minimieren, andererseits aber Benutzern den Zugriff so einfach wie möglich machen möchten. Der FTP-Server setzt normalerweise den Systemwert QMAXSIGN ein, um zu verhindern, dass einem Hacker unbegrenzt viele Versuche zur Verfügung stehen, ein Kennwort herauszufinden und damit Kennwortattacken zu starten. Im Folgenden finden Sie einige Optionen, die Sie in Betracht ziehen müssen:

- Verwenden Sie ein Exitprogramm für die FTP-Serveranmeldung, um Anmeldeanforderungen von Systembenutzerprofilen und Benutzerprofilen zurückzuweisen, denen Sie den FTP-Zugriff nicht erlauben. (Bei Verwendung eines solchen Exitprogramms werden Anmeldeversuche der von Ihnen geblockten Benutzerprofile, die vom Exitpunkt für die Serveranmeldung zurückgewiesen werden, nicht mitgezählt, wenn es um die QMAXSIGN-Anzahl des Profils geht.)
- Verwenden Sie ein Exitprogramm für die FTP-Serveranmeldung, um anzugeben, über welche Clientmaschinen ein bestimmtes Benutzerprofil auf den FTP-Server zugreifen darf. Beispiel: Wenn einem Mitarbeiter aus der Buchhaltung FTP-Zugriff gewährt wird, erlauben Sie dem entsprechenden Benutzerprofil den Zugriff auf den FTP-Server nur von den Computern aus, die über IP-Adressen in der Buchhaltungsabteilung verfügen.
- Verwenden Sie ein Exitprogramm für die FTP-Serveranmeldung, um den Benutzernamen und die IP-Adresse aller FTP-Anmeldeversuche zu protokollieren. Überprüfen Sie diese Protokolle regelmäßig; wenn ein Profil wegen Überschreitung der maximal zulässigen Anmeldeversuche inaktiviert wird, stellen Sie die Identität des Benutzers anhand der IP-Adresse fest, und ergreifen Sie entsprechende Maßnahmen.
- Verwenden Sie das Warnsystem gegen Angriffe von außen, um Denial-of-Service-Attacken auf dem System festzustellen.

Außerdem können Sie FTP-Server-Exitpunkte verwenden, um eine anonyme FTP-Funktion für Gastbenutzer zur Verfügung zu stellen. Um einen sicheren anonymen FTP-Server einzurichten, sind Exitprogramme für die FTP-Serveranmeldung und für die Exitpunkte für die Gültigkeitsprüfung der Serveranforderung erforderlich.

Sie können SSL (Secure Sockets Layer) verwenden, um sichere Kommunikationssitzungen für Ihren FTP-Server bereitzustellen. Die Verwendung von SSL stellt sicher, dass alle FTP-Übertragungen verschlüsselt werden, um die Vertraulichkeit aller Daten, einschließlich Benutzernamen und Kennwörtern, zu wahren, die zwischen dem FTP-Server und dem Client übertragen werden. Der FTP-Server unterstützt ebenfalls die Verwendung digitaler Zertifikate zur Clientauthentifizierung.

Zusätzlich zu diesen FTP-Optionen könnten Sie auch in Betracht ziehen, Benutzer über anonymes FTP auf nicht vertrauliche Informationen zugreifen zu lassen. Anonymes FTP ermöglicht den ungeschützten Zugriff (kein Kennwort erforderlich) auf ausgewählte Informationen auf einem fernen System. Am fernen Standort wird festgelegt, welche Informationen für den allgemeinen Zugriff verfügbar gemacht werden. Diese Informationen sind allgemein verfügbar und können von jedem gelesen werden. Vor der Konfiguration des anonymen FTP sind die Sicherheitsrisiken abzuwägen und ist in Erwägung zu ziehen, Ihren FTP-Server mit Exitprogrammen zu sichern.

Zugehörige Konzepte

„E-Mail-Sicherheit” auf Seite 21
Die Verwendung von E-Mail im Internet oder anderen ungesicherten Netzen birgt Sicherheitsrisiken, auch wenn das System über eine Firewall geschützt ist.

Zugehörige Tasks

Configuring anonymous File Transfer Protocol

Managing access using File Transfer Protocol exit programs

Zugehörige Informationen

Securing FTP

Using SSL to secure the FTP server

Optionen für Übertragungssicherheit

Wenn die Daten über ein ungesichertes Netz wie das Internet übertragen werden, sollten Sie zum Schutz Ihrer Daten die geeigneten Sicherheitsmaßnahmen implementieren. Zu diesen Maßnahmen gehören SSL (Secure Sockets Layer), System i Access für Windows und VPN-Verbindungen (VPN - Virtual Private Network).

