Erstellen sicherer ASP.NET-Anwendungen

Authentifizierung, Autorisierung und sichere Kommunikation

Kapitel 6 - Extranetsicherheit

J.D. Meier, Alex Mackman, Michael Dunner und Srinath Vasireddy

Microsoft Corporation

Oktober 2002

Auf der Orientierungsseite finden Sie einen Ausgangspunkt und eine vollständige Übersicht zum *Erstellen sicherer ASP.NET-Anwendungen*.

Zusammenfassung

In diesem Kapitel wird beschrieben, wie häufige Extranetanwendungsszenarien gesichert werden. Es enthält eine Darstellung der Merkmale der einzelnen Szenarien und eine Beschreibung der erforderlichen Schritte, um das Szenario zu sichern. Weitere Informationen finden Sie in den entsprechenden Analyseabschnitten.

Inhalt

Bei Extranetanwendungen handelt es sich um Anwendungen, die Ressourcen oder Anwendungen in zwei verschiedenen Firmen oder Geschäftsbereichen freigeben. Die Anwendungen und Ressourcen werden über das Internet bereitgestellt. Eine der Hauptherausforderungen bei Extranetanwendungen besteht in der Entwicklung eines Authentifizierungsverfahrens, dem beide Beteiligte zustimmen. Die Auswahlmöglichkeiten können in dieser Hinsicht eingeschränkt sein, da u. U. eine Interoperabilität mit bestehenden Authentifizierungsmechanismen erforderlich ist.

Extranetanwendungen weisen in der Regel einige gemeinsame Merkmale auf:

- Sie besitzen im Vergleich zu Internetszenarien mehr Kontrolle über Benutzerkonten.
- Die Vertrauenswürdigkeit der Benutzerkonten ist im Vergleich zu Anwendungen mit Internetbenutzern u. U. größer.

Die in diesem Kapitel behandelten Szenarien, anhand derer die empfohlenen Techniken für Authentifizierung, Autorisierung und sichere Kommunikation veranschaulicht werden, umfassen:

- Bereitstellen eines Webdienstes
- Bereitstellen einer Webanwendung

Bereitstellen eines Webdienstes

Betrachten Sie ein Szenario mit Datenaustausch zwischen Geschäftspartnern (B2B, "Business-to-business"), in dem ein Verlagsunternehmen Dienste über das Internet veröffentlicht und verkauft. Die Informationen werden für ausgewählte Partnerfirmen über einen Webdienst bereitgestellt. Die Benutzer in den Partnerfirmen greifen in diesem Szenario mit einer intranetbasierten internen Webanwendung auf den Webdienst zu (siehe Abbildung 6.1).

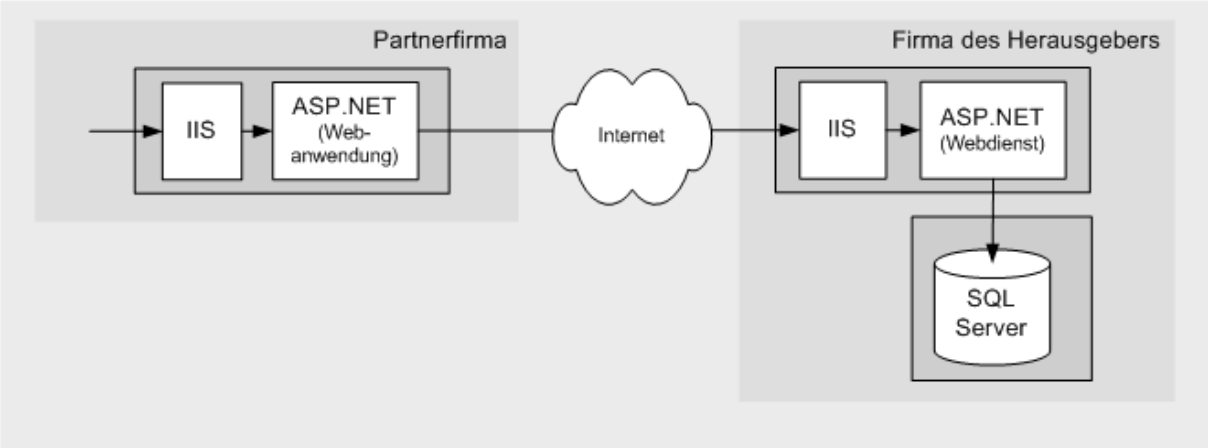

Abbildung 6.1
Extranetwebdienst für den Datenaustausch zwischen B2B-Partnern

Merkmale

Dieses Szenario weist die folgenden Merkmale auf:

