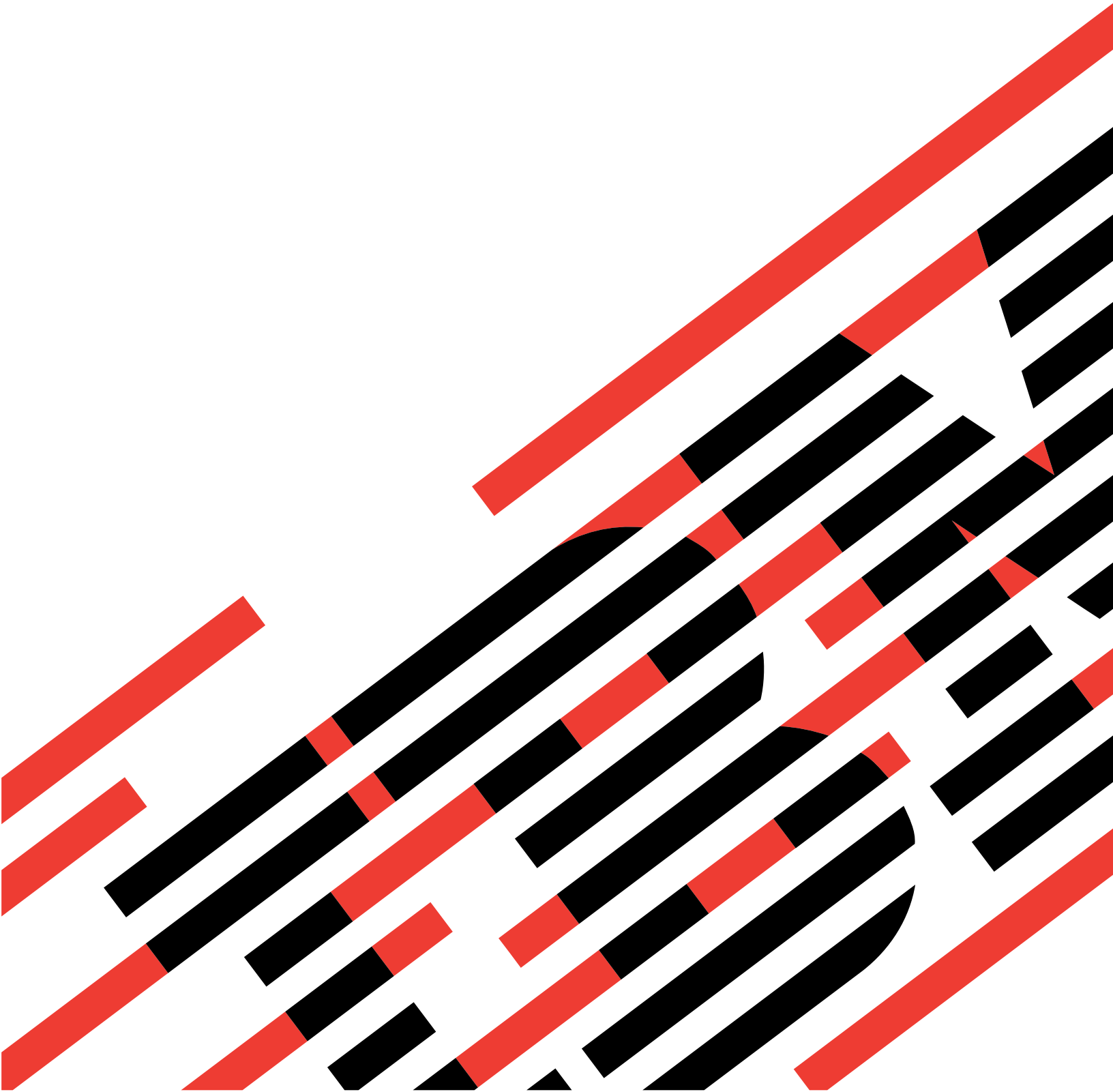
IBM

eserver

iSeries

IBM SecureWay: iSeries 400 und das Internet



IBM

@server

iSeries

IBM SecureWay: iSeries 400 und das Internet

Inhaltsverzeichnis

Teil 1. IBM SecureWay: iSeries und das Internet

Die Internet-Anbindung des eigenen LAN ist ein bedeutender Schritt in der Weiterentwicklung Ihres Netzes, der von Ihnen eine erneute Berwertung Ihrer Sicherheitsanforderungen verlangt. Glücklicherweise verfügt die iSeries 400 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 Intenetzielen 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 den Entwurf eines für Ihr Unternehmen adäquaten Sicherheitsplans nutzen.

Weitere Informationen über Internet-Sicherheitsrisiken und iSeries-Sicherheitslösungen, mit denen Sie Ihre Systeme und Ressourcen schützen können, finden Sie in den folgenden Quellen:

- **Neuheiten in V5R1**
  Diese Informationen enthalten eine Zusammenstellung der Änderungen und Erweiterungen der iSeries-Internet-Sicherheitsangebote für V5R1.
- **Thema drucken**
  Diese Informationen enthalten Anweisungen für das Anzeigen und Drucken einer Adobe Acrobat-Version dieses Themas.
- **iSeries und Internet-Sicherheit**
  Anhand dieser Informationen können Sie sich einen allgemeinen Überblick über die Stärken der iSeries-Sicherheit für e-business und der verfügbaren iSeries-Sicherheitsangebote verschaffen.
- **Internet-Sicherheit planen**
  In diesen Informationen erfahren Sie, wie Sie Sicherheitsrichtlinien erstellen können, die Ihren Sicherheitsbedürfnissen hinsichtlich Internet und e-business gerecht werden.
- **iSeries-Systemsicherheitsstufen als Voraussetzung für Internet-Zugang**
  In diesen Informationen erfahren Sie, welches Maß an Systemschutz vorhanden sein sollte, bevor Sie eine Verbindung zum Internet herstellen.
- **Optionen für Netzsicherheit**
  In diesen Informationen werden die Sicherheitsmaßnahmen beschrieben, die Sie auf Netzebene zum Schutz der internen Ressourcen treffen sollten.
- **Optionen für Anwendungssicherheit**
  In diesen Informationen werden die Internet-Sicherheitsrisiken für zahlreiche populären Internet-Anwendungen und -Dienste beschrieben sowie Maßnahmen vorgeschlagen, wie diesen Risiken begegnet werden kann.

- **Optionen für Übertragungssicherheit**
  In diesen Informationen werden die Sicherheitsmaßnahmen beschrieben, die Sie zum Schutz Ihrer Daten implementieren können, wenn diese über ein ungesichertes Netz wie das Internet übertragen werden. Sie erfahren Einzelheiten über die Sicherheitsmaßnahmen für Verbindungen hinsichtlich des Einsatzes von Secure Sockets Layer (SSL), Client Access Express und Virtual Private Network (VPN).
- **iSeries-Optionen für Internet-Sicherheit**
  Nutzen Sie diese kurze Erörterung der iSeries-Sicherheitsoptionen als Entscheidungshilfe bei der Auswahl der Angebote zum Schutz Ihrer Systeme und Ressourcen auf der Grundlage Ihrer Internet-Nutzungspläne und e-business Pläne.