Wie bereits erwähnt, verfügt das Unternehmen JKL Toy (Szenario) über zwei primäre Systeme. Eines wird für Entwicklungs- und das andere für Produktionsanwendungen eingesetzt. Auf beiden Systemen werden unternehmenskritische Daten und Anwendungen verarbeitet. Daher hat das Unternehmen beschlossen, für seine Intranet- und Internetanwendungen ein neues System auf einem Peripherienetz hinzuzufügen.

Die Einrichtung eines Peripherienetzes garantiert darüber hinaus eine physische Trennung zwischen dem unternehmensinternen Netz und dem Internet. Diese Trennung senkt die Internetrisiken, denen die internen Systeme ausgesetzt sind. Da das neue System ausschließlich als Internetserver fungiert, gestaltet sich außerdem die Verwaltung der gesamten Netzsicherheit weniger kompliziert.

Wegen des in einer Internetumgebung jederzeit und überall bestehenden Sicherheitsbedarfs entwickelt IBM ständig entsprechende Angebote, um einen sicheren Netzbetrieb für die Durchführung von e-business im Internet zu gewährleisten. In einer Internetumgebung müssen Sie sowohl für systemspezifische als auch anwendungsspezifische Sicherheit sorgen. Das Versenden vertraulicher Informationen über ein unternehmensinternes Intranet oder eine Internetverbindung erhöht jedoch die Notwendigkeit, strengere Sicherheitslösungen zu implementieren. Um derartigen Risiken zu begegnen, müssen Sie Sicherheitsmaßnahmen implementieren, die die Übertragung der Daten schützen, während sie das Internet durchlaufen.

Die Risiken im Zusammenhang mit der Übertragung von Informationen über ungesicherte Systeme können mit Hilfe zweier spezieller Sicherheitsangebote für das Betriebssystem i5/OS auf Übertragungsebene minimiert werden: Gesicherte SSL-Kommunikation (Secure Sockets Layer) und VPN-Verbindungen (Virtual Private Networking).

Das SSL-Protokoll (Secure Sockets Layer) ist ein Branchenstandard für das Sichern der Kommunikation zwischen Clients und Servern. SSL wurde ursprünglich für Web-Browseranwendungen entwickelt, doch eine zunehmende Zahl weiterer Anwendungen kann jetzt auch SSL verwenden. Dazu gehören beim Betriebssystem i5/OS:

- IBM HTTP-Server für i5/OS (Original und auf Apache-Basis)
- FTP-Server
- Telnet-Server
- DRDA (Distributed Relational Database Architecture) und DDM-Server (Distributed Data Management - Verwaltung verteilter Daten)
- Management Central im System i Navigator
- Directory Services Server (LDAP)
- System i Access für Windows-Anwendungen, einschließlich System i Navigator, und Anwendungen, die für die APIs (Anwendungsprogrammierschnittstellen) von System i Access für Windows erstellt werden.
- Programme, die mit dem Developer Kit for Java entwickelt wurden, und Clientanwendungen, die das IBM Toolkit for Java verwenden.
- Programme, die mit SSL-APIs (Secure Sockets Layer Application Programmable Interfaces) entwickelt wurden und mit denen Anwendungen für SSL konfiguriert werden können. Weitere Informationen darüber, wie Programme erstellt werden, die SSL verwenden, finden Sie unter Secure Sockets Layer APIs.

Zahlreiche dieser Anwendungen unterstützen ebenfalls die Verwendung digitaler Zertifikate für die Clientauthentifizierung. SSL stützt sich auf digitale Zertifikate, um die Kommunikationsteilnehmer zu authentifizieren und eine sichere Verbindung herzustellen.

Virtual Private Network (VPN)

Mit den VPN-Verbindungen kann ein sicherer Übertragungskanal zwischen zwei Endpunkten aufgebaut werden. Ebenso wie bei einer SSL-Verbindung können die Daten, die zwischen den Endpunkten übertragen werden, verschlüsselt werden, wodurch sowohl die Vertraulichkeit als auch die Integrität der Daten

gewahrt wird. Bei VPN-Verbindungen haben Sie jedoch die Möglichkeit, den Datenfluss zwischen den angegebenen Endpunkten zu begrenzen und anzugeben, für welche Art von Datenverkehr diese Verbindung genutzt werden darf. VPN-Verbindungen bieten daher eine gewisse Sicherheit auf Netzebene, indem sie Ihnen helfen, Ihre Netzressourcen vor unbefugtem Zugriff zu schützen.

