UEBERSICHT.FM Seite 15 Freitag, 6. Dezember 2002 2:23 14

Übersicht

Einleitung: Gesellschaftlicher Wandel und IT-Sicherheit

Die Einleitung zeigt anhand von »Meilensteinen« die Entwicklungssprünge von Kryptographie, Informationstechnologie und Informationssicherheit sowie die Vorteile der Internet- und Intranet-Technologie und die daraus folgenden gesellschaftlichen Veränderungen. Die Notwendigkeiten und Chancen von IT-Sicherheit werden erläutert und der VPN-Markt wird dargestellt (VPN: Virtual Private Network).

Notwendigkeiten, Ziele und Anwendungsformen von VPN-Systemen

Nach der Definition des Begriffs »VPN« verdeutlichen Analogien, dass die Sicherheitsmechanismen zur Absicherung von heutigen Geschäftsprozessen den neuen Bedingungen angepasst werden müssen. Die Sicherheitsziele, die mit einem VPN-System realisierbar sind, werden dargestellt, ferner die grundsätzlichen Anwendungsformen: unternehmensweites VPN, sichere Remote-Ankopplung, VPN zwischen verschiedenen Unternehmen und Kombinationen.

Bedrohungen aus dem Netz

Die Motive von Angreifern und die potenziellen Angriffe auf Kommunikationssysteme werden beschrieben und eine Abschätzung über Eintrittswahrscheinlichkeit und mögliche Schäden wird vorgenommen.

Grundlegende Sicherheitsmechanismen

Zuerst werden einige grundlegende Sicherheitsmechanismen beschrieben, mit denen Kryptographiekonzepte für VPN-Systeme aufgebaut werden können. Anschließend erfolgt die Beschreibung der eigentlichen kryptographischen Algorithmen und der zur Verwaltung von Schlüsseln benötigten Infrastruktur.

Konzepte von Virtual Private Networks

In diesem Kapitel werden verschiedene Konzepte beziehungsweise Topologien diskutiert, nach denen VPN-Systeme aufgebaut werden können, die zur Sicherstellung einer vertrauenswürdigen Kommunikation genutzt werden. Außerdem werden Aspekte des Sicherheitsmanagements beschrieben.

UEBERSICHT.FM Seite 16 Freitag, 6. Dezember 2002 2:23 14

VPN-Verfahren

Um die drei Ziele einer vertrauenswürdigen Datenübertragung – Vertraulichkeit, Authentikation und Integrität – mit einem VPN zu realisieren, müssen eine Reihe von Überlegungen durchgeführt werden. Dieses Kapitel hilft beim Verständnis der Protokolle, die den vertrauenswürdigen Transport von Daten und den Austausch der Schlüssel durchführen.

Praktischer Einsatz von Virtual Private Networks (VPNs)

In diesem Kapitel wird zunächst anhand von Praxisbeispielen vorgestellt, wie verschiedene Unternehmen beziehungsweise Organisationen mit sehr unterschiedlichen Anforderungen Virtual Private Networks aufgebaut haben, um eine vertrauenswürdige Kommunikation gewährleisten zu können. Im Anschluss werden praktische Hinweise zur Implementierung von VPN-Systemen gegeben und die prinzipielle Vorgehensweise bei der Konfiguration am Beispiel zweier gängiger VPN-Lösungen wird erläutert.

VPNs für E- und M-Business

Öffentliche Netze wie das Internet und die Mobilfunknetze haben eine zentrale Bedeutung im Leben jedes Einzelnen gewonnen. Die Stichworte »E-Business« und »M-Business« stehen für die neue Flexibilität bei der Abwicklung von Geschäften wie Einkäufen, Reisebuchungen und Bankgeschäften. »E-Business« bezeichnet ganz allgemein die Abwicklung von geschäftlichen Transaktionen über öffentliche Netzwerke, »M-Business« ihre Abwicklung über das Mobilfunknetz. Das Kapitel beschreibt, wie in Zukunft mithilfe von VPNs auch für diese Anwendungen sichere Verbindungen geschaffen werden können.

VPN-Sicherheitspolitik und weitere Sicherheitsmaßnahmen

In diesem Kapitel wird erläutert, welche Aspekte bei der Erarbeitung einer VPN-Sicherheitspolitik berücksichtigt werden müssen und welche infrastrukturellen, organisatorischen und personellen Sicherheitsmaßnahmen ein VPN-System ergänzen müssen, damit ein hohes Maß an Gesamtsicherheit erreicht werden kann.

VPN: Eine Investition für die Zukunft

In diesem Kapitel werden die Kosten eines VPN-Systems aus unterschiedlichen Blickwinkeln betrachtet. Da ein VPN-System eine Investition für die Zukunft ist, sollten die Kosten-Nutzen-Aspekte schon bei der Planung besonders berücksichtigt werden.

UEBERSICHT.FM Seite 17 Freitag, 6. Dezember 2002 2:23 14

Evaluierung und Zertifizierung von VPNs

Vor der Anschaffung eines VPNs stellt sich Kunden und Benutzern die Frage, welche Sicherheitskriterien wirklich erfüllt werden. Mit dem Mittel der Evaluation kann überprüft werden, ob angegebene Sicherheitsfunktionalitäten tatsächlich vorhanden sind und ihre Funktion korrekt erfüllen. Ziel der Evaluierung ist, dem Anwender des Sicherheitssystems das Vertrauen zu geben, dass das VPN-System ordnungsgemäß und wunschgemäß arbeitet.

VPN-Systeme versus Firewall-Systeme

Der Sicherheitsmechanismus Verschlüsselung bei VPN-Systemen wirkt nur gegen die unerlaubte Einsicht der Informationen während der Kommunikation per Internet. Zusätzlich muss noch mithilfe von Firewall-Systemen das zweite Hauptrisiko beim Anschluss an das Internet, der unerlaubte Zugriff auf die eigenen Rechnersysteme, verhindert werden. Das Kapitel beschreibt neben der Grundidee von Firewall-Systemen deren verschiedene Elemente: Wie können damit technische Sicherheitsmechanismen realisiert werden und welche konkreten Möglichkeiten bestehen, Sicherheit zu gewährleisten?

Weiterführende Aufgabenstellungen

In diesem Kapitel werden einige weiterführende Aufgabenstellungen behandelt, die mit dem Betrieb von VPN-Systemen verbunden sind. Dazu gehören die Verfügbarkeit der Netzwerkdienste, Konzepte von Redundanzsystemen, mögliche Realisierungsformen von VPN-Gateways (im Router integriert oder als separate Sicherheitskomponenten), Hilfsmechanismen für die Verwaltung großer VPN-Netzwerke sowie ein Ausblick auf die zukünftige Entwicklung bei VPN-Systemen.

Anhang

- Recht im Internet
- Computerkriminalität – Fakten und Zahlen
- TCP/IP-Technologie für Internet und Intranet
- eine Liste der auf dem Markt vertretenen VPN-Anbieter
- wichtige Adressen und Web-Links
- Literaturverzeichnis
- Glossar mit Abkürzungen
- die Legende für die Symbole, die im Buch verwendet werden
- Stichwortverzeichnis

UEBERSICHT.FM Seite 18 Freitag, 6. Dezember 2002 2:23 14