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

Kapitel 1. Neuheiten in V5R1

In V5R1 wurden zahlreiche Verbesserungen und Erweiterungen der Angebotspalette im Bereich Sicherheit für Ihre iSeries 400 implementiert. In der folgenden Liste sind einige der wichtigeren funktionalen Sicherheitsverbesserungen aufgeführt:

- **Funktionale Erweiterungen für Digital Certificate Manager (DCM)**
  Mit DCM können Sie jetzt Zertifikate erstellen und verwalten, die zum digitalen Signieren von Objekten benutzt werden. Durch die Signatur wird die Integrität der jeweiligen Objekte gewährleistet und deren Ursprung belegt. Darüber hinaus können Sie die entsprechenden Signaturüberprüfungszertifikate erstellen und verwalten, die zum Authentifizieren der Signatur auf den signierten Objekten benutzt werden. Hierdurch wird sichergestellt, dass die in den Objekten enthaltenen Daten nicht geändert wurden, und der Ursprung der Objekte wird belegt. DCM oder die entsprechenden APIs können auch zum Signieren eines Objekts und zum Prüfen der Objektsignatur eingesetzt werden.
- **Digital signiertes Betriebssystem**
  Beginnend mit V5R1 werden OS/400 und IBM Lizenzprogramme (LPPs) von IBM digital signiert, was Benutzern die Möglichkeit gibt, zu prüfen, ob IBM Programme geändert wurden. Die Prüfung digitaler Signaturen kann beim Zurückspeichern oder mit dem Befehl CHKOBJITG erfolgen. Kunden und Geschäftspartnern stehen auch APIs zur Verfügung, über die sie ihre Anwendungen digital signieren und prüfen können.
- **Neue Regeln für Benutzerprofilkennwörter (QPWDLVL 2 und 3)**
  Die maximale Länge des Benutzerprofilkennworts wurde auf 128 Zeichen erhöht. Bei Kennwörtern muss die Groß-/Kleinschreibung beachtet werden, eingebettete Leerzeichen sind zulässig; z. B. "Dies ist mein Neues Kennwort." Abschließende Leerzeichen werden entfernt, Kennwörter, die ausschließlich aus Leerzeichen bestehen, sind nicht zulässig.
- **Funktionale Erweiterungen für Benutzerprofilkennwörter**
  Mit dem neuen Systemwert QPWDLVL kann eine von 4 Optionen zur Steuerung der Kennwortebene des Systems festgelegt werden:
  - PWDLVL 0 — Es sind Kennwörter mit einer Länge von 10 Byte zulässig; Netserver-Kennwörter können beibehalten werden. Dies ist die Standardeinstellung.
  - PWDLVL 1 — Es sind Kennwörter mit einer Länge von 10 Byte zulässig; Netserver-Kennwörter werden entfernt.
  - PWDLVL 2 — Es sind Kennwörter mit einer Länge von 128 Zeichen zulässig; Kennwörter, die sowohl den alten als auch den neuen Kennwortformaten entsprechen, werden beibehalten.
  - PWDLVL 3 — Es sind Kennwörter mit einer Länge von 128 Zeichen zulässig; alte Kennwortformate werden entfernt.
- **IBM 4758–023 PCI Cryptographic Coprocessor-Unterstützung für verbesserte Sicherheit bei der Schlüsselspeicherung**
  Wenn auf Ihrem System ein IBM 4758–023 PCI Cryptographic Coprocessor installiert ist, können Sie diesen zur Erhöhung der Sicherheit beim Speichern Ihrer digitalen Zertifikatsschlüssel verwenden. Wenn Sie DCM zum Erstellen oder Verlängern von Zertifikaten verwenden, kann der zugehörige Schlüssel direkt im Koprozessor gespeichert oder der Hauptschlüssel des Koprozessors zum Verschlüsseln des privaten Schlüssels und zur Speicherung in einer speziellen Schlüsselspeicherdatei benutzt werden. Wenn Sie den Koprozessor zur Schlüsselspeicherung verwenden, können Sie auch die SSL-Leistung (SSL = Sec-

ure Sockets Layer) Ihrer für SSL definierten Anwendungen steigern, da der Koprozessor die Entschlüsselung des privaten Schlüssels für den SSL-Handshake übernimmt. Es ist auch ein Lastausgleich der SSL-Handshakeverarbeitung über mehrere 4758-Karten möglich.

- **Unterstützung für VPN-Zertifikate (VPN = Virtual Private Networking)**
  In Versionen vor V5R1 konnten sich die VPN IKE-Server (IKE = Internet Key Exchange) lediglich mit einem vorab bekannten gemeinsamen Schlüssel gegenseitig authentifizieren. Dieses Verfahren bietet ein geringeres Maß an Sicherheit, da der Administrator des anderen Endpunkts innerhalb des VPNs manuell über den verwendeten Schlüssel informiert werden muss. Hierbei ergibt sich das Risiko, dass der Schlüssel während der Übergabe möglicherweise durch Unbefugte in Erfahrung gebracht werden kann. Unter V5R1 kann dieses Risiko vermieden werden, da an Stelle vorab bekannter gemeinsamer Schlüssel nun digitale Zertifikate zur Authentifizierung der Endpunkte benutzt werden. Digital Certificate Manager (DCM) kann zum Verwalten der Zertifikate benutzt werden, die vom IKE-Server zum Herstellen einer dynamischen VPN-Verbindung verwendet werden.
- **Verbesserungen bei Anwendungen, die für SSL definiert sind**
  In V5R1 wurden zahlreiche funktionale SSL-Erweiterungen implementiert. Sie können Ihren iSeries FTP-Server (FTP = File Transfer Protocol) so konfigurieren, dass SSL für gesicherte Kommunikationssitzungen verwendet wird. Sie können den FTP-Server auch für die Verwendung digitaler Zertifikate zur Clientauthentifizierung konfigurieren. Außerdem bietet OS/400 in V5R1 Unterstützung für den AES-Cipher mit einer Größe von 128 Bit. AES ist ein neuer, schnellerer Verschlüsselungsalgorithmus, der den DES-Algorithmus ersetzt.
- **Funktionale Erweiterungen für Simple Mail Transfer Protocol (SMTP)**
  SMTP bietet jetzt Unterstützung für schwarze Listen, die anhand des Betreffs, des Absenders und der IP-Adresse erstellt werden können.
- **Internet Setup-Assistent**
  Der bekannte Internet Setup-Assistent, der im letzten Release als herunterladbare Datei verfügbar war, ist jetzt im Operations Navigator integriert. Mit Hilfe dieses Assistenten können Sie eine Internet-Verbindung für Ihr iSeries-System konfigurieren und mit automatisch generierten Filterregeln sichern.
- **Erweiterungen bei der Sicherung von Programmerstellungsdaten**
  Programme, die für iSeries-Systeme mit V5R1 oder später erstellt werden, enthalten Informationen, mit denen das entsprechende Programm, falls erforderlich, beim Zurückspeichern erneut erstellt werden kann. Diese Informationen verbleiben auch dann im Programm, wenn die überwachbaren Daten des Programms entfernt werden. Wenn beim Zurückspeichern des Programms ein Gültigkeitsfehler festgestellt wird, wird das Programm erneut erstellt, um diesen Fehler zu beheben. Das erneute Erstellen eines Programms zum Zeitpunkt des Zurückspeicherns ist keine Neuheit in V5R1. Bereits in früheren Releases führten alle Programmgültigkeitsfehler, die beim Zurückspeichern festgestellt wurden, dazu, dass das Programm, wenn möglich, erneut erstellt wurde (wenn das Programm überwachbare Daten beinhaltete). Der Unterschied zu iSeries-Programmen mit V5R1 oder später besteht darin, dass die zum erneuten Erstellen erforderlichen Informationen auch dann beibehalten werden, wenn die überwachbaren Daten aus dem Programm entfernt wurden. Daher wird jedes Programm mit V5R1 oder später, bei dem ein Gültigkeitsfehler festgestellt wird, beim Zurückspeichern erneut erstellt, und die Änderung, die den Fehler verursachte, wird entfernt.