Die für Sie geeignete Methode

Sowohl SSL als auch VPN decken die Anforderungen sichere Authentifizierung, Vertraulichkeit und Datenintegrität ab. Welche dieser Methoden für Sie geeignet ist, hängt von zahlreichen Faktoren ab. Dazu gehört, mit wem Sie kommunizieren, welche Anwendungen Sie für die Kommunikation verwenden, wie sicher die Kommunikation sein muss und welche Kompromisse Sie für die Sicherheit der Kommunikation hinsichtlich des Preis-Leistungs-Verhältnisses eingehen möchten.

Wenn Sie für eine bestimmte Anwendung SSL verwenden möchten, muss diese Anwendung für die Verwendung von SSL konfiguriert sein. Obwohl zahlreiche Anwendungen SSL nicht nutzen können, verfügen viele andere, wie beispielsweise Telnet und System i Access für Windows, über eine SSL-Funktion. VPNs ermöglichen Ihnen andererseits, den gesamten IP-Datenverkehr zwischen bestimmten Verbindungsendpunkten zu schützen.

Sie können beispielsweise derzeit HTTP über SSL nutzen, um einem Geschäftspartner die Kommunikation mit einem Web-Server in Ihrem internen Netz zu gestatten. Wenn der Web-Server die einzige sichere Anwendung ist, die zwischen Ihnen und Ihrem Geschäftspartner erforderlich ist, werden Sie wahrscheinlich nicht zu einer VPN-Verbindung wechseln wollen. Wenn Sie die Kommunikation jedoch ausweiten möchten, werden Sie möglicherweise eine VPN-Verbindung vorziehen. Möglicherweise liegt auch die Situation vor, dass Sie den Datenverkehr in einem Teil Ihres Netzes schützen müssen, aber nicht jeden Client und Server individuell für die Verwendung von SSL konfigurieren möchten. In diesem Fall können Sie eine VPN-Verbindung von Gateway zu Gateway für diesen Teil des Netzes erstellen. Der Datenverkehr kann damit geschützt werden, aber die Verbindung wäre für die einzelnen Server und Clients auf beiden Seiten der Verbindung transparent.

Zugehörige Konzepte

„Sicherheit durch mehrfache Abwehrstufen" auf Seite 4
Ihre Sicherheitsrichtlinien definieren, was Sie schützen möchten und was Sie von den Systembenutzern erwarten.

„Szenario: e-business Pläne des Unternehmens JKL Toy" auf Seite 8
Das typische Szenario des Unternehmens JKL Toy, das beschlossen hat seine Unternehmensziele mit Hilfe des Internets zu erweitern, ist möglicherweise für Sie bei der Planung Ihres eigenen e-business sehr hilfreich.

Zugehörige Verweise

Secure sockets APIs

Zugehörige Informationen

Secure Sockets Layer (SSL)

Virtual Private Network (VPN)

Digitale Zertifikate für SSL verwenden

Digitale Zertifikate bilden die Basis für die Verwendung von SSL (Secure Sockets Layer) für die sichere Kommunikation und als striktere Authentifizierungsmethode.

Auf dem Betriebssystem i5/OS können Sie mit Hilfe von Digital Certificate Manager (DCM), einem integrierten i5/OS-Feature, problemlos digitale Zertifikate für Ihre Systeme und Benutzer erstellen und verwalten.

Außerdem können Sie einige Anwendungen, beispielsweise den IBM HTTP-Server für i5/OS, so konfigurieren, dass sie statt Benutzername und Kennwort digitale Zertifikate als striktere Methode zur Clientauthentifizierung verwenden.

Digitales Zertifikat

Ein digitales Zertifikat ist ein digitaler Berechtigungsnachweis, der die Identität des Zertifikatseigners bestätigt, vergleichbar mit einem Pass. Eine anerkannte Instanz, die als Zertifizierungsinstanz (CA) bezeichnet wird, stellt digitale Zertifikate für Benutzer und Server aus. Die Anerkennung der Zertifizierungsinstanz bildet die Voraussetzung für die Anerkennung des Zertifikats als gültigem Berechtigungsnachweis.