- Die Verlagsfirma stellt über das Internet einen Webdienst bereit.
- Die Anmeldeinformationen (X.509-Clientzertifikate) der Partnerfirma (nicht einzelner Benutzer) werden vom Verlag überprüft, um den Zugriff auf Ressourcen zu autorisieren. Der Verleger braucht die Anmeldenamen der einzelnen Benutzer in der Partnerfirma nicht zu kennen.
- Die Clientzertifikate sind in der Verlagsfirma Konten im Verzeichnisdienst Active Directory® zugeordnet.
- Das Extranet enthält ein vom (internen) Active Directory der Firma getrenntes Active Directory. Das Active Directory des Extranets befindet sich in einer getrennten Gesamtstruktur, die eine getrennte Vertrauensgrenze bereitstellt.
- Die Autorisierung für den Webdienst basiert auf dem zugeordneten Active Directory-Konto. Sie können getrennte Autorisierungsentscheidungen basierend auf der Identität der Partnerfirma verwenden (die durch getrennte Active Directory-Konten für die einzelnen Firmen dargestellt werden).
- Der Zugriff auf die Datenbank erfolgt über eine einzige vertrauenswürdige Verbindung, die der Prozessidentität des ASP.NET-Webdienstes entspricht.
- Die vom Webdienst abgerufenen Daten sind vertraulich und müssen bei der Übertragung (intern in der Verlagsfirma und extern bei der Übertragung über das Internet) gesichert werden.

Sichern des Szenarios

In diesem Szenario ruft die interne Webanwendung der einzelnen Partnerfirmen über den Webdienst Daten von der Verlagsfirma ab. Die abgerufenen Daten werden anschließend für die Benutzer zugänglich gemacht. Der Verleger benötigt einen sicheren Mechanismus, um Partnerfirmen zu authentifizieren, während die Identität der einzelnen Benutzer in den Partnerfirmen ohne Belang ist.

Aufgrund der vertraulichen Natur der Daten, die zwischen den beiden Firmen über das Internet gesendet werden, müssen sie bei der Übertragung durch SSL gesichert werden.

Ein Firewall, der nur eingehende Verbindungen von den IP-Adressen der Partnerfirmen im Extranet zulässt, hindert nicht berechtigte Internetbenutzer daran, Netzwerkverbindungen zum Webdienstserver herzustellen.

Tabelle 6.1: *Sicherheitsmaßnahmen*

Kategorie	Details
Authentifizierung	● Die Partneranwendungen verwenden bei jeder Anforderung an den Webdienst Clientzertifikate. ● Die Clientzertifikate der Partnerfirmen sind einzelnen Active Directory-Konten zugeordnet. ● In der Datenbank wird die Windows®-Authentifizierung verwendet. Für die Verbindung wird die Prozessidentität des ASP.NET-Webdienstes verwendet. Die Datenbank vertraut dem Webdienst.
Autorisierung	● Der Webdienst verwendet eine .NET-rollenbasierte Autorisierung zur Überprüfung, ob die authentifizierten Active Directory-Konten Mitglied einer Partnergruppe sind.
Sichere Kommunikation	● Zum Sichern der Kommunikation zwischen der Webanwendung bei den Partnern und dem Webdienst des Verlegers wird SSL verwendet. ● Zum Sichern der gesamten Kommunikation zwischen dem Webdienst und der Datenbank wird IPSec verwendet.

Das Ergebnis

Abbildung 6.2 zeigt die empfohlene Sicherheitskonfiguration für dieses Szenario.