Kapitel 2. Thema drucken

Sie können eine PDF-Version dieses Dokuments herunterladen, um sie anzuzeigen oder zu drucken. Zum Anzeigen von PDF-Dateien muss auf Ihrem System Adobe Acrobat Reader installiert sein. Diese Software finden Sie auf der

Adobe-Homepage. 

Um die PDF-Version anzuzeigen oder herunterzuladen, wählen Sie IBM Secure-Way: iSeries und das Internet (416 KB bzw. 60 Seiten) aus.

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

1. Öffnen Sie die PDF-Datei im Browser, indem Sie auf den o.a. Link klicken.
2. Klicken Sie im Browsermenü auf **Datei**.
3. Klicken Sie auf **Speichern unter...**
4. Navigieren Sie zu dem Verzeichnis, in dem die PDF-Datei gespeichert werden soll.
5. Klicken Sie auf **Speichern**.

Kapitel 3. iSeries 400 und Internet-Sicherheit

Als Besitzer einer iSeries 400, der die Möglichkeiten einer Internet-Anbindung untersucht, wird die Frage, wie Sie den Einstieg ins Internet für Geschäftszwecke gestalten sollen, eine der ersten sein, die sich stellen. Die zweite Frage lautet, was Sie über Sicherheit und das Internet wissen müssen. Die Beantwortung dieser zweiten Frage ist das Hauptanliegen dieser Veröffentlichung.

Die Antwort auf die Frage nach der Sicherheit und dem Internet lautet, dass es darauf ankommt, 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 zu erstellen.

Vor dem Einstieg ins Internet sollten Sie genau überlegen, was Sie tun möchten und wie Sie es tun möchten. Die Entscheidungsfindung sowohl hinsichtlich Internet-Nutzung als auch Internet-Sicherheit kann eine komplizierte Angelegenheit sein. Bei der Entwicklung Ihres eigenen Internet-Nutzungsplans kann sich die Seite Szenario: e-business Pläne des Unternehmens JKL Toy 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 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.

Kenndaten des iSeries 400-Systemschutzes

Neben zahlreichen speziellen Sicherheitsangeboten zum Schutz Ihres Systems im Internet verfügt die iSeries 400 bereits über Kenndaten, 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 einer iSeries 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. Mit Hilfe des Technical Studio Security Advisor 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 Internet-Anbindung verbessern können. Je nachdem, wie Sie das Internet nutzen, können Sie eins oder mehrere dieser Angebote nutzen:

- Virtual Private Networks (VPNs) stellen eine Ausweiterung des privaten Intranets eine 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 OS/400-Feature, das über die Operations Navigator-Schnittstelle zugänglich ist.
- Paketregeln sind ein integriertes OS/400-Feature, das über die Operations Navigator-Schnittstelle zugänglich ist. Mit Hilfe dieses Features können Sie Regeln für IP-Paketfilter und die Netzadresskonvertierung (Network Address Translation - NAT) konfigurieren, um den TCP/IP-Datenverkehr Ihres iSeries-Systems zu steuern.
- Das Sichern von Anwendungen mit Secure Sockets Layer (SSL) 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, wie beispielsweise IBM HTTP-Server für iSeries, Client Access Express, File Transfer Protocol (FTP), Telnet und viele andere.

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: Einzelheiten über den Einstieg ins Internet zu Geschäftszwecken finden Sie unter folgendem Online-Thema und IBM Redbook im Information Center:

- *Verbindung zum Internet*
- *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* (SG24-4929).

Kapitel 4. Internet-Sicherheit planen

Bei der Entwicklung Ihrer Internet-Nutzungspläne müssen Sie Ihren Sicherheitsbedürfnissen besondere Beachtung schenken. Sie müssen detaillierte Informationen über Ihre Internet-Nutzungspläne zusammenstellen und Ihre interne Netzkonfiguration dokumentieren. Auf der Grundlage dieser Informationen können Sie Ihre Sicherheitsbedürfnisse genau ermitteln.

Sie sollten beispielsweise folgende Dinge dokumentieren und beschreiben:
- Ihre aktuelle Netzkonfiguration.
- Konfigurationsdaten für DNS und E-Mail-Server.
- Ihre Verbindung zum Internet-Service-Provider (ISP).
- Welche Internet-Dienste Sie nutzen möchten.
- Welche Internet-Dienste Sie anderen Internet-Nutzern 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 Ihren Bedarf (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 Secure Sockets Layer(SSL)).

Bei der Entwicklung Internet-Nutzungs- 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 helfen, die Problematik beim Erstellen eines umfassenden Sicherheitsplans besser zu verstehen.
- **Szenario: e-business Pläne des Unternehmens JKL Toy** enthält ein praxisnahes Modell der Internet-Nutzungs- und Sicherheitspläne eines Unternehmens, das Sie beim Erstellen Ihrer eigenen Pläne nutzen können.

Obwohl das Produkt eingestellt wurde, können Sie nach wie vor die Planungsarbeitsblätter von IBM Firewall for AS/400 für die Dokumentation Ihrer eigenen Pläne nutzen. Diese Arbeitsblätter können Ihnen bei der Zusammenstellung wichtiger Zusatzinformationen über Ihre Internet-Nutzungspläne und die interne Netzkonfiguration sowie bei der Ermittlung Ihrer Sicherheitsbedürfnisse behilflich sein. Der Zugriff auf die Arbeitsblätter erfolgt über das Thema Firewall: Getting started

 im iSeries Information Center für V4R5. Ob Sie sich für ein Firewall-Produkt

entscheiden oder nicht - die Daten, die Sie für die Planung Ihrer Internet-Sicherheitsrichtlinien zusammenstellen müssen, sind im Großen und Ganzen dieselben.

Sicherheit durch mehrfache Abwehrstufen

Durch Ihre **Sicherheitsrichtlinien** wird definiert, 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 der Umgang mit dem 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 400 minimiert werden, sofern diese richtig konfiguriert sind. Bei der Anbindung Ihrer iSeries ans Internet müssen Sie jedoch zusätzliche Maßnahmen ergreifen, um die Sicherheit Ihres internen Netzes auch weiterhin zu gewährleisten.