Für jede Zertifizierungsinstanz gelten bestimmte Richtlinien bei der Festlegung, welche Identifikationsdaten zur Ausstellung eines Zertifikats erforderlich sind. Einige Internet-Zertifizierungsinstanzen verlangen möglicherweise nur wenige Informationen, wie beispielsweise einen registrierten Namen. Ein registrierter Name ist der Name der Person oder des Systems, für die/den eine Zertifizierungsinstanz ein digitales Zertifikat und eine digitale E-Mail-Adresse ausstellt. Für jedes Zertifikat wird ein privater und ein öffentlicher Schlüssel generiert. Der öffentliche Schlüssel ist Teil des Zertifikats selbst, wohingegen der private Schlüssel im Browser oder in einer gesicherten Datei gespeichert wird. Das dem Zertifikat zugeordnete Schlüsselpaar kann verwendet werden, um Daten wie Nachrichten und Dokumente, die zwischen Benutzern und Servern hin- und hergesendet werden, zu "signieren" und zu verschlüsseln. Durch solche digitalen Signaturen kann der Ursprung eines Objektes zuverlässig festgestellt und seine Integrität gewährleistet werden.

Obwohl zahlreiche Anwendungen SSL nicht nutzen können, verfügen viele andere, wie beispielsweise Telnet und System i Access für Windows, über eine SSL-Funktion.

Zugehörige Konzepte

Digital Certificate Manager konfigurieren

Secure Sockets Layer (SSL)

Zugehörige Verweise

Terminologie zum Thema Sicherheit

Secure Sockets Layer für sicheren Telnet-Zugriff

Sie können Ihren Telnet-Server für die Verwendung von SSL (Secure Sockets Layer) konfigurieren, um Telnet-Kommunikationssitzungen zu sichern.

Um den Telnet-Server für die Verwendung von SSL zu konfigurieren, müssen Sie mit Digital Certificate Manager (DCM) das Zertifikat konfigurieren, das der Telnet-Server verwenden soll. Standardmäßig verarbeitet der Telnet-Server sowohl sichere als auch ungesicherte Verbindungen. Sie können Telnet jedoch so konfigurieren, dass nur sichere Telnet-Sitzungen zulässig sind. Außerdem können Sie den Telnet-Server für die Verwendung digitaler Zertifikate zwecks strikterer Clientauthentifizierung konfigurieren.

Wenn Sie sich bei Telnet für SSL entscheiden, bieten sich Ihnen erhebliche Sicherheitsvorteile. Außer der Serverauthentifizierung werden bei Telnet die Daten verschlüsselt, bevor Telnet-Protokolldaten fließen. Nach Herstellung der SSL-Sitzung werden alle Telnet-Protokolle einschließlich Benutzer-ID- und Kennwortaustausch verschlüsselt.

Bei Verwendung des Telnet-Servers muss insbesondere die Sensibilität der Informationen beachtet werden, die in einer Clientsitzung benutzt werden. Bei sensiblen oder persönlichen Informationen werden Sie es möglicherweise vorteilhaft finden, Ihren Telnet-Server für SSL zu konfigurieren. Wenn Sie ein digitales Zertifikat für die Telnet-Anwendung konfigurieren, kann der Telnet-Server sowohl SSL-Clients bedienen als auch solche, für die SSL nicht konfiguriert ist. Wenn es auf Grund Ihrer Sicherheitsrichtlinien erforderlich ist, dass Sie Ihre Telnet-Sitzungen immer verschlüsseln, können Sie alle Telnet-Sitzungen, die nicht mit SSL gesichert sind, inaktivieren. Wenn Sie den SSL-Telnet-Server nicht benötigen, können Sie den SSL-Port ausschalten. Sie können die Verwendung von SSL für Telnet-Sitzungen über den Parameter ALWSSL

(SSL zulassen) des Befehls CHGTELNA (TELNET-Attribute ändern) steuern. Um sicherzustellen, dass die Anwendungen die SSL- oder Nicht-SSL-Ports jeweils nicht verwenden können, können Sie darüber hinaus die Verwendung mit dem Befehl ADDTCPPORT (TCP/IP-Port-Einschränkung hinzufügen) einschränken.