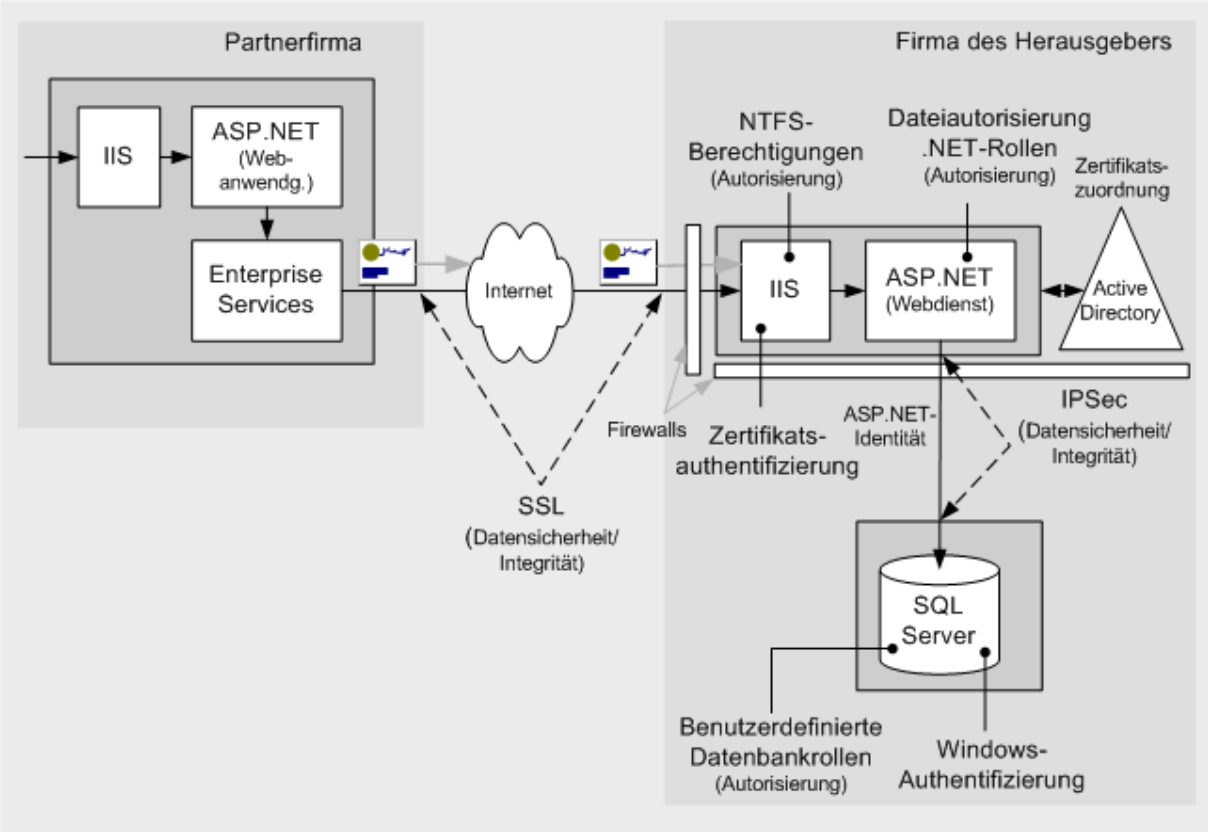

Abbildung 6.2
Webdienst für den Datenaustausch zwischen B2B-Partnern - Empfohlene Sicherheitskonfiguration

Konfigurationsschritte für die Sicherheit

Bevor Sie beginnen, sollten Sie sich über folgende Themen informieren:

- Erstellen benutzerdefinierter ASP.NET-Konten (siehe "Vorgehensweise: Erstellen eines benutzerdefinierten Kontos zum Ausführen von ASP.NET" im Abschnitt "Referenz" dieses Handbuchs)
- Erstellen eines Datenbankkontos mit möglichst geringen Rechten (siehe Kapitel 12, "Datenzugriffssicherheit")
- Konfigurieren von SSL auf einem Webserver (siehe "Vorgehensweise: Einrichten von SSL auf einem Webserver" im Abschnitt "Referenz" dieses Handbuchs)
- Konfigurieren von IPSec (siehe "Vorgehensweise: Verwenden von IPSec zum Sichern der Kommunikation zwischen zwei Servern" im Abschnitt "Referenz" dieses Handbuchs)
- Konfigurieren von IPSec durch Firewalls (siehe Artikel Q233256, "How to Enable IPSec Traffic Through a Firewall" (US) in der Microsoft® Knowledge Base).
- Aufrufen eines Webdienstes mit SSL (siehe "Vorgehensweise: Aufrufen eines Webdienstes unter Verwendung von SSL" im Abschnitt "Referenz" dieses Handbuchs – diese Lösungstechnik wird in der Partnerfirma benötigt)
- Die Erklärung der Zertifikatsverwaltung und der Infrastruktur würde den Rahmen dieses Themas sprengen. Weitere Informationen erhalten Sie in Microsoft TechNet unter "Certificates and Authenticode" (US).

Konfigurieren der Partneranwendung

In diesem Kapitel werden keine Einzelheiten der Partneranwendung und deren Sicherheitskonfiguration behandelt. Allerdings müssen die folgenden Punkte berücksichtigt werden, um die Kommunikation zwischen der Partneranwendung und dem Webdienst zu vereinfachen:

- Die Webanwendung der Partnerfirma kann einen Authentifizierungsmechanismus auswählen, der die Authentifizierung und Autorisierung der internen Benutzer ermöglicht. Diese Benutzer werden nicht zur weiteren Authentifizierung an den Webdienst übertragen.
- Die Webanwendung der Partnerfirma führt die Aufrufe an den Webdienst im Namen der Benutzer durch. Die Benutzer können den Webdienst nicht direkt aufrufen.
- Die Webanwendung der Partnerfirma verwenden ein Clientzertifikat, um ihre Identität gegenüber dem Webdienst zu beweisen.
- Falls es sich bei der Partneranwendung um eine ASP.NET-Webanwendung handelt, muss eine zwischengelagerte prozessexterne Komponente (eine Enterprise Services-Anwendung oder ein Windows-Dienst) verwendet werden, um das Zertifikat zu laden und es an den Webdienst weiterzuleiten.

  Weitere Informationen zu den Gründen dafür und den entsprechenden Schritte für eine Umsetzung finden Sie unter "Vorgehensweise: Aufrufen eines Webdienstes mit Clientzertifikaten von ASP.NET" im Abschnitt "Referenz" dieses Handbuchs.

Konfigurieren des Extranetwebservers

Konfigurieren von IIS	
Schritt	**Weitere Informationen**
Deaktivieren des anonymen Zugriffs für das virtuelle Stammverzeichnis des Webdienstes	Die IIS-Authentifizierungseinstellungen können Sie mit dem IIS-MMC-Snap-In bearbeiten. Klicken Sie mit der rechten Maustaste auf das virtuelle Verzeichnis der Anwendung, und klicken Sie dann auf **Eigenschaften**. Klicken Sie auf die Registerkarte **Verzeichnissicherheit** und dann im Gruppenfeld **Authentifizierung und Zugriffssteuerung** auf **Bearbeiten**.
Aktivieren der Zertifikatsauthentifizierung für das virtuelle Stammverzeichnis der Webanwendung und des Webdienstes	Siehe "Vorgehensweise: Einrichten von SSL auf einem Webserver" im Abschnitt "Referenz" dieses Handbuchs. Siehe "Vorgehensweise: Aufrufen eines Webdienstes mit Clientzertifikaten von ASP.NET" im Abschnitt "Referenz" dieses Handbuchs.
Konfigurieren von Active Directory (Extranet)	
Schritt	**Weitere Informationen**
Einrichten von Active Directory-Konten zur Darstellung der Partnerfirmen	Für das Extranet wird ein getrenntes Active Directory verwendet, das sich in einer eigenen Gesamtstruktur befindet und vom Active Directory der Firma vollkommen getrennt ist.
Konfigurieren der Zertifikatszuordnung	Siehe "Step-by-Step Guide to Mapping Certificates to User Accounts" (nur auf Englisch verfügbar) in Microsoft TechNet. Entsprechende Informationen finden Sie auch im Artikel Q313070, "HOW TO: Configure Client Certificate Mappings in IIS 5.0" (US) in der Microsoft Knowledge Base.