Der Internet-Zugriff zwecks Durchführung geschäftlicher Aktivitäten birgt zahlreiche Risiken. Beim Erstellen der Sicherheitsrichtlinien gilt es zwischen dem Abgebot an Diensten und 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 Internet-Dienste 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.

Im Internet tummeln sich die verschiedensten Individuen, die die Sicherheit der Internet-Kommunikation 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 lediglich 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 Internet-Sicherheitsrisiken auf verschiedenen Ebenen geben kann, müssen Sie Sicherheitsmaßnahmen ergreifen, die mehrfache Abwehrstufen umfassen. Im Allgemeinen sollten Sie sich vor der Internet-Anbindung 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 aus einer durchdachten proaktiven Offensive. Wenn Sie bei der Planung der Internet-Sicherheit 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 die 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 Internet-Sicherheitsstrategie darin bestehen, die grundlegenden Einstellungen für den iSeries-Systemschutz sorgfältig zu konfigurieren.

Sicherheit auf Netzebene
Maßnahmen zur Netzsicherheit regeln den Zugriff auf Ihre iSeries und andere Netzsysteme. 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 Netzschutzmethode sollte die vom ISP gebotenen Sicherheitsmaßnahmen umreißen, wie beispielsweise Filterregeln für die ISP-Routerverbindung sowie Sicherheitsvorkehrungen für den öffentlichen Domain Name Service (DNS).

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 beschaffen. Die Sicherheitsmaßnahmen, für die Sie sich entscheiden, müssen sowohl die Sicherheitsrisiken auf der Serverseite als auch die auf der Clientseite abdecken.

Sicherheit auf Übertragungsebene

Sicherheitsmaßnahmen auf Übertragungsebene schützen die Datenübertragung innerhalb eines Netzes und zwischen verschiedenen Netzen. Wenn Sie Daten über ein ungesichertes Netz wie das Internet übertragen, können Sie den Datenfluss zwischen Quelle und Ziel nicht steuern. Der Datenverkehr fließt durch viele verschiedene Server, auf die Sie keinen Einfluss haben. Sofern Sie keine Sicherheitsmaßnahmen treffen, beispielsweise indem Sie Ihre Anwendungen für die Verwendung von Secure Sockets Layer (SSL) konfigurieren, kann jeder Ihre weitergeleiteten Daten einsehen und verwenden. Sicherheitsmaßnahmen auf Übertragungsebene schützen Ihre Daten, während sie zwischen den anderen geschützten Bereichen hin und her fließen.

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

Sicherheitsrichtlinien und Sicherheitsziele

Ihre Sicherheitsrichtlinien

Jeder Internet-Dienst, 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 betreffen 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 Umgang mit dem 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, um sicherzustellen, dass Sie alle neuen Risiken erfassen, die sich durch die Änderungen ergeben. Ein Beispiel für die Sicherheitsrichtlinien des Unternehmens JKL Toy finden Sie im iSeries 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 sie vorgibt zu sein. Eine gründliche Authentifizierung schützt ein System vor dem Sicherheitsrisiko des betrügerischen Auftretens, wobei ein Absender oder Empfänger eine falsche Identität verwendet, um auf ein System zuzugreifen. Traditionell werden auf Systemen Kennwörter und Benutzernamen für die Authentifizierung verwendet; Digitale Zertifikate können eine noch sicherere Authentifizierungsmethode darstellen, während sie außerdem zusätzliche Sicherheitsleistungen bieten. Wenn Sie Ihr System mit einem öffentlichen Netz wie dem Internet verbinden, gelten für die Benutzerauthentifizierung ganz neue Maßstäbe. Ein wichtiger Unterschied zwischen dem Internet und Ihrem Intranet besteht darin, dass Sie beim Intranet der Identität eines Benutzers, der sich anmeldet, eher trauen können. Daher sollten Sie ernstlich in Betracht ziehen, striktere Authentifizierungsmethoden als beim traditionellen Anmeldeverfahren mit Benutzername und Kennwort anzuwenden. Authentifizierte Benutzer können je nach Berechtigungsstufe unterschiedliche Zugangsberechtigungen haben.

Berechtigung

Die Gewissheit, dass eine Person oder ein Computer am anderen Ende der Sitzung berechtigt ist, die Anforderung auszuführen. Beim Erteilen einer Berechtigung wird festgelegt, wer oder was auf Systemressourcen zugreifen oder bestimmte Aktivitäten auf einem System ausführen darf. Normalerweise geschieht das Erteilen 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 garantierten, wenn Daten aus ungesicherten Quellen auf Ihr System gelangen. Für Daten, die aus einem öffentlichen Netz auf Ihrem System ankommen, sind möglicherweise Sicherheitsvorkehrungen mit dem folgenden Zielen erforderlich:

- Die Daten vor dem „Ausschnüffeln" (Sniffing) und Interpretieren schützen, was normalerweise durch Verschlüsseln geschieht.
- 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. Da die Systemintegrität bei der iSeries ein wesentlicher Bestandteil der Architektur ist, wird sie als Sicherheitskomponente meist übersehen. 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 öffentlichem 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 (verweigerten) 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 all Ihre Sicherheitsbedürfnisse hinsichtlich Netzbetrieb und Internet abdecken. 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 Internet-Nutzungsplanung und die Sicherheitsplanung des Beispielunternehmens sind ein repräsentatives Modell für viele reale Unternehmen.

Szenario: e-business Pläne des Unternehmens JKL Toy

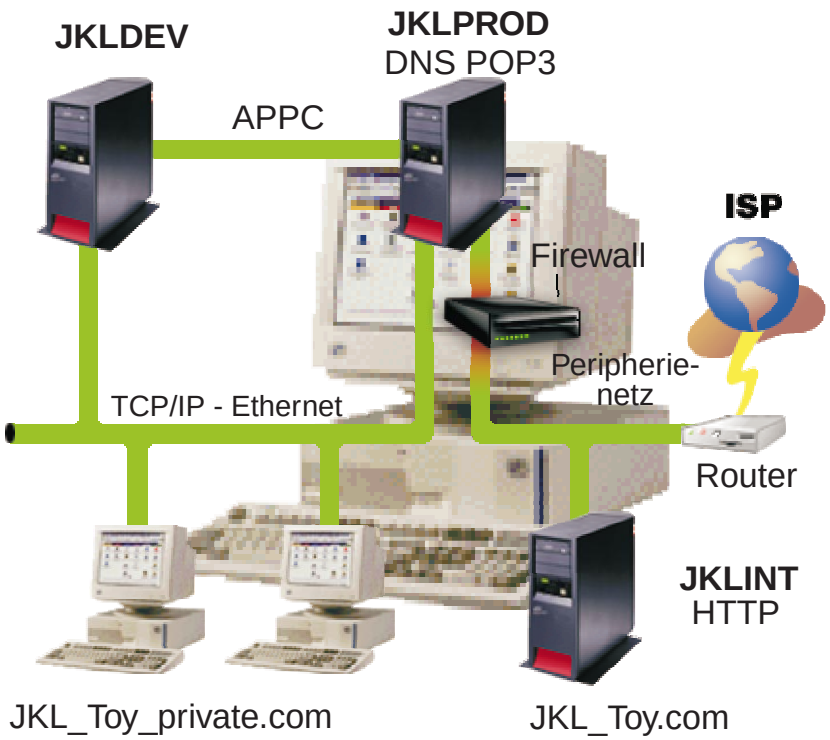
In diesem Szenario wird ein typisches Unternehmen beschrieben (JKL Toy), das seine Unternehmensziele mittels Internet ausweiten möchte. Auch wenn es sich hierbei nur um ein fiktives Unternehmen handelt, sind doch die Pläne zur Nutzung des Internets für e-business und des sich daraus ergebenden Sicherheitsbedürfnisses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