Weitere Informationen über Telnet und Sicherheitstipps für Telnet mit und ohne SSL finden Sie unter dem Thema zu IBM Systems Software Information Center bei Telnet. Dieses Thema enthält die Informationen, die Sie benötigen, um Telnet auf Ihrem Betriebssystem i5/OS zu verwenden.

Zugehörige Konzepte

Telnet scenario: Securing Telnet with SSL

Digital Certificate Manager planen

Zugehörige Informationen

Telnet

Secure Sockets Layer für sicheres System i Access für Windows

Zum Sichern von System i Access für Windows-Kommunikationssitzungen können Sie Secure Sockets Layer (SSL) für System i Access für Windows konfigurieren.

Die Verwendung von SSL garantiert, dass der gesamte Datenverkehr für die System i Access für Windows-Sitzungen verschlüsselt wird. Es besteht damit keine Möglichkeit, dass Daten gelesen werden, während sie zwischen dem lokalen und dem fernen Host übertragen werden.

Zugehörige Informationen

Secure Sockets Layer administration

Java security

Security classes

Virtual Private Network für sichere private Kommunikation

Virtual Private Network (VPN), eine Erweiterung des Intranets eines Unternehmens auf das vorhandene Gerüst eines öffentlichen oder privaten Netzes, kann Ihnen helfen, vertraulich und sicher innerhalb Ihres Unternehmens zu kommunizieren.

Angesichts der zunehmenden Verwendung von VPNs und der von ihnen gebotenen Sicherheit untersucht das Unternehmen JKL Toy solche Möglichkeiten, um Daten über das Internet zu übertragen. Das Unternehmen hat vor kurzem eine weitere kleine Spielzeugfabrik übernommen, die als Tochtergesellschaft von JKL geführt werden soll. JKL wird zwischen den beiden Unternehmen Informationen übertragen müssen. Beide Unternehmen verwenden das Betriebssystem i5/OS und eine VPN-Verbindung, die den notwendigen Schutz bieten kann, der für die Übertragung zwischen den beiden Netzen erforderlich ist. Das Erstellen eines VPN ist kosteneffizienter als die Verwendung herkömmlicher Standleitungen.

Folgende Benutzer können beispielsweise VPNs für die Konnektivität verwenden:

- Ferne und mobile Benutzer
- Heimbüros und Zweigstellen oder andere ausgelagerte Standorte
- Business-to-Business-Kommunikation

Es kommt zu Sicherheitsrisiken, wenn Sie den Benutzerzugriff auf sensible Daten nicht beschränken. Ohne Zugriffsbeschränkungen kann eine erhöhte Gefahr bestehen, dass Unternehmensdaten nicht vertraulich bleiben. Sie benötigen einen Plan, der nur denjenigen Benutzern den Zugriff auf ein bestimmtes System gestattet, die gemeinsam Informationen auf dem System benutzen müssen. Mittels eines VPN können Sie den Datenaustausch auf dem Netz steuern, während Sie gleichzeitig wichtige Sicherheitseinrichtungen wie Authentifizierung und Datenschutz bereitstellen. Wenn Sie mehrere VPN-Verbindungen herstellen, können Sie für jede Verbindung steuern, wer auf welche Systeme zugreifen darf. So könnten beispielsweise Buchhaltung und Personalabteilung über ein eigenes VPN miteinander verbunden werden.

Wenn Sie Benutzern den Zugriff auf das System über das Internet gestatten, senden Sie möglicherweise sensible Unternehmensdaten über öffentliche Netze und setzen die Daten damit möglichen Angriffen aus. Eine Möglichkeit, übertragene Daten zu schützen, besteht in der Anwendung von Verschlüsselungs- und Authentifizierungsmethoden, um Vertraulichkeit und Sicherheit zu gewährleisten. VPN-Verbindungen bieten eine Lösung für ein spezielles Sicherheitsbedürfnis: den Schutz der Datenübertragung zwischen Systemen. VPN-Verbindungen schützen Daten, die zwischen den beiden Endpunkten der Verbindung hin und her fließen. Außerdem können Sie über Paketregeln definieren, welche IP-Pakete über das VPN übertragen werden dürfen.