Konfigurieren von ASP.NET (Webdienst)	
Schritt	Weitere Informationen
Konfigurieren des ASP.NET-Webdienstes für die Windows-Authentifizierung	Bearbeiten Sie **Web.config** im virtuellen Stammverzeichnis des Webdienstes. Legen Sie das <**authentication**>-Element fest auf: `<authentication mode="Windows" />`

Zurücksetzen des Kennworts des Kontos **ASPNET** (unter dem ASP.NET ausgeführt wird) auf ein bekanntes starkes Kennwort	Dadurch können Sie ein doppeltes lokales Konto (mit demselben Benutzernamen und demselben Kennwort) auf dem Datenbankserver erstellen. Dies ist erforderlich, damit das Konto **ASPNET** Authentifizierungsanforderungen des Datenbankservers über das Netzwerk beantworten kann, wenn die Verbindung mit der Windows-Authentifizierung hergestellt wird.
	
	Als Alternative kann hier ein Domänenkonto mit möglichst geringen Rechten verwendet werden (falls eine Windows-Authentifizierung durch den Firewall zulässig ist).
	Weitere Informationen finden Sie unter "Prozessidentität für ASP.NET" in Kapitel 8, "ASP.NET-Sicherheit".
	
	Bearbeiten Sie **Machine.config** in **%windir%\Microsoft.NET\Framework\v1.0.3705\CONFIG**.
	
	Legen Sie die Attribute für den Benutzernamen und das Kennwort des benutzerdefinierten Kontos im <**processModel**>-Element fest.
	
	Die Standardeinstellung
	
	`<!-- userName="machine" password="AutoGenerate" -->`
	
	wird geändert in
	
	`<!-- userName="machine"`
	`password="YourStrongPassword" -->`

Konfigurieren von SQL Server

Schritt	Weitere Informationen
Erstellen eines Windows-Kontos auf dem Computer mit Microsoft SQL Server™, das dem ASP.NET-Prozesskonto entspricht, mit dem der Webdienst ausgeführt wird (standardmäßig **ASPNET**)	Benutzername und Kennwort müssen mit dem ASP.NET-Prozesskonto übereinstimmen. Erteilen Sie dem Konto die folgenden Rechte: - Auf diesen Computer vom Netzwerk aus zugreifen - Lokale Anmeldung verweigern - Anmelden als Stapelverarbeitungsauftrag
Konfigurieren von SQL Server für die Windows-Authentifizierung	

Erstelen eines SQL Server-Benutzernamens für das Konto **ASPNET**	Dadurch wird der Zugriff auf SQL Server gewährt.
Erstellen eines neuen Datenbankbenutzers und Zuordnen des Benutzernamens zum Datenbankbenutzer	Dadurch wird der Zugriff auf die angegebene Datenbank gewährt.
Erstellen einer neuen benutzerdefinierten Datenbankrolle in der Datenbank und Einfügen des Datenbankbenutzers in die Rolle	
Einrichten der Datenbankberechtigungen für die Datenbankrolle	Gewähren Sie minimale Rechte. Siehe Kapitel 12, "Datenzugriffssicherheit".

Konfigurieren der sicheren Kommunikation

Schritt	Weitere Informationen
Konfigurieren der Website auf dem Webserver für SSL	Siehe "Vorgehensweise: Einrichten von SSL auf einem Webserver" im Abschnitt "Referenz" dieses Handbuchs.
Konfigurieren von IPSec zwischen Webserver und Datenbankserver	Siehe "Vorgehensweise: Verwenden von IPSec zum Sichern der Kommunikation zwischen zwei Servern" im Abschnitt "Referenz" dieses Handbuchs.