Das Unternehmen JKL Toy ist ein zwar kleiner doch rasch wachsender Spielwarenhersteller, dessen Palette vom Springseil über Papierdrachen bis hin zum Plüschleoparden reicht. Der Firmenchef zeigt sich enthusiastisch 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 Internet-Marketingpräsenz zu verschaffen, einschließlich Online-Katalog. 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 Internet-Zugriff zu Forschungs- und Entwicklungszwecken gestatten. Schließlich sollen Kunden die Möglichkeit erhalten, die Website des Unternehmens für direkte Online-Bestellungen 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 Internet-Präsenz:
- Förderung des Firmenimages und der Firmenpräsenz im Rahmen einer umfassenden Werbekampagne
- Bereitstellung eines Online-Produktkatalogs 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-Systeme über einen wirksamen Basissystemschutz verfügen, hat sich JKL Toy dafür entschieden, ein Firewall-Produkt für die Sicherheit auf Netzebene einzusetzen. Die Firewall schirmt das interne Netz vor zahlreichen potenziellen Internet-Risiken 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-Systeme. Ein System wird für Entwicklungs- und eins für Produktionsanwendungen ((JKLDEV bzw. JKLPROD) eingesetzt. Da auf beiden Systemen unternehmenskritische Daten und Anwendungen verarbeitet werden, gibt es Bedenken, die Internet-Anwendungen ebenfalls auf diesen Systemen auszuführen. Stattdessen soll ein neues iSeries-System (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 Internet-Risiken, denen die internen Systeme ausgesetzt sind. Dadurch dass 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-System aus. Während dieser Phase der e-business Planung stellt das neue System lediglich eine statische öffentliche Website zur Verfügung. Das Unternehmen möchte jedoch Sicherheitsmaßnahmen zum Schutz des Systems und der öffentlichen Website implementieren, und auf diese Weise Serviceunterbrechungen und andere möglichen Angriffe zu verhindern. Aus diesem Grund schützt das Unternehmen das System sowohl mit Regeln zur Paketfilterung und Netzadresskonvertierung als auch mit strengen allgemeinen Sicherheitsmaßnahmen.

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

Kapitel 5. Sicherheitsstufen als Voraussetzung für Internet-Zugang

Ihre Systemschutzmaßnahmen bilden die letzte Verteidigungslinie gegen ein internetbasiertes Sicherheitsproblem. Daher muss der erste Schritt beim Aufbau einer umfassenden Internet-Sicherheitsstrategie darin bestehen, die grundlegenden OS/400-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.

  Anmerkung: Bei einer stark transaktionsorientierten Anwendung oder einer Anwendung mit extensiver Nutzung des Integrated File System (IFS) kann der Betrieb mit Sicherheitsstufe 50 zu einer Verschlechterung der System- oder Anwendungsleistung führen.

  Einzelheiten zu den jeweiligen iSeries-Sicherheitsstufen finden Sie in Tips and Tools for Securing your iSeries.

  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 zu einer höheren Sicherheitsstufe wechseln.
- Setzen Sie Ihre sicherheitsrelevanten Systemwerte auf Werte, die mindestens den empfohlenen Einstellungen entsprechen. Sie können Ihre und die empfohlenen Einstellungen mit Hilfe des Sicherheitsassistenten des Operations Navigator oder des Technical Studio Security Advisor vergleichen.
- 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. Das heißt, 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 Internet-Umgebung nicht aus.
- Sie **müssen** die Objektberechtigung auf Ihrem System definieren. Weitere Informationen über das Arbeiten mit der Objektberechtigung finden Sie im Kapitel über iSeries Navigator in Tips and Tools for Securing your iSeries

Zur Konfiguration dieser Mindestanforderungen an den Systemschutz können Sie entweder den **Security Advisor** (verfügbar über die Technical Studio-Website) oder den **Sicherheitsassistenten** (verfügbar über die iSeries Navigator-Schnittstelle) verwenden. Der Technical Studio Security Advisor 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 ebenfalls Empfehlungen ausgehend von Ihren Antworten auf eine Reihe von Fragen. 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 Internet-Nutzung beginnen.

Kapitel 6. Optionen für Netzsicherheit

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 Netzschutzmethode 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 Internet-Sicherheitsrisiken 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 Ihr iSeries-System oder internes Netz mit dem Internet oder einem anderen ungesicherten Netz verbinden, ziehen Sie auf jeden Fall den Einsatz eines Firewall-Produkts 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.

Weitere Informationen über die Umstellung von einer vorhandenen IBM Firewall for AS/400 auf andere Produkte oder auf die nativen Netzsicherheitseinrichtungen der iSeries finden Sie in All You Need to Know When Migrating from IBM Firewall for AS/400 (SG24-6152).

Da kommerzielle Firewall-Produkte 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 Firewall-Produkt bieten kann. Sie sollten Ihre Sicherheitsbedürfnisse und Sicherheitsziele sorgfältig analysieren, wenn es darum geht, sich zwischen einem vollständigen Firewall-Produkt und den iSeries-Paketregeln zu entscheiden.

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

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 Firewall-Funktionen 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, dessen Zutritt Sie 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.
- Software. Die Firewall-Software stellt diverse Anwendungen zur Verfügung. Hinsichtlich der Netzsicherheit bietet eine Firewall Schutz mit Hilfe der folgenden Verfahren:
  - IP-Paketfilterung (IP = Internet Protocol)
  - Netzadresskonvertierung (NAT)
  - SOCKS-Server
  - Proxy-Server für diverse Dienste wie beispielsweise HTTP, Telnet, FTP u.s.w.
  - Mail Relay Services
  - Split Domain Name Services (DNS)
  - Protokollierung
  - Echtzeitüberwachung

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

Firewall-Verfahren 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 Internet-Benutzern 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 über Ihre internen Systeme steuern.

