IBM Systems - iSeries

Sicherheit
iSeries und Internetsicherheit

Version 5 Release 4

IBM Systems - iSeries

Sicherheit
iSeries und Internetsicherheit

Version 5 Release 4

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter „Bemerkungen", auf Seite 39 gelesen werden.

Siebte Ausgabe (Februar 2006)

Diese Ausgabe bezieht sich auf Version 5, Release 4, Modifikation 0 des Betriebssystems IBM i5/OS (Produktnummer 5722-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 (Reduced Instruction Set Computer) ausgeführt werden. Auf CICS-Modellen ist sie nicht ausführbar.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Systems - iSeries Security iSeries and Internet Security, Version 5 Release 4,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
Februar 2006

Inhaltsverzeichnis

iSeries und Internetsicherheit

Die Internetanbindung des eigenen LAN ist ein bedeutender Schritt in der Weiterentwicklung Ihres Netzes, der von Ihnen eine erneute Berwertung Ihrer Sicherheitsanforderungen verlangt.

Der IBM @server iSeries-Server verfügt über integrierte Softwarelösungen und eine Sicherheitsarchitektur, mit deren Hilfe wirksame Abwehrmaßnahmen gegen potenzielle Sicherheitsfallen und Eindringlinge aus dem Internet errichtet werden können. Der richtige Einsatz dieser iSeries-Sicherheitsangebote garantiert, dass Ihre Kunden, Mitarbeiter und Geschäftspartner alle erforderlichen Geschäftsdaten in einer sicheren Umgebung abrufen können.

Anhand der vorliegenden Informationen können Sie sich über allgemein bekannte Sicherheitsrisiken und den Zusammenhang zwischen diesen Risiken und Ihren Internetzielen und e-business Zielen unterrichten. Sie erfahren auch, wie die Risiken gegenüber den Vorteilen der verschiedenen Sicherheitsoptionen einzuschätzen sind, die von der iSeries geboten werden, um diesen Risiken zu begegnen. Zum Schluss können Sie selbst entscheiden, wie Sie diese Informationen für die Entwicklung eines für Ihr Unternehmen adäquaten Netzsicherheitsplans nutzen.

Druckbare PDF-Datei

Verwenden Sie diesen Abschnitt, um eine PDF-Datei mit diesen Informationen anzuzeigen und zu drucken.

Zum Anzeigen oder Herunterladen der PDF-Version dieses Dokuments wählen Sie iSeries und Internetsicherheit aus (416 KB oder 60 Seiten).

Sie können auch die folgenden Referenzinformationen anzeigen oder herunterladen:

- Intrusion detection (ca. 160 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. 700 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. 600 KB). Die Lösung für Einzelanmeldung reduziert die Anzahl der Anmeldungen, die ein Benutzer für den Zugriff auf mehrere Anwendungen und Server ausführen muss, sowie die Anzahl der Kennwörter.
- Plan and Set Up System Security (ca. 3500 KB).

PDF-Dateien speichern

So können Sie eine PDF-Datei auf Ihrer Workstation speichern, um diese anzuzeigen oder zu drucken:

1. Klicken Sie im Browser mit der rechten Maustaste auf die PDF-Datei (klicken Sie mit der rechten Maustaste auf den o. a. 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 diese 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

Plan and Set Up System Security

---

iSeries und Überlegungen zur Internetsicherheit

Bietet einen Überblick über die Sicherheitsfunktionen und -angebote der iSeries.

Die Antwort auf die Frage nach der Sicherheit und dem Internet ist davon abhängig, wie Sie das Internet nutzen möchten. Die Sicherheitsprobleme im Zusammenhang mit dem Internet sind signifikant. Welche Probleme für Sie relevant sind, hängt davon ab, wie Sie das Internet nutzen möchten. Ihr erster Schritt mag darin bestehen, den Benutzern Ihres internen Netzes den Zugriff auf das Web und Internet-E-Mail zu gewähren. Sie werden ebenfalls in Erwägung ziehen, sensible Informationen von einem Standort an einen anderen zu übertragen. Schließlich planen Sie möglicherweise 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. Bei der Entwicklung Ihres eigenen Plans zur Internetnutzung kann sich die Seite *Szenario: e-business Pläne des Unternehmens JKL Toy* im IBM Systems Software Information Center als hilfreich erweisen. (Hinweis: 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* im IBM Systems Software Information Center 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.

Systemsicherheitsmerkmale des iSeries-Servers

Neben zahlreichen speziellen Sicherheitsangeboten zum Schutz Ihres Systems im Internet verfügt der iSeries-Server über Merkmale, die einen äußerst wirksamen Systemschutz bieten. Dazu gehören beispielsweise:

- 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 iSeries-Server kann eine Datei weder vorgeben, ein Programm zu sein, noch kann ein Programm ein anderes Programm ändern. Auf Grund von Integritätsmerkmalen der iSeries 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 eine bei Hackern beliebte Methode auf anderen Systemarchitekturen.

- Flexibilität, die Ihnen ermöglicht, den Systemschutz so zu gestalten, dass er Ihren speziellen Anforderungen gerecht wird. Über den Link @server Security Planner können Sie feststellen, welche Sicherheitsempfehlungen für Ihre Sicherheitsbedürfnisse in Frage kommen.

Spezielle Sicherheitsangebote der iSeries

Die iSeries 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:

- Virtual Private Networks (VPNs) stellen 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 i5/OS-Feature, das über die iSeries Navigator-Schnittstelle zugänglich ist. Weitere Informationen über VPNs finden Sie unter dem Thema "Virtual Private Networking (VPN)" im IBM Systems Software Information Center.
- Paketregeln sind ein integriertes Feature von i5/OS, das über iSeries Navigator zugänglich ist. Mit Hilfe dieses Features können Sie Regeln für IP-Paketfilter und die Netzwerkadresskonvertierung (Network Address Translation - NAT) konfigurieren, um den TCP/IP-Datenverkehr Ihres iSeries-Servers zu steuern. Weitere Informationen über die Paketregeln finden Sie unter dem Thema "Paketregeln" im IBM Systems Software Information Center.
- Das Sichern von Anwendungen mit SSL (Secure Sockets Layer) ermöglicht die Konfiguration von Anwendungen für SSL, um sichere Verbindungen zwischen Serveranwendungen und den entsprechenden Clients herzustellen. SSL wurde ursprünglich für sichere Webbrowser- und Serveranwendungen entwickelt, aber auch andere Anwendungen können für die Verwendung von SSL konfiguriert werden. Zahlreiche iSeries-Serveranwendungen sind jetzt SSL-fähig, darunter IBM HTTP-Server für iSeries, iSeries Access Express, FTP (File Transfer Protocol), Telnet und viele andere. Weitere Informationen über SSL finden Sie unter dem Thema "Securing applications with SSL" im IBM Systems Software Information Center.

Sobald Sie sich darüber im Klaren sind, wie Sie das Internet 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 Systemsicherheit.

Anmerkung: Detaillierte Informationen über den Einstieg ins Internet zu Geschäftszwecken finden Sie in folgenden Quellen:

- Unter dem Thema *Verbindung zum Internet* im IBM Systems Software Information Center.
- Im Redbook *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* (SG24-4929)

Zugehörige Konzepte

„Sicherheitsrichtlinien und Sicherheitsziele" auf Seite 7
Definieren, was geschützt werden soll und was von den Benutzern erwartet wird.

Internetsicherheit planen

Enthält Informationen, die Sie bei der Erstellung von Sicherheitsrichtlinien unterstützen, die Ihre Anforderungen bezüglich Internetsicherheit erfüllen.

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 sollten beispielsweise Folgendes dokumentieren und beschreiben:

- Ihre aktuelle Netzkonfiguration.
- Konfigurationsdaten für DNS und E-Mail-Server.
- Ihre Verbindung zum Internet-Service-Provider (ISP).
- Welche Internetdienste Sie nutzen möchten.
- Welche Internetdienste 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 Bedenken hinsichtlich vertraulicher Daten, die ungeschützt über das Internet transportiert werden. Das Abfangen und Verwerten 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 (Aktivierung von SSL (Secure Sockets Layer)).

Bei der Entwicklung Ihrer Internetnutzungs- und Sicherheitspläne können Ihnen die folgenden Themen behilflich sein:

- *Sicherheit durch mehrfache Abwehrstufen* enthält Informationen über die Problematik beim Erstellen eines umfassenden Sicherheitsplans.
- *Sicherheitsrichtlinien und Sicherheitsziele* enthält Informationen, die Ihnen bei der Entscheidung helfen, was Sie als Bestandteil Ihrer Sicherheitsrichtlinien dokumentieren sollen.
- *Szenario: e-business Pläne des Unternehmens JKL Toy* enthält ein praxisnahes Modell der Internetnutzungs- und Sicherheitspläne eines Unternehmens, das Sie beim Erstellen Ihrer eigenen Pläne nutzen können.

Sicherheit durch mehrfache Abwehrstufen

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.

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 der iSeries minimiert werden, sofern diese richtig konfiguriert sind. Bei der Anbindung Ihres iSeries-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 sollten 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 ein Angreifer, Ihren Arbeitsablauf zu stören oder zu stoppen, indem er den Datenverkehr umleitet oder Ihr System mit Junk-Nachrichten bombardiert.
  - Bei **verschlüsselten Attacken** versucht ein 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 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 sollten Maßnahmen beinhalten, die Schutz auf den folgenden Ebenen des traditionellen Network-Computing-Modells bieten. Ganz allgemein sollten Sie bei der Planung der Sicherheitsmaßnahmen von unten (Sicherheit auf Systemebene) nach oben (Sicherheit auf Transaktionsebene) vorgehen.

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. Sicherheitsstufen als Voraussetzung für Internetzugang beschreiben, welche Einstellungen Sie verwenden sollten, wenn Sie eine Internetverbindung herstellen.