Analyse

- ASP.NET wird auf dem Webserver als lokales Konto mit möglichst geringen Rechten (dem Standardkonto **ASPNET**) ausgeführt, sodass ein mögliches Risiko einer Offenlegung gemindert wird.
- Die ASP.NET-Webanwendungen in den Partnerfirmen verwenden die integrierte Windows-Authentifizierung und führen eine Autorisierung durch, um die berechtigten Benutzer für den Zugriff auf den Webdienst zu ermitteln.
- Die ASP.NET-Webanwendung in der Partnerfirma verwendet eine zwischengelagerte Enterprise Services-Anwendung, um die Clientzertifikate abzurufen und Aufrufe an den Webdienst auszuführen.
- Die Verlagsfirma verwendet den Namen der Partnerorganisation (der im Zertifikat enthalten ist), um die Zertifikatszuordnung in IIS durchzuführen.
- Der Webdienst verwendet das zugeordnete Active Directory-Konto, um die Autorisierung mithilfe von **PrincipalPermission**-Forderungen und .NET-Rollenprüfungen durchzuführen.
- Durch die Windows-Authentifizierung gegenüber SQL Server wird das Speichern der Anmeldeinformationen auf dem Webserver sowie das Senden der Anmeldeinformationen über das interne Netzwerk an den SQL Server-Computer vermieden. Wenn die SQL-Authentifizierung verwendet wird, muss die Verbindungszeichenfolge (die einen Benutzernamen und ein Kennwort enthält) in der Anwendung und bei der Übertragung über das Netzwerk gesichert werden. Verwenden Sie DPAPI oder eine der alternativen sicheren Speicherstrategie, die in Kapitel 12, “Datenzugriffssicherheit”, behandelt werden, um die Verbindungszeichenfolgen zu speichern, und schützen Sie die Verbindungszeichenfolge (sowie vertrauliche Anwendungsdaten) bei der Übertragung zwischen dem Webdienst und der Datenbank mit IPSec.

- SSL zwischen Partnerfirma und Webdienst schützt die über das Internet übertragenen Daten.
- IPSec zwischen Webdienst und Datenbank schützt die im Firmennetzwerk von und zu der Datenbank übertragenen Daten. In einigen Szenarien, in denen Partner und Verleger über ein privates Netzwerk kommunizieren, kann IPSec zusätzlich zur sicheren Kommunikation eventuell auch für die Computerauthentifizierung verwendet werden.

Fallstricke

- Die Verwendung eines duplizierten lokalen Windows-Kontos im Datenbankserver (das mit dem IIS-lokalen ASP.NET-Prozesskonto übereinstimmt) führt zu einem geringeren Verwaltungsaufwand. Die Kennwörter sollten regelmäßig von Hand aktualisiert und synchronisiert werden.
- Da die .NET-rollenbasierte Sicherheit auf der Windows-Gruppenmitgliedschaft basiert, wird bei dieser Lösung vorausgesetzt, dass die Windows-Gruppen entsprechend den Kategorien der Benutzer (mit gleichen Sicherheitsrechten), die auf die Anwendung zugreifen, feinstufig genug eingerichtet sind. In diesem Szenario müssen Active Directory-Konten Mitglied einer Partnergruppe sein.

Fragen und Antworten

- **Die Datenbank kennt den ursprünglichen Aufrufer nicht. Wie kann eine Überwachungsliste erstellt werden?**
  Überwachen Sie die Aktivitäten der Endbenutzer (Partnerfirma) im Webdienst. Übergeben Sie die Identität der Partnerfirma auf Anwendungsebene mithilfe von Parametern gespeicherter Prozeduren an die Datenbank.

Verwandte Szenarien

Die Verlagsfirma veröffentlicht möglicherweise nicht vertrauliche Daten, wie z. B. Softkopien von Zeitschriften, Zeitungen usw. In diesem Szenario kann der Verleger einen eindeutigen Benutzernamen und ein Kennwort bereitstellen, damit die einzelnen Partner eine Verbindung herstellen und die Daten vom Webdienst abrufen können.

In diesem verwandten Szenario ist die Website des Verlegers so konfiguriert, dass die Benutzer anhand der Standardauthentifizierung authentifiziert werden. Die Partneranwendung verwendet Benutzername und Kennwort, um die Anmeldeinformationen für den Webdienstproxy explizit festzulegen.