Bei der Definition einer Firewall-Strategie 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 Ihre Firewall steuern soll, 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 (siehe Tabelle unten). Da Sie nur einen Berührungspunkt haben, können Sie besser kontrollieren, welche Daten Sie ins Netz hinein lassen 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 Netzadresskonvertierung (NAT) zur Verfügung, wobei sie Ihre internen Netzadressen 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) benutzen könnte, 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

iSeries 400-Paketregeln ist ein integriertes OS/400-Feature, das über die Operations 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:

- Netzadresskonvertierung (NAT)
- IP-Paketfilterung

Da NAT und IP-Filterung integrierte OS/400-Bestandteile sind, bieten sie Ihnen eine wirtschaftliche Möglichkeit zum Schutz Ihres System. 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 Netzadresskonvertierung (NAT) werden die Quellen- oder die Ziel-IP-Adressen 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 Operations 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 Zugriff auf Ihr Netz gewährt und welchen er verweigert wird. Wenn Filterregeln erstellt werden, werden sie auf eine physische Schnittstelle (z. B. eine Token-Ring- oder Ethernetleitung) 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:
  - Ziel-IP-Adresse
  - Protokoll der Quellen-IP-Adresse (z. B. TCP, und UDP)
  - Zielport (z. B. Port 80 für HTTP)
  - Ausgangsport
  - 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.

Optionen für iSeries-Netzsicherheit wählen

Lösungen für die Netzsicherheit, die vor unbefugtem Zugriff schützen, basieren in der Regel auf Firewalls. Sie können sich für ein mit allen Funktionen ausgestattetes Firewall-Produkt als Schutz für Ihr iSeries 400-System entscheiden, oder Sie aktivieren spezielle Netzsicherheitstechnologien als Bestandteil der OS/400 TCP/IP-Implementation. Diese Implementation besteht aus dem Feature Paketregeln (enthält IP-Filterung und NAT) und dem Feature HTTP for 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 Firewall-Produkts als wichtigste Abwehrmaßnahme in Betracht ziehen, wann immer Sie Ihr iSeries-System oder 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 OS/400 TCP/IP-Technologien für den Internet-Zugriffsschutz 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 Firewall-Produkt stellt keinerlei weiteren 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 brauchbarer 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 Firewall-Einheit 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.

Sicherheits-technologie	OS/400 TCP/IP-Technologie	Mit allen Funktionen ausgestattete Firewall
IP-Paketfilterung	• **Zusätzlicher** Schutz für ein einzelnes iSeries-System wie beispielsweise ein öffentlicher Webserver oder ein Intranet-System mit sensiblen Daten. • Schutz für ein Teilnetz eines unternehmensweiten **Intranets**, wenn das iSeries-System als Gateway (gewöhnlicher Router) für das restliche Netz fungiert. • Steuerung der Kommunikation mit einem vertrauenswürdigen Partner über ein **privates Netz** oder ein Extranet, wobei das iSeries-System 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.
Netzadresskonvertierung (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 OS/400 TCP/IP-Sicherheitseinrichtungen finden Sie in folgenden Quellen:

- Paketregeln (Filterung und NAT).
- HTTP Server Documentation Center.
- AS/400 Internet Security Scenarios: A Practical Approach (SG24-5954).

Kapitel 7. Optionen für Anwendungssicherheit

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 leicht von Unbefugten missbraucht werden, die eine Möglichkeit suchen, sich Zugriff auf Ihre Netzsysteme zu beschaffen. Die von Ihnen angewandten Sicherheitsmaßnahmen müssen sowohl die Sicherheitsrisiken auf der Serverseite als auch die auf der Clientseite abdecken.

Während es wichtig ist, alle von Ihnen benutzten Anwendungen zu schützen, 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 Internet-Anwendungen finden Sie auf den folgenden Seiten:
- „Sicherheit für Webserving"
- „Java-Internet-Sicherheit" auf Seite 29
- „E-Mail-Sicherheit" auf Seite 31
- „FTP-Sicherheit" auf Seite 33

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 400 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 Programme 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 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-Server für iSeries verwenden, um den Webzugriff zu konsolidieren. Der Proxy-Server kann ebenfalls Protokolle aller URL-Anforderungen erstellen, die Überwachungszwecken dienen können. Anhand dieser Protokolle können Sie Gebrauch und Missbrauch von Netzressourcen überprüfen.

Weitere Informationen zu diesem Themenkreis finden Sie im Buch *Tips and Tools for Securing Your iSeries*.

Java-Internet-Sicherheit

In den Datenverarbeitungsumgebungen 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 Internet-Sicherheitsrisiken 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 über das Zusammenwirken von Java und Ressourcenschutz hinsichtlich Authentifizierung und Berechtigung für Java-Programme Bescheid wissen.

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. Zeigermanipulation ist nicht zulässig, 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 Ihrer iSeries 400 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 hat jedoch die Möglichkeit, auf Ihre iSeries 400 zuzugreifen. (Ein ODBC-Programm oder ein APPC-Programm (APPC = 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 Sitzung 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 Ihrer iSeries 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-System 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-Viewer 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 Ihrer iSeries 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.

Möglicherweise müssen Sie signierte Applets einsetzen, die Ihre iSeries dann bereit stellt. 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 (SSL = Secure Sockets Layer) definieren. Außerdem können Sie den 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 von IBM HTTP-Server für iSeries gehört, bietet Unterstützung für die Verwendung von Servlets auf iSeries-Systemen.

Auf Servletobjekte, 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 in folgenden Quellen:

- IBM Developer Kit for Java - Java Security.
- IBM Toolbox for Java - Security Classes.
- Tips and Tools for Securing Your iSeries  .

Java-Authentifizierung und -Berechtigung für Ressourcen

Die IBM Toolbox for Java enthält Sicherheitsklassen, um die Identität eines Benutzers zu prüfen und diese Identität wahlweise dem Betriebssystemthread für eine Anwendung oder einen Server zuzuordnen, der auf einem iSeries-System läuft. Nachfolgende Ressourcenschutzüberprüfungen finden unter der zugeordneten Identität statt. Einzelheiten zu diesen Sicherheitsklassen finden Sie unter IBM Toolbox for Java - Authentication Services.

Das IBM Developer Kit for Java unterstützt JAAS (Java Authentication and Authorization Service), 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 Basis der Codequelle). Weitere Informationen über die Verwendung von J2SDK finden Sie unter Java Authentication and Authorization Service.

Java-Anwendungen mit SSL sichern

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

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

- IBM Toolbox for Java - Secure Sockets Layer (SSL).
- IBM Developer Toolkit for Java - Making a Java application secure with SSL.

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 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 zu überlasten. Ohne entsprechende Sicherheitseinrichtungen kann auf dem Zielserver ein Servicezusammenbruch (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 Ausgangs- und Ziel-IP-Adresse, vertraulich behandelt werden?

Einige Anwendungen verfügen über integrierte Sicherheitseinrichtungen, die den Schutz bieten, den Sie benötigen. Lotus Notes Domino bietet beispielsweise zahlreiche integrierte Sicherheitseinrichtungen, zu denen u.a. die Verschlüsselung eines gesamten Dokuments oder einzelner Felder in einem Dokument gehört.

Zur Verschlüsselung von Mail 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 verschlüsselte 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.

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

- Auf der Website Lotus Domino Reference Library.
- Auf der Website Lotus Notes User Assistance.
- 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 Secure Sockets Layer (SSL) unterstützt, können Sie eine sichere Kommunikationssitzung zwischen dem Server und E-Mail-Clients einrichten. SSL bietet ebenfalls Unterstützung für die wahlweise Authentifizierung auf 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 (VPN = 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.