Sicherheit auf Netzebene
Maßnahmen zur Netzsicherheit steuern den Zugriff auf Ihre iSeries und andere Systeme im Netz. Wenn Sie Ihr Netz mit dem Internet verbinden, sollten 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 und sollte 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 den allgemein zugänglichen Domain Name Service (DNS). Optionen für Netzsicherheit beschreiben die Sicherheitsmaßnahmen, die Sie zum Schutz der internen Ressourcen auf der Netzebene implementieren sollten.

Sicherheit auf Anwendungsebene

Sicherheitsmaßnahmen auf Anwendungsebene regeln, wie Benutzer mit bestimmten Anwendungen umgehen 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. Optionen für Anwendungssicherheit beschreiben neben den Sicherheitsrisiken auch die Möglichkeiten, wie diesen Risiken für zahlreiche populäre Internetanwendungen und -dienste begegnet werden kann.

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 Server, 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. Optionen für Übertragungssicherheit enthalten Informationen über die Sicherheitsmaßnahmen, die Sie zum Schutz Ihrer Daten implementieren können, wenn diese über ein ungesichertes Netz wie das Internet übertragen werden.

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 11
Beschreibt, welches Maß an Systemschutz vorhanden sein sollte, bevor Sie eine Verbindung zum Internet herstellen.

„Optionen für Netzsicherheit" auf Seite 12
Beschreibt die Sicherheitsmaßnahmen, die Sie auf Netzebene zum Schutz der internen Ressourcen treffen sollten.

„Optionen für Anwendungssicherheit" auf Seite 18
Enthält Informationen über die Sicherheitsrisiken für zahlreiche populäre Internetanwendungen und -dienste sowie über Maßnahmen, wie diesen Risiken begegnet werden kann.

„Optionen für Übertragungssicherheit" auf Seite 26
Enthält Informationen über die Sicherheitsmaßnahmen, die Sie zum Schutz Ihrer Daten implementieren können, wenn diese über ein ungesichertes Netz wie das Internet übertragen werden. Zu diesen Maßnahmen gehören SSL (Secure Sockets Layer), iSeries Access Express und VPN-Verbindungen (VPN - Virtual Private Network).

„Sicherheitsrichtlinien und Sicherheitsziele" auf Seite 7
Definieren, was geschützt werden soll und was von den Benutzern erwartet wird.

„E-Mail-Sicherheit" auf Seite 22
Die Verwendung von E-Mail im Internet oder anderen ungesicherten Netzen birgt Sicherheitsrisiken, vor denen eine Firewall möglicherweise nicht schützen kann.

Virtual private network (VPN)

„FTP-Sicherheit” auf Seite 24
Mit Hilfe von FTP (File Transfer Protocol) können Dateien zwischen einem Client (einem Benutzer auf einem anderen System) und Ihrem Server übertragen werden.

Zugehörige Verweise

Terminologie zum Thema Sicherheit

Sicherheitsrichtlinien und Sicherheitsziele

Definieren, was geschützt werden soll und was von den Benutzern erwartet wird.

Ihre Sicherheitsrichtlinien

Jeder Internetdienst, den Sie nutzen oder anbieten, birgt Risiken für Ihr iSeries-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. Sobald Sie Sicherheitsrichtlinien erstellen, müssen Sie 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. Ein Beispiel für die Sicherheitsrichtlinien des Unternehmens JKL Toy finden Sie im IBM Systems Software Information Center unter dem Thema ″Systemsicherheit und Planung″.

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 der iSeries. 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 Anmeldeverfah-

ren 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 möglicherweise Sicherheitsvorkehrungen mit den folgenden Zielen erforderlich:

  – 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, erwartete Ergebnisse mit erwartetem Durchsatz. Bei der iSeries wird die Systemintegrität als Sicherheitskomponente meist übersehen, da sie ein wesentlicher Bestandteil der iSeries-Architektur ist. Die iSeries-Architektur macht es beispielsweise einem Störenfried extrem schwer, ein Betriebssystemprogramm zu imitieren oder zu ändern, wenn Sicherheitsstufe 40 oder 50 verwendet wird.

Unbestreitbarkeit
Die Unbestreitbarkeit ist ein 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 stattgefunden hat. 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 mittels digitaler Zertifikate und Secure Socket Layer (SSL) 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 gewährleisten möchten, die Ihr Netz verlassen.

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.

Wenn Sie sich über die Sicherheitsziele im Klaren sind, können Sie Sicherheitsrichtlinien erarbeiten, die alle Ihre Sicherheitsanforderungen hinsichtlich Netzbetrieb und Internet umfassen. Bei der Definition

Ihrer Ziele und dem Erstellen Ihrer Sicherheitsrichtlinien kann Ihnen möglicherweise das Szenario: e-business Pläne des Unternehmens JKL Toy behilflich sein. Die Internetnutzungsplanung und die Sicherheitsplanung des Beispielunternehmens sind ein repräsentatives Modell für viele reale Unternehmen.

Zugehörige Konzepte

„iSeries und Überlegungen zur Internetsicherheit" auf Seite 2
Bietet einen Überblick über die Sicherheitsfunktionen und -angebote der iSeries.

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

Konfiguration von DCM

Secure Socket Layer (SSL)

„Szenario: e-business Pläne des Unternehmens JKL Toy"
Beschreibt ein typisches Unternehmen (JKL Toy), das seine Unternehmensziele mittels Internet ausweiten möchte. Auch wenn es sich hierbei nur um ein fiktives Unternehmen handelt, sind doch die Pläne zur Nutzung des Internets für e-business und des sich daraus ergebenden Sicherheitsbedürfnisses repräsentativ für zahlreiche reale Unternehmen.

Szenario: e-business Pläne des Unternehmens JKL Toy

Beschreibt ein typisches Unternehmen (JKL Toy), das seine Unternehmensziele mittels Internet ausweiten möchte. Auch wenn es sich hierbei nur um ein fiktives Unternehmen handelt, sind doch die Pläne zur Nutzung des Internets für e-business und des sich daraus ergebenden Sicherheitsbedürfnisses repräsentativ für zahlreiche reale Unternehmen.

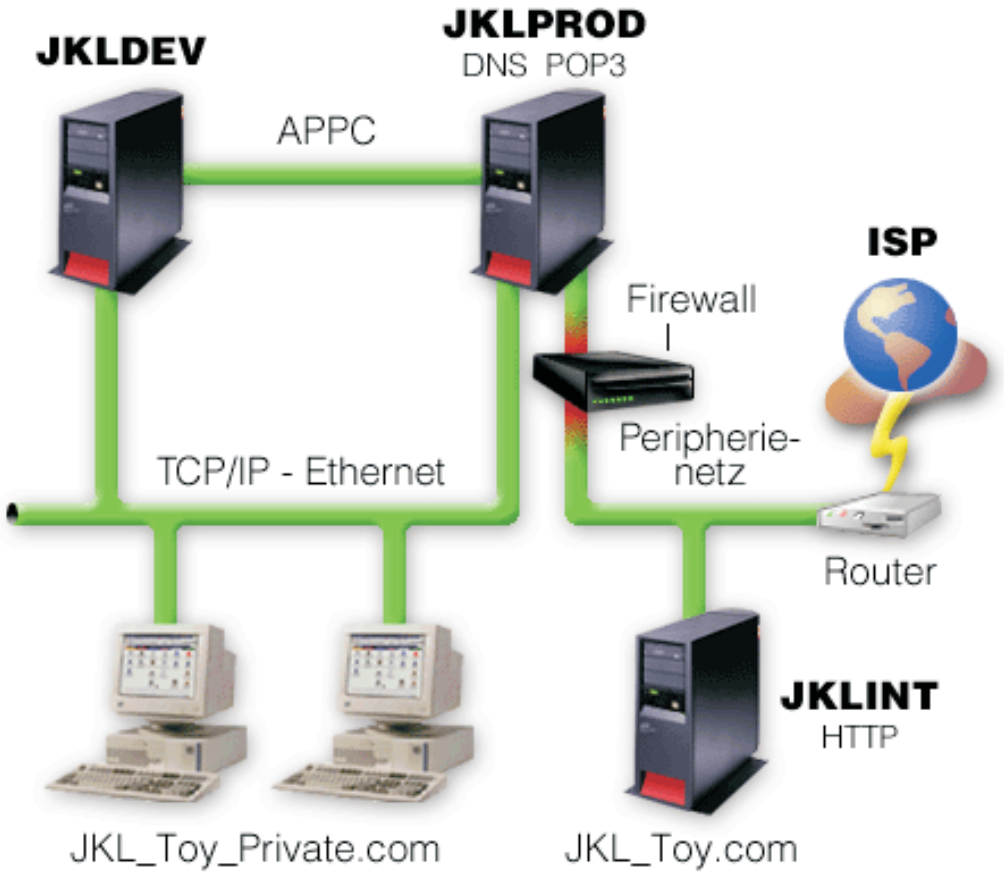
Das Unternehmen JKL Toy ist ein zwar kleiner, jedoch rasch wachsender Spielwarenhersteller, dessen Palette vom Springseil über Papierdrachen bis hin zum Plüschleoparden reicht. Der Firmenchef zeigt sich begeistert über das Wachstum des Unternehmens und darüber, wie die dadurch verursachten Gemeinkosten durch das neue iSeries-System in Grenzen gehalten werden können. Sharon Jones, Leiterin des Rechnungswesens, ist für die Systemverwaltung und -sicherheit der iSeries 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 zeichnet 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 die iSeries-Server über einen wirksamen Basissystemschutz verfügen, hat sich JKL Toy dafür entschieden, ein Firewallprodukt für die Sicherheit auf Netzebene einzusetzen. Die Firewall schirmt das interne Netz vor zahlreichen potenziellen Internetrisiken ab. Im Folgenden finden Sie eine Darstellung der Internet-/Netzkonfiguration des Unternehmens.



Wie aus dem Diagramm ersichtlich, verfügt das Unternehmen JKL Toy über zwei primäre iSeries-Server. Ein System wird für Entwicklungsanwendungen, das andere für Produktionsanwendungen (JKLDEV bzw. JKLPROD) eingesetzt. Auf beiden Systemen werden unternehmenskritische Daten und Anwendungen verarbeitet.