Mit Hilfe von VPN können Sie sichere Verbindungen herstellen, um den Datenverkehr zwischen kontrollierten und vertrauenswürdigen Endpunkten zu schützen. Dennoch müssen Sie nach wie vor vorsichtig sein, wenn es darum geht, in welchem Umfang Sie Ihren VPN-Partnern Zugriff gewähren. Eine VPN-Verbindung kann Daten verschlüsseln, während sie öffentliche Netze durchlaufen. Je nach Konfiguration kann es jedoch vorkommen, dass über das Internet übertragene Daten nicht über eine VPN-Verbindung transportiert werden. In diesem Fall sind die Daten nicht verschlüsselt, wenn sie durch die internen Netze fließen, die über die Verbindung kommunizieren. Sie müssen deshalb die Konfiguration jeder VPN-Verbindung sorgfältig planen. Vergewissern Sie sich, dass Sie Ihren VPN-Partnern nur Zugriff auf diejenigen Hosts oder Ressourcen in Ihrem internen Netz erteilen, die für sie vorgesehen sind.

Beispiel: Einer Ihrer Lieferanten benötigt möglicherweise Informationen über Ihren Lagerbestand. Diese Informationen sind in einer Datenbank gespeichert, mit deren Hilfe Sie Webseiten in Ihrem Intranet aktualisieren. Sie möchten diesem Lieferanten gestatten, direkt über eine VPN-Verbindung auf diese Seiten zuzugreifen. Der Lieferant soll aber keine Möglichkeit haben, auf andere Systemressourcen, wie beispielsweise die Datenbank selbst, zuzugreifen. Sie können Ihre VPN-Verbindung so konfigurieren, dass der Datenverkehr zwischen beiden Endpunkten nur über Port 80 erfolgen darf. Port 80 ist der Standardport für den HTTP-Datenverkehr. Folglich kann Ihr Lieferant nur über diese Verbindung HTTP-Anforderungen und -Antworten senden und empfangen.

Da Sie die Art des Datenverkehrs, der über die VPN-Verbindung fließt, einschränken können, stellt die Verbindung auch ein Maß für die Sicherheit auf Netzebene dar. VPN regelt den Datenverkehr des Systems jedoch anders als eine Firewall. Außerdem ist eine VPN-Verbindung nicht die einzige Möglichkeit für die Herstellung einer sicheren Kommunikation zwischen Ihrem Betriebssystem i5/OS und anderen Systemen. Je nach Sicherheitsbedürfnis ist in Ihren Augen SSL vielleicht besser geeignet.

Ob eine VPN-Verbindung Ihr Sicherheitsbedürfnis befriedigen kann, hängt davon ab, was Sie schützen möchten und zu welchen Kompromissen Sie bereit sind, um diesen Schutz zu gewährleisten. Wie bei jeder Entscheidung, die Sie im Zusammenhang mit der Sicherheit treffen müssen, müssen Sie auch hier beachten, auf welche Weise eine VPN-Verbindung Ihre Sicherheitsrichtlinien unterstützt.

Zugehörige Konzepte

„System i und Überlegungen zur Internetsicherheit" auf Seite 2
Die Sicherheitsprobleme im Zusammenhang mit dem Internet sind signifikant. Dieser Abschnitt bietet einen Überblick über die Sicherheitsfunktionen und -angebote von i5/OS.

Virtual private networks (VPN)

Anhang. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. An Stelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete, der IBM Lizenzvereinbarung für Maschinencode oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Musteranwendungsprogramme, die in Quellensprache geschrieben sind. Sie dürfen diese Musterprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Musterprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten.

Kopien oder Teile der Musterprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Musterprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. _Jahr/Jahre angeben_. Alle Rechte vorbehalten.

Informationen zu Programmierschnittstellen

In der vorliegenden Veröffentlichung werden vorgesehene Programmierschnittstellen dokumentiert, mit deren Hilfe Kunden Programme für den Zugriff auf die Services von IBM i5/OS schreiben können.

Marken

Folgende Namen sind Marken der IBM Corporation in den USA und/oder anderen Ländern:

Domino
Distributed Relational Database Architecture (DRDA)
i5/OS
IBM

IBM (Logo)
Lotus Notes
Notes
System i
WebSphere

Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken von Sun Microsystems, Inc. in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

Bedingungen

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Persönliche Nutzung: Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM weder weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Kommerzielle Nutzung: Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Abgesehen von den hier gewährten Berechtigungen erhalten Sie keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum.

IBM behält sich das Recht vor, die in diesem Dokument gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Verordnungen, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf ″as-is″-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit oder die Freiheit der Rechte Dritter zur Verfügung gestellt.