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 sich über diese Risiken im Klaren sein, damit Sie in Ihren Sicherheitsrichtlinien beschreiben können, wie Sie diese Risiken minimieren möchten.

- 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.

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.

Ab V5R1 können Sie Secure Sockets Layer (SSL) verwenden, um sichere Kommunikationssitzungen für Ihren FTP-Server herzustellen. 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.

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

- Implementing FTP security
- Anonymous FTP.
- Securing FTP.
- Tips and Tools for Securing your iSeries  .

Kapitel 8. Optionen für Übertragungssicherheit

Wie bereits erwähnt, verfügt das Unternehmen JKL Toy über zwei primäre iSeries 400-Systeme. Eins wird für Entwicklungs- das andere für Produktionsanwendungen eingesetzt. Da sich auf beiden Systemen unternehmenskritische Daten und Anwendungen befinden, hat das Unternehmen beschlossen, für seine Intranet- und Internet-Anwendungen 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 Internet-Risiken, denen die internen Systeme ausgesetzt sind. Dadurch dass die neue iSeries 400 lediglich als Internet-Server zugeordnet wird, gestaltet sich auch der Verwaltungsaufwand für die Netzsicherheit weniger kompliziert.

Wegen des jederzeit und überall in einer Internet-Umgebung bestehenden Bedarfs an Sicherheit, entwickelt IBM ständig entsprechende Angebote, um einen sicheren Netzbetrieb für die Durchführung von e-business im Internet zu gewährleisten. In einer Internet-Umgebung müssen Sie sowohl für systemspezifische als auch anwendungsspezifische Sicherheit sorgen. Das Versenden vertraulicher Informationen über ein unternehmensinternes Intranet oder eine Internet-Verbindung 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 iSeries-Sicherheitsangebote auf Übertragungsebene minimiert werden: Gesicherte SSL-Kommunikation (SSL = Secure Sockets Layer) und VPN-Verbindungen (VPN = Virtual Private Networking).

Anwendungen mit SSL sichern

Das Protokoll Secure Sockets Layer (SSL) 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 die folgenden iSeries-Anwendungen:

- IBM HTTP-Server für iSeries (Original und auf Apache-Basis)
- FTP-Server
- Telnet-Server
- DRDA (Architektur einer verteilten relationalen Datenbank) und Verwaltung für verteilte Daten
- (DDM)-Server
- Management Central
- Directory Services Server (LDAP)
- Client Access Express-Anwendungen, einschließlich Operations Navigator, und Anwendungen, die für die APIs (Anwendungsprogrammierschnittstellen) von Client Access Express erstellt werden.

- Programme, die mit Developer Kit for Java entwickelt wurden, und Clientanwendungen, die 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 das Bedürfnis nach sicherer 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-/Leistungsverhältnisses Sie 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 Client Access Express bereits über diese Möglichkeit. 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.

Digitale Zertifikate für SSL verwenden

Digitale Zertifikate bilden die Basis für die Verwendung von Secure Sockets Layer (SSL) für die sichere Kommunikation und als striktere Authentifizierungsmethode. Auf der iSeries 400 können Sie mit Hilfe von Digital Certificate Manager (DCM), einem integrierten OS/400-Feature, problemlos Zertifikate für Ihre Systeme und Benutzer erstellen und verwalten.

Außerdem können Sie einige Anwendungen, beispielsweise IBM HTTP-Server für iSeries, derart 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 gültiger Berechtigungsnachweis.

Für jede Zertifizierungsinstanz gelten bestimmte Richtlinien bei der Festlegung, welche Identifikationsdaten zur Ausstellung eines Zertifikats erforderlich sind. Einige Internet-Zertifizierungsinstanzen verlangen möglicherweise nur wenige Informationen, wie beispielsweise einen registrierten Namen. Ein registrierter Name ist der Name der Person oder des 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 einer gesicherten Datei gespeichert wird. Der Zertifikatseigner kann diese Schlüssel verwenden, um Daten wie Nachrichten und Dokumente, die zwischen Benutzern und Servern hin- und hergesendet werden, zu "signieren" und zu verschlüsseln. Durch solche digitalen Signaturen kann der Ursprung eines Objektes zuverlässig festgestellt und seine Integrität gewährleistet werden.

Obwohl zahlreiche Anwendungen SSL noch nicht nutzen können, verfügen viele andere wie beispielsweise Telnet und Client Access Express bereits über diese Möglichkeiten. Informationen darüber, wie Sie SSL für iSeries-Anwendungen nutzen können, finden Sie unter dem Thema **Anwendungen mit SSL sichern** im iSeries Information Center.

SSL für sicheren Telnet-Zugriff

Ab V4R4 können Sie Ihren Telnet-Server für die Verwendung von Secure Sockets Layer (SSL) 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 Server-Authentifizierung werden bei Telnet die Daten verschlüsselt, noch 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 Sensitivität der Informationen beachtet werden, die in einer Client-Sitzung 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 ADDTCP-PORT. 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 in den folgenden Quellen:

- Unter dem Thema Telnet im Information Center finden Sie Informationen, die Sie für die Verwendung von Telnet auf Ihrer iSeries benötigen.
- Securing Telnet enthält Informationen über die gemeinsame Verwendung von SSL und Telnet zum Sichern von Telnet-Kommunikationssitzungen.
- Tips and Tools for Securing Your iSeries  enthält im Abschnitt über TCP/IP detaillierte Informationen über die Telnet-Sicherheit.

SSL für sicheres Client Access Express

Ab V4R4 können Sie Ihre Client Access Express-Server für die Verwendung von Secure Sockets Layer (SSL) konfigurieren, um Client Access Express-Kommunikationssitzungen zu sichern. Beispiel: Im Zuge des Wachstums des Unternehmens JKL Toy wurden zahlreiche regionale Außendienstmitarbeiter eingestellt. Diese müssen von Ihren Heimbüros aus auf Informationen in den iSeries-Produktionssystemen zugreifen können, die Auskunft über den Stand der Warenverfügbarkeit und über Produktionsdaten geben. Da es sich hierbei um sensible Daten handelt, hat JKL Toy beschlossen, den Außendienstmitarbeitern den Zugriff auf diese Informationen nur über sicheres Client Access Express zu gewähren.

Die Verwendung von SSL garantiert, dass der gesamte Datenverkehr für die Client 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 Client Access Express mit SSL finden Sie in den folgenden Quellen:

- Secure Sockets Layer Administration
- Securing Client Access Express and Operations Navigator
- IBM Developer Kit for Java - SSL
- IBM Java Toolbox - SSL

Virtual Private Networks (VPN) für sichere private Kommunikation

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-Systemen, 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 kostenintensiver als die Verwendung herkömmlicher Standleitungen.

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

Folgende Benutzer könnten Nutznießer der Verwendung von VPNs für die Konnektivität sein:

- 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: dem 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 vor 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 durchläuft. Je nach Konfiguration kann es vorkommen, dass für eine VPN-Verbindung Daten unverschlüsselt durch interne Netze fließen. 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 die 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. Auch ist eine VPN-Verbindung nicht die einzige Möglichkeit für die Herstellung einer sicheren Kommunikation zwischen Ihrer iSeries 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.