Daher gibt es Bedenken, die Internetanwendungen ebenfalls auf diesen Systemen auszuführen. Stattdessen soll ein neuer iSeries-Server (JKLINT) hinzugefügt werden, auf dem diese Anwendungen laufen sollen.

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 die neue iSeries ausschließlich als Internet-Server fungiert, gestaltet sich außerdem die Verwaltung der gesamten Netzsicherheit weniger kompliziert.

Das Unternehmen führt zu diesem Zeitpunkt keine unternehmenskritischen Anwendungen auf dem neuen iSeries-Server 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 7
Definieren, was geschützt werden soll und was von den Benutzern erwartet wird.

„Optionen für Netzsicherheit" auf Seite 12
Beschreibt die Sicherheitsmaßnahmen, die Sie auf Netzebene zum Schutz der internen Ressourcen treffen sollten.

„Optionen für Übertragungssicherheit" auf Seite 26
Enthält Informationen über die Sicherheitsmaßnahmen, die Sie zum Schutz Ihrer Daten implementieren können, wenn diese über ein ungesichertes Netz wie das Internet übertragen werden. Zu diesen Maßnahmen gehören SSL (Secure Sockets Layer), iSeries Access Express und VPN-Verbindungen (VPN - Virtual Private Network).

Sicherheitsstufen als Voraussetzung für Internetzugang

Beschreibt, welches Maß an Systemschutz vorhanden sein sollte, bevor Sie eine Verbindung zum Internet herstellen.

Ihre Maßnahmen zum Systemschutz bilden die letzte Verteidigungslinie gegen ein internetbasiertes Sicherheitsproblem. Daher muss der erste Schritt beim Aufbau einer umfassenden Internetsicherheitsstrategie 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 dringend empfohlen wird. Detailliertere Informationen zu jeder iSeries-Sicherheitsstufe finden Sie unter Plan and set up system security.

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

- Setzen Sie Ihre sicherheitsrelevanten Systemwerte auf Werte, die mindestens den empfohlenen Einstellungen entsprechen. Mit dem iSeries 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 **@server Security Planner** (verfügbar über die Website des IBM Systems Software Information Center) oder den **Sicherheitsassistenten** (verfügbar über die iSeries Navigator-Schnittstelle) 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. Der Sicherheitsassistent gibt Ihnen, ausgehend von Ihren Ant-

worten auf eine Reihe von Fragen, ebenfalls Empfehlungen. Im Unterschied zum Security Advisor können Sie den Assistenten jedoch anweisen, anhand dieser Empfehlungen die Systemsicherheitseinstellungen für Sie zu konfigurieren.

Zahlreiche Risiken können mit Hilfe der internen Sicherheitseinrichtungen der iSeries minimiert werden, sofern diese richtig konfiguriert und verwaltet werden. Wenn Sie Ihre iSeries mit dem Internet verbinden, müssen Sie jedoch zusätzliche Sicherheitsmaßnahmen ergreifen, um die Sicherheit Ihres internen Netzes zu gewährleisten. Nachdem Sie sichergestellt haben, dass Ihre iSeries über einen guten allgemeinen Systemschutz verfügt, 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 Informationen

iSeries Security Reference

Optionen für Netzsicherheit

Beschreibt die Sicherheitsmaßnahmen, die Sie auf Netzebene zum Schutz der internen Ressourcen treffen sollten.

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.

Auch Ihr Internet-Service-Provider (ISP) kann und sollte ein wichtiger Bestandteil Ihres Netzsicherheitsplans sein. Ihre Methode zur Netzsicherung sollte die vom ISP gebotenen Sicherheitsmaßnahmen umreißen, wie beispielsweise Filterregeln für die ISP-Routerverbindung und Vorkehrungen für den öffentlichen Domain Name Service (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.

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, 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.

Wann immer Sie Ihren iSeries-Server oder Ihr internes Netz mit dem Internet verbinden, ziehen Sie auf jeden Fall den Einsatz eines Firewallprodukts als wichtigste Abwehrmaßnahme in Betracht. Das Produkt IBM Firewall for AS/400 ist zwar nicht mehr lieferbar, und es gibt auch keine Produktunterstützung mehr, aber es stehen zahlreiche andere Produkte zur Auswahl. Szenarien zu verschiedenen Migrationsoptionen finden Sie unter "All You Need to Know When Migrating from IBM Firewall for AS/400".

Da kommerzielle Firewallprodukte eine breite Palette von Technologien für die Netzsicherheit bieten, hat sich das Unternehmen JKL Toy in seinem e-business Sicherheitsszenario dafür entschieden, ein solches Produkt zum Schutz des Netzes einzusetzen. Die Firewall bietet jedoch keinerlei Schutz für den neuen iSeries-Internet-Server. Folglich hat sich das Unternehmen dafür entschieden, das iSeries-Feature Paketregeln zu implementieren, um Filter- und NAT-Regeln zu erstellen, die den Datenverkehr für den Internet-Server steuern.

iSeries-Paketregeln

Paketfilterregeln können Ihre Computersysteme insofern schützen, als 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, wobei eine IP-Adresse durch eine andere, öffentliche IP-Adresse ersetzt 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 iSeries-Feature Paketregeln zu entscheiden.

Unter dem Thema ″Optionen für iSeries-Netzsicherheit wählen″ finden Sie Informationen, die Ihnen helfen, die für Ihre Sicherheitsanforderungen geeignete Lösung zu finden.

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 9
Beschreibt ein typisches Unternehmen (JKL Toy), das seine Unternehmensziele mittels Internet ausweiten möchte. Auch wenn es sich hierbei nur um ein fiktives Unternehmen handelt, sind doch die Pläne zur Nutzung des Internets für e-business und des sich daraus ergebenden Sicherheitsbedürfnisses repräsentativ für zahlreiche reale Unternehmen.

„iSeries-Paketregeln” auf Seite 15
Die Paketregeln von iSeries sind ein integriertes Feature von i5/OS, das über die iSeries Navigator-Schnittstelle zugänglich ist.

„Optionen für iSeries-Netzsicherheit wählen” auf Seite 17
Enthält einen kurze Erörterung der Sicherheitsoptionen, für die Sie sich auf der Grundlage Ihrer Internetnutzungspläne entscheiden sollten.

Zugehörige Informationen

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

- ermöglicht Benutzern in Ihrem internen Netz den Zugriff auf ausgewählte Ressourcen, die sich in dem externen Netz befinden.
- verweigert unbefugten Benutzern im externen Netz den Zugriff auf Ressourcen, die sich in Ihrem internen Netz befinden.

Wenn Sie eine Firewall als Gateway zum Internet (oder einem anderen Netz) verwenden, verringern Sie das Risiko für Ihr internes Netz erheblich. 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 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 Services (DNS)
  - Protokollierung
  - Echtzeitüberwachung

Anmerkung: Einige Firewalls stellen VPN-Dienste (Virtual Private Networking) 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 einen öffentlichen Server 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 Abwehrmaßnahmen 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, 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.

iSeries-Paketregeln

Die Paketregeln von iSeries sind ein integriertes Feature von i5/OS, das über die iSeries Navigator-Schnittstelle zugänglich ist.

Mit Hilfe der Paketregeln können Sie zum Schutz Ihres iSeries-Systems zwei der wichtigsten Netzsicherheitstechnologien konfigurieren, um den TCP/IP-Datenverkehr zu steuern:

- Netzwerkadresskonvertierung (NAT)
- IP-Paketfilterung

Da NAT und IP-Filterung integrierte i5/OS-Bestandteile 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: Handelt es sich bei dem zu schützenden iSeries-System um ein Produktionssystem, sollten Sie sich nicht von den Kosteneinsparungen allein leiten lassen. In einem solchen Fall sollte die absolute Sicherheit Ihres Systems Vorrang vor den Kosten haben. Um sicherzugehen, dass Sie Ihrem Produktionssystem den maximal möglichen Schutz bieten, sollten Sie den Einsatz einer Firewall in Betracht ziehen.

Bedeutung und Zusammenwirken von NAT 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 iSeries-System 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 Webservers hinter einer Firewall erleichtern. Öffentliche IP-Adressen für den Webserver 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 iSeries Navigator können Sie schnell und einfach Grundregeln für das Filtern konfigurieren, um unerwünschten Datenaustausch auf dem Netz zu blockieren.

IP-Paketfilterung kann für folgende Zwecke 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 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. Sobald die Informationen in ein Systemjournal aufgenommen werden, kann der Protokolleintrag nicht mehr geändert werden. Aus diesem Grund ist das Protokoll ein ideales Tool zur Überwachung der Netzaktivität.

Zugehörige Konzepte

„Optionen für Netzsicherheit" auf Seite 12
Beschreibt die Sicherheitsmaßnahmen, die Sie auf Netzebene zum Schutz der internen Ressourcen treffen sollten.

Netzwerkadresskonvertierung (NAT)

IP-Paketfilterung

Optionen für iSeries-Netzsicherheit wählen

Enthält einen kurze Erörterung der Sicherheitsoptionen, für die Sie sich auf der Grundlage Ihrer Internetnutzungspläne entscheiden sollten.

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 iSeries-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 iSeries Proxy-Server.

Ob Sie sich für das Feature "Paketregeln" oder eine Firewall entscheiden, hängt von Ihrer Netzumgebung, den Zugriffsbedürfnissen und den Sicherheitsbedürfnissen ab. Sie sollten **unbedingt** die Verwendung eines Firewallprodukts als wichtigste Abwehrmaßnahme in Betracht ziehen, wenn Sie Ihren iSeries-Server oder Ihr internes Netz mit dem Internet oder einem anderen ungesicherten Netz verbinden.

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.

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 Ihrer iSeries umgeht, hat er potenziell Zugriff auf eine Vielzahl nützlicher Anwendungen, Dienste und Daten. Der Angreifer kann diese dann benutzen, um erheblichen Schaden auf dem System selbst anzurichten oder Zugriff auf andere Systeme in Ihrem internen Netz zu erlangen.

Es stellt sich daher die Frage, ob es überhaupt jemals akzeptabel ist, die TCP/IP-Sicherheitseinrichtungen der iSeries zu verwenden. 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 sollten.

Sicherheitstechnologie	Verwendung der TCP/IP-Technologie von i5/OS	Verwendung einer mit allen Funktionen ausgestatteten Firewall
IP-Paketfilterung	• **Zusätzlicher** Schutz für einen einzelnen iSeries-Server, z. B. einen allgemein zugänglichen Webserver oder ein Intranetsystem mit sensiblen Daten. • Schutz für ein Teilnetz eines unternehmensweiten **Intranets**, wenn der iSeries-Server als Gateway (gewöhnlicher Router) für das restliche Netz fungiert. • Steuerung der Kommunikation mit einem vertrauenswürdigen Partner über ein **privates Netz** oder ein Extranet, wobei der iSeries-Server 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**.

Weitere Informationen über die Verwendungsweise der TCP/IP-Sicherheitseinrichtungen von i5/OS finden Sie in folgenden Quellen:

- Thema *Packet rules (filtering and NAT)* im IBM Systems Software Information Center von V5R1.
- *HTTP Server Documentation Center* unter dieser URL:
  `http://www.iseries.ibm.com/domino/reports.htm`
- Redbook AS/400 Internet Security Scenarios: A Practical Approach (SG24-5954).

Zugehörige Konzepte

„Optionen für Netzsicherheit" auf Seite 12
Beschreibt die Sicherheitsmaßnahmen, die Sie auf Netzebene zum Schutz der internen Ressourcen treffen sollten.

Optionen für Anwendungssicherheit

Enthält Informationen über die Sicherheitsrisiken für zahlreiche populäre Internetanwendungen und -dienste sowie über Maßnahmen, wie diesen Risiken begegnet werden kann.

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, 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.

Weitere Informationen über die von Ihnen zu ergreifenden Sicherheitsmaßnahmen für zahlreiche Internetanwendungen finden Sie auf den folgenden Seiten:

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 Webserving

Wenn Sie Besuchern Zugriff auf Ihre Website bieten, sollen Informationen über den Aufbau der Site und die Codierung, mit der die Seite generiert wurde, außen vor bleiben.

Der Besuch Ihrer Seite soll einfach, schnell und reibungslos erfolgen; die Verarbeitung, die dahinter steht, soll hinter den Kulissen ablaufen. Als Administrator möchten Sie sicherstellen, dass Ihre Sicherheitsmaßnahmen keinen negativen Einfluss auf die Website haben. Wenn Sie die iSeries als Webserver einsetzen, sollten Sie folgende Punkte beachten:

- Der Serveradministrator muss Direktiven für den Server definieren, bevor ein Client mit dem HTTP-Server interagieren kann. Zum Erstellen von Sicherheitsüberprüfungen gibt es zwei Methoden: allgemeine Serverdirektiven und Serverschutzdirektiven. Alle Anforderungen an den Webserver müssen sämtliche Rahmenbedingungen dieser Direktiven erfüllen, bevor der Server die Anforderung annimmt.
- Diese Direktiven können mit Hilfe der Verwaltungswebseiten für die Serverkonfiguration erstellt und bearbeitet werden. Serverdirektiven geben Ihnen die Möglichkeit, das gesamte Verhalten des Webservers zu steuern. Serverschutzdirektiven geben Ihnen die Möglichkeit, die Sicherheitsmodelle zu definieren und zu steuern, die der Server für die jeweiligen URLs verwendet, die vom Webserver verwaltet werden.
- Der Server kann unter Verwendung von Zuordnungs- oder Übergabedirektiven (MAP- bzw. PASS-Direktiven) sowie der Verwaltungswebseiten konfiguriert werden.
  - Verwenden Sie Zuordnungs- oder Übergabedirektiven, um die Dateinamen auf Ihrem iSeries-Webserver zu maskieren. Genauer gesagt, es gibt PASS- und MAP-Serverdirektiven, die die Verzeichnisse steuern, die der Webserver für die Bereitstellung der URLs benötigt. Es ist auch eine EXEC-Serverdirektive vorhanden, die die Bibliotheken steuert, in denen sich CGI-BIN-Programme befinden.

    Schutzdirektiven werden für jede Server-URL definiert. Zwar benötigen nicht alle URLs eine Schutzdirektive, doch wenn Sie steuern möchten, wie oder von wem auf eine URL-Ressource zugegriffen wird, dann ist eine Schutzdirektive für diese URL erforderlich.
  - Außerdem können Sie für die Serverkonfiguration die Verwaltungswebseiten verwenden, statt den Befehl WRKHTTPCFG (Mit HTTP-Konfiguration arbeiten) und die Direktiven einzugeben. Das Arbeiten mit Schutzdirektiven über die Befehlszeilenschnittstelle kann sehr kompliziert sein. Daher ist es empfehlenswert, die Verwaltungswebseiten zu verwenden, um sicherzustellen, dass Sie Ihre Direktiven korrekt definieren.

HTTP bietet Ihnen zwar die Möglichkeit, Daten anzuzeigen, nicht jedoch, Daten in einer Datenbankdatei zu ändern. Sie werden jedoch einige Anwendungen erstellen, für die eine Datenbankdatei aktualisiert werden muss. Dazu können Sie dann CGI-BIN-Programme verwenden. Es kann beispielsweise sein, dass Sie Formulare erstellen möchten, mit denen eine iSeries-Datenbank aktualisiert wird, nachdem sie vom Benutzer ausgefüllt wurden. Als Sicherheitsadministrator müssen Sie die Berechtigungen für dieses Benutzerprofil und die Funktionen überwachen, die von den CGI-Programmen ausgeführt werden. Denken Sie auch daran festzustellen, welche sensiblen Objekte eine ungeeignete allgemeine Berechtigung haben könnten.

Anmerkung: Common Gateway Interface (CGI) ist ein Branchenstandard für den Austausch von Informationen zwischen einem Webserver und externen Computerprogrammen. Die Pro-

gramme können in einer beliebigen Programmiersprache erstellt sein, die von dem Betriebssystem unterstützt wird, unter dem der Webserver läuft.

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

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

Der Proxy-Server empfängt HTTP-Anforderungen von Webbrowsern und leitet Sie an Webserver weiter. Webserver, die diese Anforderungen empfangen, kennen nur die IP-Adresse des Proxy-Servers. Die Namen und Adressen der PCs, von denen die Anforderungen ursprünglich stammen, können diese Webserver nicht feststellen. Der Proxy-Server kann URL-Anforderungen für HTTP, FTP (File Transfer Protocol), Gopher und WAIS verarbeiten.

Sie können auch die HTTP-Proxy-Unterstützung des IBM HTTP-Servers für iSeries verwenden, um den Webzugriff zu konsolidieren. Der Proxy-Server kann außerdem alle URL-Anforderungen protokollieren, die Überwachungszwecken dienen. Anhand dieser Protokolle können Sie Gebrauch und Missbrauch von Netzressourcen überprüfen. Weitere Informationen über die Verwendung des HTTP-Proxy-Servers finden Sie im Documentation Center des IBM HTTP-Servers für iSeries unter der URL:

| `http://www.ibm.com/eserver/iseries/products/http/docs/doc.htm`

Zugehörige Konzepte

„Java-Internetsicherheit"
In den IT-Umgebungen von heute nimmt die Java-Programmierung mehr und mehr zu.

Java-Internetsicherheit

In den IT-Umgebungen von heute nimmt die Java-Programmierung mehr und mehr zu.

Sie verwenden vielleicht bereits die IBM Toolbox for Java oder das IBM Development Kit for Java auf Ihrem System, um neue Anwendungen zu entwickeln. Folglich müssen Sie 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 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 sollten die gleichen Sicherheitsregeln für die Anwendungsentwicklung beachten, die auch für andere Sprachen auf Ihrem iSeries-Server gelten.

Java-Applets

Java-Applets sind kleine Java-Programme, die in HTML-Seiten integriert werden können. Da Applets auf dem Client ausgeführt werden, ist das, was sie bewirken, Sache des Clients. Ein Java-Applet bietet jedoch die Möglichkeit, auf Ihren iSeries-Server zuzugreifen. (Ein ODBC-Programm oder ein APPC-Programm (Advanced Program-to-Program Communications), das auf einem PC in Ihrem Netz betrieben wird, kann ebenfalls auf Ihre iSeries zugreifen.) Im Allgemeinen können Java-Applets nur mit dem Server eine Sit-

zung aufbauen, von dem das Applet ursprünglich stammt. Daher kann ein Java-Applet nur dann von einem angeschlossenen PC aus auf Ihre iSeries zugreifen, wenn das Applet von Ihrem iSeries-Server stammt (beispielsweise von Ihrem Webserver).

Ein Applet kann versuchen, zu jedem TCP/IP-Port auf einem Server eine Verbindung herzustellen. Es muss keinen Kontakt zu einem Software-Server aufnehmen, der in Java erstellt wurde. Bei Servern, 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 Server herstellt. Alle in dieser Veröffentlichung beschriebenen Server sind iSeries-Server. (Ein in Java erstellter Server 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 iSeries-Server 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 im Benutzerprofil unbeachtet.

Mit Hilfe des Applet-Viewers können Sie ein Applet auf dem Serversystem testen; er ist dabei jedoch nicht den Sicherheitsbeschränkungen eines Browsers unterworfen. Sie sollten den Applet-Viewer deshalb nur zum Testen Ihrer eigenen Applets einsetzen, und niemals, um Applets von externen Quellen auszuführen. Java-Applets schreiben häufig auf das PC-Laufwerk des Benutzers, wodurch das Applet die Gelegenheit erhalten kann, 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 iSeries-Servers schreiben, da sich diese dem PC gegenüber wie lokale Laufwerke darstellen.