Kapitel 9. Internet-Sicherheit - Terminologie

Als Grundlage für die Erörterung der Internet-Sicherheit beginnen Sie mit der Definition einiger Internet-Begriffe. Wenn Sie bereits mit der Internet-Terminologie vertraut sind, können Sie diesen Abschnitt überspringen.

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

Cracker
Ein Hacker mit unlauteren Absichten.

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 Algorithmus und eine geheime Folge von Daten (der Schlüssel) benötigt.

Es gibt zwei Arten von Kryptografie:
- Bei der Kryptografie mit einem geheimen Schlüssel für gemeinsame Benutzung **(symmetrische Kryptografie)** wird ein geheimer Schlüssel von beiden Kommunikationsteilnehmern gemeinsam verwendet. Für die Ver- und Entschlüsselung wird der gleiche Schlüssel verwendet.
- Bei der Kryptografie mit einem öffentlichen Schlüssel **(asymmetrische Kryptografie)** werden für die Ver- und Entschlüsselung unterschiedliche Schlüssel verwendet. Ein Teilnehmer hat 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. Auf diese Weise wird der Ursprung des Dokuments belegt.

Digitales Zertifikat
Ein digitales Zertifikat ist 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 gültiger Berechtigungsnachweis. Zertifikate können für folgende Zwecke eingesetzt werden:
- Identifikation - wer ist der Benutzer
- Authentifizierung - Sicherstellen, dass der Benutzer derjenige ist, der er vorgibt zu sein.

- Integrität - Feststellen, ob der Inhalt eines Dokuments geändert wurde, indem die digitale ″Signatur″ des Absenders verifiziert wird.
- Unbestreitbarkeit - Garantieren, 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
Eine digitale Signatur auf einem elektronischen Dokument 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)
Digital Certificate Manager lässt OS/400 als lokale Zertifizierungsinstanz (CA) zu. 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 OS/400-Benutzerprofil zuordnen. DCM wird weiterhin dazu verwendet, Anwendungen für die sichere Kommunikation mit Secure Sockets Layer (SSL) zu konfigurieren.

Registrierter Name
Ein registrierter Name ist 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.

Domänennamensserver (DNS)
Ein Internet-Host, der Internet-Namen in IP-Adressen konvertiert, häufig indem er mit anderen DNS-Servern im Internet interagiert. Beispiel: Viele DNS-Server könnten

```
vnet.ibm.com
```

erkennen, aber wahrscheinlich kennen nur ein paar wenige die vollständige IP-Adresse für:

```
system1.vnet.ibm.com
```

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

Verschlüsselung
Bei der Verschlüsselung werden Daten in ein Format umgewandelt, das nur von jemandem mit der richtigen Entschlüsselungsmethode gelesen werden kann. Unbefugte können die Informationen zwar immer noch abfangen, aber ohne die richtige Entschlüsselungsmethode sind die Informationen unverständlich.

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.

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

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

Hypertext-Links
Eine Möglichkeit, online Informationen über Verbindungen—(den sog. Hypertext-Links) 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 Transport Protocol (HTTP)
Die Standardmethode für den Zugriff auf Hypertextdokumente.

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 Internet-Diensten 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.

Internet Key Exchange (IKE)
Wenn das Protokoll IKE mit IPSec verwendet wird, unterstützt es sowohl die automatische Vereinbarung von Sicherheitszuordnungen als auch die automatische Generierung und Aktualisierung von Chiffrierschlüsseln. Im Allgemeinen wird IKE als Bestandteil des Virtual Private Networking verwendet.

Internet-Name
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 Internet-Namen wie

```
system1.vnet.ibm.com
```

zugeordnet werden.

Ein Internet-Name wird auch als vollständig qualifizierter Domänenname bezeichnet. Bei einer Werbung wie „Besuchen Sie unsere Homepage", beinhaltet die "Homepage-Adresse" den Internet-Namen und nicht die IP-Adresse, da der Internet-Name leichter zu merken ist.

Ein vollständig qualifizierter Domänenname hat zahlreiche Bestandteile. Z. B. hat

```
system1.vnet.ibm.com
```

die folgenden Bestandteile:

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 diese Kennung haben.

```
ibm.com
```

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 Internet-Zugang 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
In einem TCP/IP-Netz (das Internet ist ein sehr großes TCP/IP-Netz) sind Sie unter der IP-Adresse (IP = Internet Protocol) bekannt. 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 Ursprung und Ziel.

IP-Filter
IP-Filter bilden die Grundlage des Schutzmechanismus der Firewall. Anhand von IP-Sitzungsdetails kann durch Filter bestimmt werden, welcher Datenverkehr die Firewall durchfließen darf. 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 verweigert allen Crackern, außer den ganz wild entschlossenen, den Zugriff.

IPSec Eine Gruppe von Protokollen zur Unterstützung des sicheren Austauschs von Paketen auf der IP-Schicht. IPSec ist eine Gruppe von Standards, die von iSeries 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.

Netzadresskonvertierung (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. Sie kann einen öffentlichen Webserver schützen, den Sie in Ihrem internen Netz betreiben möchten. 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 bietet internen Benutzern außerdem die Möglichkeit, auf das Internet zuzugreifen, ohne ihre privaten internen IP-Adressen preiszugeben. Wenn Sie internen Benutzern gestatten, auf Internet-Dienste zuzugreifen, bietet NAT insofern Schutz, als Sie die privaten Adressen der Benutzer verbergen können.

Unbestreitbarkeit
Die Unbestreitbarkeit ist ein 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.

Paket Ein Datagramm, das Informationen über das Leitungsprotokoll, beispielsweise Ethernet Token-Ring oder Frame-Relay, beinhaltet.

Proxy Proxy-Server ist 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, CA und anderen Registrierungsinstanzen, die die Gültigkeit aller an einer Internet-Transaktion beteiligten Teilnehmer verifizieren.

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 (elektronisches Schnüffeln)
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. Hinweise auf erfolgreiches Ausspionieren 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
SOCKS ist eine Client/Serverarchitektur, 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.

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 Trojanisches Pferd ist ein Computerprogramm, das eine vermeintlich hilfreiche, harmlose Funktion ausführt. Tatsächlich trägt es jedoch versteckte Funktionen in sich, die dem Benutzer zugeordnete anerkannte Berechtigungen nutzen, sobald sie das Programm starten. Das Programm kann beispielsweise interne Berechtigungsinformationen von Ihrem Computer kopieren und zurück an den Absender des Trojanischen Pferdes senden.

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

Webbrowser
Die HTTP-Clientanwendung. Ein Webbrowser interpretiert HTML, um dem Benutzer Hypertextdokumente 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.

World Wide Web (WWW)
Ein Netz untereinander verbundener Server und Clients, die das gleiche Standardformat für das Erstellen von Dokumenten (HTML) und das Zugreifen auf Dokumente (HTTP) verwenden. Das Ineinandergreifen von Links sowohl von Server zu Server als auch von Dokument zu Dokument wird bildhaft auch als **das Web** (das Netz) bezeichnet.