Anmerkung: Das oben beschriebene Verhalten gilt normalweise für Netscape Navigator und MS Internet Explorer. Was im Einzelnen stattfindet, hängt davon ab, wie Sie die von Ihnen verwendeten Browser konfigurieren und verwalten.

Für Java-Applets, die von Ihrem iSeries-Server stammen, müssen Sie möglicherweise signierte Applets einsetzen. Sie sollten 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 verwenden, um registrierte Java-Programme für die Verwendung von SSL zu konfigurieren.

Java-Servlets

Servlets sind serverseitige, in Java erstellte Komponenten, die die Funktionalität eines Webservers dynamisch erweitern, ohne dessen Code zu ändern. Der IBM WebSphere Application Server, der zum Lieferumfang des IBM HTTP-Servers für iSeries gehört, bietet Unterstützung für die Verwendung von Servlets auf iSeries-Systemen.

Auf Servlet-Objekte, die vom Server verwendet werden, muss der Ressourcenschutz angewendet werden. Der Ressourcenschutz kann ein Servlet jedoch nicht ausreichend schützen. Wenn ein Webserver ein Servlet lädt, verhindert der Ressourcenschutz nicht, dass andere dieses Servlet ebenfalls ausführen. Folglich sollten 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 Webservers ausgeführt werden können. Sie sollten zusätzlich mit Hilfe von HTTP-Servergruppen und

Zugriffssteuerungslisten (ACL) kontrollieren, wer das Servlet ausführen darf (Schlüsselwörter in der Schutzdirektive maskieren). Auch sollten Sie die Sicherheitseinrichtungen Ihrer Servlet-Entwicklungstools nutzen, wie sie beispielsweise im WebSphere Application Server for iSeries enthalten sind.

Weitere Informationen über allgemeine Sicherheitsmaßnahmen für Java finden Sie unter den folgenden Themen im IBM Systems Software Information Center.

- Java Security for the *IBM Developer Kit for Java*
- Security classes for the *IBM Toolbox for Java*

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 iSeries-System läuft, zugeordnet werden kann. Nachfolgende Ressourcenschutzüberprüfungen finden unter der zugeordneten Identität statt. Detaillierte Informationen zu diesen Sicherheitsklassen finden Sie unter dem Thema IBM Toolbox for Java Authentication Services im IBM Systems Software Information Center.

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). Weitere Informationen zum J2SDK finden Sie unter dem Thema Java Authentication and Authorization Service for the IBM Developer Kit for Java im in the IBM Systems Software Information Center.

Java-Anwendungen mit SSL sichern

Mit Hilfe von SSL (Secure Sockets Layer) kann die Übertragung für iSeries-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.

Weitere Informationen über die SSL-Verwaltung für Java-Anwendungen finden Sie unter den folgenden Themen im IBM Systems Software Information Center:

- IBM Toolbox for Java Secure Sockets Layer (SSL) environment
- IBM Developer Toolkit for Java to make a Java application secure with SSL

Zugehörige Konzepte

„Sicherheit für Webserving" auf Seite 19
Wenn Sie Besuchern Zugriff auf Ihre Website bieten, sollen Informationen über den Aufbau der Site und die Codierung, mit der die Seite generiert wurde, außen vor bleiben.

Konfiguration von DCM

Authentication Services

Zugehörige Tasks

Make a Java application secure with SSL

Zugehörige Informationen

Java Authentication and Authorization Service

Secure Sockets Layer (SSL) environment

E-Mail-Sicherheit

Die Verwendung von E-Mail im Internet oder anderen ungesicherten Netzen birgt Sicherheitsrisiken, vor denen eine Firewall möglicherweise nicht schützen kann.

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 äußerst wichtig, beim Versenden vertraulicher Informationen über E-Mail besonnen vorzugehen. Da eine E-Mail zahlreiche Server durchläuft, bevor Sie sie erhalten, besteht für Dritte die Gelegenheit, die Mail abzufangen und zu lesen. Daher werden Sie Sicherheitsmaßnahmen ergreifen wollen, 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 der Server nicht mehr reagiert, da sämtliche Serverressourcen 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 Server, bevor sie den gewünschten Empfänger erreicht. Wenn Sie Ihre Nachricht nicht verschlüsselt haben, kann ein Hacker Ihre 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 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.

Detaillierte Informationen zu Sicherheitseinrichtungen für Domino auf der iSeries finden Sie in folgenden Quellen:

- Lotus Domino Referenzbibliothek unter dieser URL:
  `http://www.ibm.com/eserver/iseries/domino/library.htm`
- Lotus Notes and Domino R5.0 Security Infrastructure Revealed (SG24-5341)
- Lotus Domino for AS/400 Internet Mail and More (SG24-5990)

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. Ab V4R4 können Sie mit Ihrer iSeries verschiedene VPN-Verbindungen konfigurieren, zu denen auch Verbindungen zwischen fernen Clients und Ihrem iSeries-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

Virtual private network (VPN)

„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.

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

Zugehörige Verweise

Terminologie zum Thema Sicherheit

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 können außerdem die Funktion für ferne Befehle (Remote Command) verwenden, um Befehle an den Server zu übergeben. Aus diesem Grund bietet sich FTP besonders 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. Sie müssen diese Risiken kennen, damit Sie in Ihren Sicherheitsrichtlinien auch beschreiben können, wie diese Risiken minimiert werden sollen.

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

  Beispiel: Die allgemeine Berechtigung für Ihre Objekte ist *USE, 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 iSeries-Objektsicherheit auf dem System (mit anderen Worten: Ändern Sie das Sicherheitsmodell des Systems von ″Menüschutz″ in ″Objektschutz″). Dies ist die beste und sicherste Option, die Ihnen zur Verfügung steht.
– Schreiben Sie Exitprogramme für FTP, um den Zugriff auf Dateien zu beschränken, die über FTP übertragen werden können. Diese Exitprogramme sollten mindestens das gleiche Maß an Schutz bieten wie das Menüprogramm. Viele Kunden werden wahrscheinlich eine noch restriktivere FTP-Zugriffssteuerung wünschen. Diese Maßnahme gilt nur für FTP, nicht für andere Schnittstellen wie ODBC, DDM oder DRDA.

  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 sollten:
  – 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** 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 haben Sie auch die Möglichkeit, 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 sollten Sie die Sicherheitsrisiken abwägen und in Erwägung ziehen, Ihren FTP-Server mit Exitprogrammen zu sichern.

- Anonymes FTP konfigurieren
- Zugriff mit FTP-Exitprogrammen verwalten

Weitere Informationen über die Verwendung und Risiken von FTP sowie über die verfügbaren Sicherheitsmaßnahmen finden Sie in folgenden Quellen:

- Unter dem Thema ″Implementing FTP security″ im IBM Systems Software Information Center.
- Unter dem Thema ″Anonymous FTP″ im IBM Systems Software Information Center.
- Unter dem Thema ″Securing FTP with SSL″ im IBM Systems Software Information Center.

Zugehörige Konzepte

„E-Mail-Sicherheit" auf Seite 22
Die Verwendung von E-Mail im Internet oder anderen ungesicherten Netzen birgt Sicherheitsrisiken, vor denen eine Firewall möglicherweise nicht schützen kann.

Virtual private network (VPN)

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

Intrusion detection

Zugehörige Verweise

Terminologie zum Thema Sicherheit

Optionen für Übertragungssicherheit

Enthält Informationen über die Sicherheitsmaßnahmen, die Sie zum Schutz Ihrer Daten implementieren können, wenn diese über ein ungesichertes Netz wie das Internet übertragen werden. Zu diesen Maßnahmen gehören SSL (Secure Sockets Layer), iSeries Access Express und VPN-Verbindungen (VPN - Virtual Private Network).

Wie bereits erwähnt, verfügt das Unternehmen JKL Toy (Szenario) über zwei primäre iSeries-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 iSeries-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 die neue iSeries ausschließlich als Internet-Server 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, sollten 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 iSeries auf Übertragungsebene minimiert werden: Gesicherte SSL-Kommunikation (Secure Sockets Layer) und VPN-Verbindungen (Virtual Private Networking).

Securing applications with SSL

Das SSL-Protokoll (Secure Sockets Layer) ist de facto ein Branchenstandard für das Sichern der Kommunikation zwischen Clients und Servern. SSL wurde ursprünglich für Webbrowseranwendungen entwickelt, doch eine zunehmende Zahl weiterer Anwendungen kann jetzt auch SSL verwenden. Dazu gehören beim iSeries-Server folgende Anwendungen:

- IBM HTTP-Server für iSeries (Original und auf Apache-Basis)
- FTP-Server
- Telnet-Server
- DRDA (Distributed Relational Database Architecture) und Verwaltung für verteilte Daten
- (DDM)-Server
- Management Central in iSeries Navigator
- Directory Services Server (LDAP)
- iSeries Access Express-Anwendungen, einschließlich iSeries Navigator, und Anwendungen, die für die APIs (Anwendungsprogrammierschnittstellen) von iSeries Access Express 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.

iSeries Virtual Private Networking (VPN)

Mit den VPN-Verbindungen des iSeries-Systems 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.

Welche Methode ist für Sie geeignet?

Beide Sicherheitsmethoden 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 noch nicht nutzen können,

verfügen viele andere, wie beispielsweise Telnet und iSeries Access Express, bereits 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 Webserver in Ihrem internen Netz zu gestatten. Wenn der Webserver 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. Es kann auch die Situation vorliegen, 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 könnten Sie eine VPN-Verbindung von Gateway zu Gateway für diesen Teil des Netzes erstellen. Der Datenverkehr würde damit geschützt, 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 9
Beschreibt ein typisches Unternehmen (JKL Toy), das seine Unternehmensziele mittels Internet ausweiten möchte. Auch wenn es sich hierbei nur um ein fiktives Unternehmen handelt, sind doch die Pläne zur Nutzung des Internets für e-business und des sich daraus ergebenden Sicherheitsbedürfnisses repräsentativ für zahlreiche reale Unternehmen.

„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.

„Virtual Private Networks (VPN) für sichere private Kommunikation" auf Seite 30
Sie können ein VPN (Virtual Private Network) verwenden, um vertraulich und sicher innerhalb Ihres Unternehmens zu kommunizieren.

Zugehörige Verweise

Secure Sockets Layer APIs

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 iSeries-Server 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 iSeries, so konfigurieren, dass sie statt Benutzername und Kennwort digitale Zertifikate als striktere Methode zur Clientauthentifizierung verwenden.

Was ist ein 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, die festlegen, 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 Servers, 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.

Weitere Informationen zur Verwendung von Digital Certificate Manager finden Sie im IBM Systems Software Information Center.

Obwohl zahlreiche Anwendungen SSL noch nicht nutzen können, verfügen viele andere, wie beispielsweise Telnet und iSeries Access Express, bereits über eine SSL-Funktion. Informationen zur Nutzung von SSL für iSeries-Anwendungen finden Sie unter dem Thema **Securing applications with SSL** im IBM Systems Software Information Center.

Zugehörige Konzepte

„Optionen für Übertragungssicherheit" auf Seite 26
Enthält Informationen über die Sicherheitsmaßnahmen, die Sie zum Schutz Ihrer Daten implementieren können, wenn diese über ein ungesichertes Netz wie das Internet übertragen werden. Zu diesen Maßnahmen gehören SSL (Secure Sockets Layer), iSeries Access Express und VPN-Verbindungen (VPN - Virtual Private Network).

Konfiguration von DCM

Securing applications with SSL

Zugehörige Verweise

Terminologie zum Thema Sicherheit

SSL 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. Sobald die SSL-Sitzung hergestellt ist, 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 iSeries-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. Die Inaktivierung der Ports erfolgt mit dem Befehl ADDTCPPORT. Sobald der Port ausgeschaltet ist, stellt der Server den Clients Telnet ohne SSL zur Verfügung, und die SSL-Telnet-Sitzungen werden inaktiviert.

Weitere Informationen über Telnet und Sicherheitstipps für Telnet mit und ohne SSL finden Sie unter dem Thema zu Telnet im IBM Systems Software Information Center. Dieses Thema enthält die Informationen, die Sie benötigen, um Telnet auf Ihrem iSeries-Server zu verwenden.

Zugehörige Konzepte

Secure Telnet

Planung von DCM

SSL für sicheres iSeries Access Express

Sie können Ihre iSeries Access Express-Server für die Verwendung von SSL (Secure Sockets Layer) konfigurieren, um iSeries Access Express-Kommunikationssitzungen zu schützen.

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

Weitere Informationen über die Verwendung von iSeries Access Express mit SSL finden Sie unter den folgenden Themen im IBM Systems Software Information Center:

- Secure Sockets Layer Administration
- IBM Developer Kit for Java SSL
- IBM Java Toolbox SSL

Virtual Private Networks (VPN) für sichere private Kommunikation

Sie können ein VPN (Virtual Private Network) verwenden, um vertraulich und sicher innerhalb Ihres Unternehmens zu kommunizieren.

Angesichts der zunehmenden Verwendung von Virtual Private Networks (VPN) 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 arbeiten mit iSeries-Servern, und die Verwendung einer VPN-Verbindung kann den notwendigen Schutz bieten, der für die Übertragung zwischen den beiden Netzen erforderlich ist. Das Erstellen eines VPN ist kosteneffizienter als die Verwendung herkömmlicher Standleitungen.

VPN-Verbindungen bieten Ihnen die Möglichkeit, Verbindungen mit Zweigstellen, Außendienstmitarbeitern, Lieferanten, Geschäftspartnern usw. zu kontrollieren und zu sichern.

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 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.

Glücklicherweise können Sie 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 iSeries-System 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.

Weitere Informationen über die Verwendung von VPN-Verbindungen finden Sie unter dem Thema *Virtual private networking* im IBM Systems Software Information Center.

Zugehörige Konzepte

„Optionen für Übertragungssicherheit" auf Seite 26
Enthält Informationen über die Sicherheitsmaßnahmen, die Sie zum Schutz Ihrer Daten implementieren können, wenn diese über ein ungesichertes Netz wie das Internet übertragen werden. Zu diesen Maßnahmen gehören SSL (Secure Sockets Layer), iSeries Access Express und VPN-Verbindungen (VPN - Virtual Private Network).

Virtual private networks (VPN)

Terminologie zum Thema Sicherheit

Dieses Thema enthält Begriffe und Definitionen, die sich auf Sicherheitsinformationen beziehen.

A C D E F H I K N P R S T U V W

A

Authentifizierung
Prüfung, ob ein ferner Client oder Server wirklich der ist, der er vorgibt zu sein. Die Authentifizierung stellt sicher, dass Sie dem fernen Partner, zu dem eine Verbindung hergestellt wird, vertrauen können.

C

Cipher
Ein anderer Begriff für Verschlüsselungsalgorithmus.

Ciphertext
Verschlüsselte Texte und Daten.

Cracker
Ein Hacker mit unlauteren Absichten.

D

Datenvertraulichkeit
Der Inhalt einer Nachricht wird verborgen, normalerweise durch Verschlüsselung.

Datenintegrität
Überprüft, ob der Inhalt eines Datagramms während der Übertragung geändert wurde, entweder absichtlich oder auf Grund von Zufallsfehlern.

Denial-of-Service-Attacke
Wird auch als DoS-Attacke bezeichnet. Überlastet ein Netzwerk mit nutzlosem IP-Verkehr und bewirkt dadurch, dass ein Service wie ein Webserver nicht verfügbar ist oder nicht verwendet werden kann.

Digitales Zertifikat
Ein digitales Dokument, das 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. Zertifikate können für folgende Zwecke eingesetzt werden:

- Identifikation - Zeigt, wer der Benutzer ist.
- Authentifizierung - Stellt sicher, dass der Benutzer derjenige ist, der er vorgibt zu sein.
- Integrität - Stellt fest, ob der Inhalt eines Dokuments geändert wurde, indem die digitale Signatur des Absenders verifiziert wird.
- Unbestreitbarkeit - Garantiert, dass ein Benutzer nicht vorgeben kann, er habe eine bestimmte Aktion nicht ausgeführt. Beispiel: Der Benutzer kann nicht bestreiten, dass er einen elektronischen Einkauf mit einer Kreditkarte getätigt hat.

Digitale Signatur
Entspricht einer persönlichen Unterschrift auf einem Papierdokument. Eine digitale Signatur belegt den Ursprung des Dokuments. Der Zertifikatseigner ″signiert″ ein Dokument, indem er den privaten Schlüssel verwendet, der dem Zertifikat zugeordnet ist. Der Empfänger des Dokuments verwendet den entsprechenden öffentlichen Schlüssel, um die Signatur zu entschlüsseln, wodurch der Absender als Ursprung verifiziert wird.

Digital Certificate Manager (DCM)
Ermöglicht es einer iSeries, als lokale Zertifizierungsinstanz (CA) zu fungieren. Mit Hilfe von

DCM können Sie digitale Zertifikate erstellen, die von Servern oder Benutzern verwendet werden. Sie können digitale Zertifikate importieren, die von anderen CAs ausgegeben werden. Sie können ein digitales Zertifikat auch einem i5/OS-Benutzerprofil zuordnen. DCM wird weiterhin dazu verwendet, Anwendungen für die sichere Kommunikation mit SSL (Secure Sockets Layer) zu konfigurieren.

Domain Name System (DNS)
Die Datengruppe, mit der ein einzelner Eigner eines digitalen Zertifikats identifiziert wird. Bei einem digitalen Zertifikat der Klasse 1 sind dies Informationen wie Ihr Name, Ihre E-Mail-Adresse und der Aussteller des digitales Zertifikats (VeriSign, Inc.).

Wenn Sie eine Verbindung zum Internet herstellen, verwendet Ihr Internet-Client einen DNS-Server, um die IP-Adresse des Hostsystems festzustellen, mit dem Sie kommunizieren möchten.

E

Einzelanmeldung (Single Sign-on - SSO)
Eine Form der Authentifizierung, bei der ein Benutzer, der einmal authentifiziert wurde, auf die Ressourcen mehrerer Systeme oder Anwendungen zugreifen kann. Siehe ″Enterprise Identity Mapping″.

Enterprise Identity Mapping (EIM)
EIM ist ein Mechanismus für die Zuordnung von Personen oder Entitäten zu den entsprechenden Benutzeridentitäten in verschiedenen Benutzerregistern im gesamten Unternehmen. EIM bietet APIs für die Erstellung und Verwaltung dieser Beziehungen für Identitätsabgleich und APIs, die Anwendungen für die Abfrage dieser Informationen verwenden.

Erkennung von unbefugtem Zugriff
Ein allgemeiner Begriff, der die Feststellung zahlreicher nicht erwünschter Aktivitäten umfasst. Das Ziel eines unbefugten Zugriffs ist es möglicherweise, sich Informationen anzueignen, für die eine Person nicht berechtigt ist (Informationsdiebstahl). Möglicherweise soll ein Unternehmen geschädigt werden, indem ein Netz, ein System oder eine Anwendung außer Gefecht gesetzt wird (Denial-of-Service-Attacke), oder der Angreifer möchte sich Zugriff auf ein System verschaffen, um weitere unberechtigte Zugriffe auf anderen Systemen durchzuführen. Bei den meisten Manipulationen werden zunächst Informationen gesammelt, dann ein Zugriffsversuch durchgeführt und anschließend zerstörerische Angriffe ausgeführt. Einige Angriffe werden vom Zielsystem erkannt und bekämpft. Andere Angriffe kann das Zielsystem nicht wirksam bekämpfen. Bei den meisten Angriffen werden ″spoofed″ Pakete verwendet, deren tatsächliche Herkunft kaum feststellbar ist. Viele Angriffe werden heute über Maschinen oder Netze ausgeführt, die ohne Berechtigung und ohne Kenntnis der jeweiligen Eigner verwendet werden, um die Identität des Angreifers zu verschleiern. Aus diesen Gründen konzentrieren sich Maßnahmen zur Erkennung von unbefugtem Zugriff auf Aktivitäten zur Informationssammlung, auf Zugriffsversuche und auf verdächtiges Verhalten.

Extranet
Ein privates Geschäftsnetz mehrerer kooperierender Unternehmen außerhalb der unternehmensweiten Firewall. Ein Extranetdienst nutzt die vorhandene Infrastruktur des Internet, einschließlich Standardservern, E-Mail-Clients und Webbrowsern. Deshalb ist die Nutzung eines Extranet wirtschaftlicher als das Erstellen und Warten eines privaten Netzes. Geschäftspartner, Lieferanten und Kunden mit gemeinsamen Interessen können das erweiterte Internet sowohl für den Aufbau enger Geschäftsbeziehungen als auch für die intensive Kommunikation nutzen.

F

Firewall
Eine logische Barriere zwischen dem internen und einem externen Netz wie dem Internet. Eine Firewall besteht aus einem oder mehreren Hardware- und Softwaresystemen oder Partitionen. Sie steuert den Zugriff und den Informationsfluss zwischen sicheren oder vertrauenswürdigen Systemen und ungesicherten oder nicht vertrauenswürdigen Systemen.

H

Hacker
Eine unbefugte Person, die versucht, in ein System einzudringen.

Hypertextverbindungen
Eine Möglichkeit, online Informationen über Verbindungen (sog. Hypertextverbindungen) zwischen einer Information (dem Hypertextknoten) und einer anderen darzustellen.

Hypertext Markup Language (HTML)
Die Sprache, mit der Hypertextdokumente definiert werden. Mit HTML kann das Aussehen eines Dokuments (z. B. Hervorhebung und Schriftart) und die Art und Weise angegeben werden, wie es mit anderen Dokumenten oder Objekten verbunden werden soll.

Hypertext Transfer Protocol (HTTP)
Die Standardmethode für den Zugriff auf Hypertextdokumente.

I

Internet
Das weltweite ″Netz der Netze″, die untereinander verbunden sind, und eine Gruppe kooperierender Anwendungen, die es Computern, die mit diesem ″Netz der Netze″ verbunden sind, ermöglicht, miteinander zu kommunizieren. Das Internet bietet anzeigbare Informationen, Dateiübertragung, fernes Anmelden, E-Mail, Nachrichten und andere Dienste an. Das Internet wird häufig auch als ″das Netz″ bezeichnet.

Internet-Client
Ein Programm (oder Benutzer), das (der) das Internet nutzt, um Anforderungen an ein Internet-Serverprogramm zu stellen und Ergebnisse von diesem zu erhalten. Es stehen unterschiedliche Clientprogramme zur Verfügung, um unterschiedliche Arten von Internetdiensten anzufordern. Ein Webbrowser ist ein solches Clientprogramm, File Transfer Protocol (FTP) ein anderes.

Internet-Host
Ein Computer, der mit dem Internet oder einem Intranet verbunden ist. Auf einem Internet-Host können mehrere Internet-Serverprogramme ausgeführt werden. Auf dem Internet-Host könnte beispielsweise ein FTP-Server vorhanden sein, um Anforderungen von FTP-Clientanwendungen zu beantworten. Auf dem gleichen Host könnte ein HTTP-Server vorhanden sein, um Anforderungen von Client-Webbrowsern zu beantworten. Serverprogramme werden normalerweise im Hintergrund (im Stapelbetrieb) auf dem Hostsystem ausgeführt.

IKE-Protokoll (Internet Key Exchange)
Unterstützt sowohl die automatische Vereinbarung von Sicherheitszuordnungen als auch die automatische Generierung und Aktualisierung von Chiffrierschlüsseln als Teil des Virtual Private Networking (VPN).

Internetname
Ein Aliasname für eine IP-Adresse. Eine IP-Adresse hat ein langes numerisches Format, das man sich nur schwer merken kann (z. B. 10.5.100.75). Diese IP-Adresse kann einem Internetnamen zugeordnet werden, z. B. system1.vnet.ibm.com. Ein Internetname wird auch als vollständig qualifizierter Domänenname bezeichnet. Bei einer Werbung wie ″Besuchen Sie unsere Homepage″ beinhaltet die Homepage-Adresse den Internetnamen und nicht die IP-Adresse, da der Internetname leichter zu merken ist. Ein vollständig qualifizierter Domänenname hat zahlreiche Bestandteile. Beispielsweise verfügt system1.vnet.ibm.com über die folgenden Teile:

com: Alle kommerziellen Netze. Dieser Bestandteil des Domänennamens wird von der jeweiligen Internetverwaltungsorganisation (eine externe Organisation) zugeordnet. Für unterschiedliche Arten von Netzen werden unterschiedliche Zeichen vergeben (z. B. *com* für kommerzielle und *edu* für Bildungseinrichtungen).

ibm: Die Kennung der Organisation. Dieser Bestandteil des Domänennamens wird ebenfalls von der Internetverwaltungsorganisation zugeordnet und ist eindeutig. Nur eine einzige Organisation weltweit kann die Kennung ibm.com haben.

vnet: Eine Gruppierung von Systemen innerhalb von ibm.com. Diese Kennung wird intern zugeordnet. Der Administrator von ibm.com kann eine oder mehrere Gruppierungen erstellen.

system1:
Der Name eines Internet-Hosts innerhalb der Gruppe vnet.ibm.com.

Internet-Server
Ein Programm (oder eine Programmgruppe), das (die) Anforderungen von entsprechenden Clientprogrammen über das Internet annimmt und diesen Clients über das Internet antwortet. Einen Internet-Server kann man sich als Site vorstellen, auf die ein Internet-Client zugreifen oder die ein Internet-Client besuchen kann. Unterschiedliche Serverprogramme unterstützen unterschiedliche Dienste, wie beispielsweise die folgenden:

- Durchsuchen (einer "Homepage" und Links auf andere Dokumente und Objekte).
- Dateiübertragung. Der Client kann beispielsweise anfordern, Dateien vom Server an den Client zu übertragen. Bei den Dateien könnte es sich um Software-Updates, Produktlisten oder Dokumente handeln.
- E-Commerce, wie beispielsweise die Möglichkeit, Informationen anzufordern oder Produkte zu bestellen.

Internet-Service-Provider (ISP)
Ein Unternehmen, das Ihnen den Internetzugang anbietet (vergleichbar mit einer örtlichen Telefongesellschaft, die Ihnen Zugang zu weltweiten Telefonnetzen bietet).

Intranet
Das interne Netz eines Unternehmens, das Internet-Tools, wie einen Webbrowser oder FTP, benutzt.

IP-Adresse
Eine eindeutige Kennung in einem TCP/IP-Netz (das Internet ist ein sehr großes TCP/IP-Netz). Einem Internet-Server ist normalerweise eine eindeutige IP-Adresse zugeordnet. Ein Internet-Client kann eine temporäre, jedoch eindeutige IP-Adresse verwenden, die vom ISP zugeteilt wird.

IP-Datagramm
Eine Informationseinheit, die über ein TCP/IP-Netz gesendet wird. Ein IP-Datagramm (auch: Paket) enthält sowohl Daten als auch Headerdaten, wie etwa die IP-Adressen von Ursprungs- und Zielmaschine.

IP-Filter
Steuern, welcher IP-Verkehr in das Netz hinein und aus dem Netz heraus gelangt, indem Pakete gemäß definierter Regeln gefiltert werden. Dies schützt das sichere Netz vor Außenstehenden, die entweder harmlose (z. B. Suchen nach Sicherheitsservern) oder aber auch ausgefeilteste Methoden (z. B. Spoofing von IP-Adressen) verwenden. Stellen Sie sich das Filtern als die Grundlage vor, auf der die übrigen Tools aufbauen. Das Filtern stellt die Infrastruktur für diese Tools zur Verfügung und kann die Mehrzahl aller Zugriffsversuche von Crackern abwehren.

IPSec-Protokoll (IP Security)
Eine Gruppe von Protokollen zur Unterstützung des sicheren Austauschs von Paketen auf der Netzebene. IPSec ist eine Gruppe von Standards, die von i5/OS und vielen anderen Systemen bei der Realisierung von VPNs verwendet wird.

IP-Spoofing
Der Versuch, durch Vortäuschen eines vertrauenswürdigen Systems (einer IP-Adresse) auf Ihr System zuzugreifen. Der potenzielle Eindringling versieht ein System mit einer IP-Adresse, der Sie vertrauen. Router-Hersteller haben daran gearbeitet, Schutzmaßnahmen in ihre Systeme zu integrieren, um Spoofing-Versuche zu erkennen und zurückzuweisen.

K

Kryptografie
Die Wissenschaft, die sich mit der Gewährleistung der Datensicherheit befasst. Sie ermöglicht das

Speichern von Informationen und das Übertragen von Daten an andere Personen, ohne dass Unbefugte die gespeicherten Informationen lesen oder die Kommunikation mit diesen Personen verstehen können. Bei der Verschlüsselung wird lesbarer Text in unlesbare Daten (sog. Ciphertext) umgesetzt. Bei der Entschlüsselung wird aus den unlesbaren Daten wieder der ursprüngliche, lesbare Text hergestellt. Für beide Prozesse wird eine mathematische Formel oder ein Algorithmus und eine geheime Folge von Daten (der Schlüssel) benötigt.

Es gibt zwei Arten von Kryptografie:

- **Symmetrische Kryptografie**: Die Kommunikationsteilnehmer benutzen gemeinsam einen geheimen Schlüssel, der sowohl für die Verschlüsselung als auch die Entschlüsselung verwendet wird. Wird auch als Kryptografie mit einem geheimen Schlüssel für gemeinsame Benutzung bezeichnet.
- **Asymmetrische Kryptografie**: Jeder Kommunikationsteilnehmer at zwei Schlüssel: einen öffentlichen und einen privaten. Zwischen beiden Schlüsseln besteht zwar eine mathematische Relation, aber es ist praktisch unmöglich, den privaten Schlüssel von dem öffentlichen abzuleiten. Eine Nachricht, die mit dem öffentlichen Schlüssel eines Teilnehmers verschlüsselt ist, kann nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden. Alternativ kann ein Server oder Benutzer einen privaten Schlüssel verwenden, um ein Dokument zu ″signieren″, und einen öffentlichen Schlüssel, um eine digitale Signatur zu entschlüsseln. Wenn der Hashwert, der sich aus der Entschlüsselung der Signatur mit dem öffentlichen Schlüssel ergibt, einem Echtzeithashwert des Dokuments selbst entspricht, wird die Signatur als gültig und die Quelle des Dokuments als bestätigt betrachtet. Wird auch als Kryptografie mit öffentlichem Schlüssel bezeichnet.

N

Netzwerkadresskonvertierung (NAT)
Eine Alternative zu den Proxy- und SOCKS-Servern, die mehr Transparenz bietet. Außerdem vereinfacht sie die Netzkonfiguration dadurch, dass auch Netze mit nicht kompatiblen Adressierungsstrukturen miteinander verbunden werden können. NAT stellt zwei Hauptfunktion zur Verfügung. Der Schutz besteht darin, dass es Ihnen erlaubt ist, die ″wahre″ Adresse Ihres Servers hinter einer anderen Adresse zu verbergen, die Sie der Öffentlichkeit zur Verfügung stellen. NAT kann beispielsweise einen öffentlichen Webserver schützen, den Sie in Ihrem internen Netz betreiben möchten. NAT bietet internen Benutzern außerdem eine Möglichkeit, auf das Internet zuzugreifen, ohne ihre persönlichen internen IP-Adressen preiszugeben. Wenn Sie internen Benutzern gestatten, auf Internetdienste zuzugreifen, bietet NAT insofern Schutz, als Sie die privaten Adressen der Benutzer verbergen können.

P

Paket Eine Informationseinheit, die über ein TCP/IP-Netz gesendet wird. Ein Paket (auch: Datagramm) enthält sowohl Daten als auch Headerdaten, wie etwa die IP-Adressen von Ursprungs- und Zielmaschine, und umfasst Informationen über das Leitungsprotokoll, beispielsweise Ethernet Token-Ring oder Frame-Relay.

Proxy-Server
Eine TCP/IP-Anwendung, die Anforderungen und Antworten zwischen Clients auf Ihrem sicheren internen Netz und Servern auf dem ungesicherten Netz erneut sendet. Der Proxy-Server unterbricht die TCP/IP-Verbindung, um Ihre internen Netzinformationen (wie interne IP-Adressen) zu verdecken. Hosts außerhalb Ihres Netzes nehmen den Proxy-Server als Quelle der Übertragung wahr.

PKI-Infrastruktur (Public Key Infrastructure)
Ein System aus digitalen Zertifikaten, CAs und anderen Registrierungsinstanzen, die die Gültigkeit aller an einer Internettransaktion beteiligten Teilnehmer verifizieren.

R

Registrierter Name
Der Name der Person oder des Servers, für die/den eine Zertifizierungsinstanz (CA) ein digitales

Zertifikat ausstellt. Das Zertifikat enthält diesen Namen, um das Zertifikatseigentumsrecht nachzuweisen. Je nach Richtlinie der CA, die ein Zertifikat ausgibt, kann der registrierte Name noch weitere Berechtigungsinformationen enthalten.

S

Secure Sockets Layer (SSL)
Der von Netscape erstellte Standard SSL ist de facto ein Branchenstandard für die Verschlüsselung von Sitzungen zwischen Clients und Servern. Für SSL wird die Verschlüsselung mit symmetrischen Schlüsseln verwendet, um die Sitzung zwischen Server und Client (Benutzer) zu verschlüsseln. Client und Server handeln den Sitzungsschlüssel während des Austauschs digitaler Zertifikate aus. Für jede Client- und Server-SSL-Sitzung wird ein anderer Schlüssel erstellt. Folglich können unbefugte Benutzer einen Sitzungsschlüssel selbst dann nicht zum Abhören aktueller, künftiger oder vergangener SSL-Sitzungen verwenden, wenn sie ihn abfangen und entschlüsseln können (was unwahrscheinlich ist).

Sniffing
Das Überwachen oder Abhören elektronischer Übertragungen. Informationen, die über das Internet gesendet werden, können zahlreiche Router durchlaufen, bevor sie ihr Ziel erreichen. Hersteller von Routern, ISPs und Entwickler von Betriebssystemen haben intensiv daran gearbeitet, das Ausspionieren auf der Internet-Zentralverbindung zu verhindern. Derartige Attacken werden immer seltener. Die meisten Fälle treten auf privaten LANs auf, die mit dem Internet verbunden sind, und nicht auf der Internet-Zentralverbindung selbst. Dennoch müssen Sie sich darüber im Klaren sein, dass ein Ausspionieren möglich ist, da die meisten TCP/IP-Übertragungen nicht verschlüsselt sind.

SOCKS
Eine Client/Server-Architektur, die den TCP/IP-Datenverkehr durch ein sicheres Gateway transportiert. Ein SOCKS-Server bietet viele der Dienste an, die auch ein Proxy-Server anbietet.

Spoofing
Angreifer tarnen sich als vertrauenswürdiges System, um Sie dazu zu bringen, ihnen vertrauliche Informationen zu senden.

T

TCP/IP
Das wichtigste Übertragungsprotokoll im Internet. TCP/IP steht für Transmission Control Protocol/Internet Protocol. Sie können TCP/IP auch in Ihrem internen Netz verwenden.

Trojanisches Pferd
Ein Computerprogramm, ein Befehl oder ein Script, das/der eine vermeintlich hilfreiche, harmlose Funktion ausführt. Tatsächlich trägt es/er jedoch versteckte Funktionen in sich, die den Benutzern zugeordnete anerkannte Berechtigungen nutzen, sobald diese das Programm starten. Das Programm kann beispielsweise interne Berechtigungsinformationen von Ihrem Computer kopieren und zurück an den Absender des Trojanischen Pferdes senden.

U

Unbestreitbarkeit
Bietet den Beweis dafür, dass eine Transaktion stattgefunden hat oder dass Sie eine Nachricht gesendet oder empfangen haben. Die Verwendung digitaler Zertifikate und der Kryptografie mit öffentlichem Schlüssel, um Transaktionen, Nachrichten und Dokumente zu "signieren", unterstützt die Unbestreitbarkeit.

Ursprungsauthentifizierung für Daten
Prüft, ob ein IP-Datagramm tatsächlich vom angeblichen Absender gesendet wurde.

V

Verschlüsselung
Der Prozess der Umwandlung von Daten in ein Format, das nur von jemandem mit der richtigen

Methode und dem richtigen Schlüssel für die Entschlüsselung gelesen werden kann. Unbefugte können die Informationen zwar immer noch abfangen, aber ohne die richtige Methode und den richtigen Schlüssel für die Entschlüsselung sind die Informationen unverständlich.

Virtual Private Network (VPN)
Eine Erweiterung des privaten Intranets eines Unternehmens. Die Erweiterung kann über ein öffentliches Netz wie das Internet erfolgen, wobei eine sichere private Verbindung hergestellt wird, im Wesentlichen durch einen privaten ″Tunnel″. VPNs befördern Informationen sicher durch das Internet und verbinden so andere Benutzer mit Ihrem System. Dazu gehören:

- Ferne Benutzer
- Zweigstellen
- Geschäftspartner und Lieferanten

W

Webbrowser
Die HTTP-Clientanwendung. Ein Webbrowser interpretiert HTML, um dem Benutzer Hypertext-dokumente anzuzeigen. Der Benutzer kann auf ein Objekt zugreifen, das über einen Hyperlink verbunden ist, indem er einen Bereich des aktuellen Dokuments anklickt (auswählt). Dieser Bereich wird häufig auch als **Hotspot** bezeichnet. Internet Connection Web Explorer und Netscape Navigator sind Beispiele für Webbrowser.

Wiederholschutz
Stellt sicher, dass ein Angreifer ein Datagramm nicht abfangen und zu einem späteren Zeitpunkt erneut senden kann.

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. Anstelle der IBM Produkte, Programme oder Services können auch andere ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen.Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices 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:

IBM Europe
Director of Licensing
92066 Paris La Defense Cedex
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 jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen 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 unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

| Director of Licensing
| 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 im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der 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 gesteuerten 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 abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Informationen über Nicht-IBM Produkte wurden von den Herstellern dieser Produkte zur Verfügung gestellt, bzw. aus von ihnen veröffentlichten Ankündigungen oder anderen öffentlich zugänglichen Quellen entnommen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen hinsichtlich des Leistungsspektrums von Produkten anderer Hersteller als IBM sind an den jeweiligen Hersteller des Produkts zu richten.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht der IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele der IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

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 Lizenzprogrammes 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, verwenden, 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.

Marken

Folgende Namen sind in gewissen Ländern Marken der International Business Machines Corporation:

| AIX
| AIX 5L
| e(logo) server
| eServer
| i5/OS
| IBM
| iSeries
| pSeries
| xSeries
| zSeries

| Intel, Intel Inside (Logos), MMX und PentiumIntel sind in gewissen Ländern Marken der Intel Corpora-
| tion.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

Java und alle Java-basierten Marken sind in gewissen Ländern Marken von Sun Microsystems, Inc.

| Linux ist eine eingetragene Marke von Linus Torvalds.

UNIX ist in gewissen Ländern eine eingetragene Marke der Open Group.

Andere Namen von Unternehmen, Produkten oder Services können Marken oder Servicemarken anderer Unternehmen 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 der IBM nicht weitergeben, anzeigen oder abgeleitete Arbeiten 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 andere 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 Vorschriften, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden ohne Wartung (auf ″as-is″-Basis) und ohne jede Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit der Rechte Dritter zur Verfügung gestellt.