Weitere Informationen

Weitere Informationen zum Konfigurieren von Webdienstproxys finden Sie in Kapitel 10, "Webdienstsicherheit".

Bereitstellen einer Webanwendung

In diesem Szenario gewährt die Verlegerfirma ihren Partnern exklusiven Zugriff über das Internet auf ihre Anwendung. Sie stellt eine Partnerportalanwendung bereit, um beispielsweise Dienste zu verkaufen, Partner laufend mit aktuellen Informationen zu Produkten zu versorgen, eine Onlinezusammenarbeit zu ermöglichen usw. (siehe Abbildung 6.3).

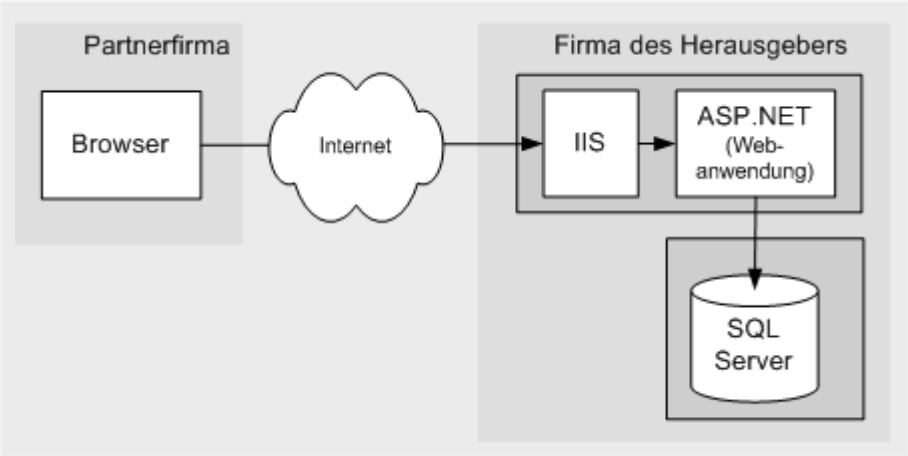

Abbildung 6.3
Szenario mit Partnerportal

Merkmale des Szenarios

Dieses Szenario weist die folgenden Merkmale auf:

- Die Partnerwebanwendung übernimmt die Anmeldeinformationen entweder mithilfe einer Formularanmeldeseite oder stellt in IIS einen Anmeldedialog das, der die Standardauthentifizierung verwendet.
- Die Anmeldeinformationen werden anhand eines getrennten Active Directory im Perimeternetzwerk (auch DMZ, demilitarisierte Zone und abgeschirmtes Subnetz genannt) des Extranets überprüft. Das Active Directory des Extranets befindet sich in einer getrennten Gesamtstruktur, die eine getrennte Vertrauensgrenze bereitstellt.
- Der Zugriff auf die Datenbank erfolgt über eine einzige vertrauenswürdige Verbindung, die der Prozessidentität der ASP.NET-Webanwendung entspricht.
- Die Autorisierung der Webanwendung basiert auf einem **GenericPrincipal**-Objekt (das bei dem Vorgang der Formularauthentifizierung erstellt wird) bzw. einem **WindowsPrincipal**-Objekt (wenn die Standardauthentifizierung verwendet wird).
- Die von der Webanwendung abgerufenen Daten sind vertraulich und müssen bei der Übertragung (intern in der Verlagsfirma und extern bei der Übertragung über das Internet) gesichert werden.

Sichern des Szenarios

Aufgrund der vertraulichen Natur der Daten, die zwischen den beiden Firmen über das Internet gesendet werden, müssen sie bei der Übertragung durch SSL gesichert werden.

Ein Firewall, der nur eingehende Verbindungen von den IP-Adressen der Partnerfirmen im Extranet zulässt, hindert nicht berechtigte Internetbenutzer daran, Netzwerkverbindungen zum Webserver zu öffnen.

Tabelle 6.2: *Sicherheitsmaßnahmen*

Kategorie	Details
Authentifizierung	• Die Benutzer in den Partnerfirmen werden von der Webanwendung entweder mit der Standardauthentifizierung oder der Formularauthentifizierung gegenüber dem Active Directory des Extranets authentifiziert. • In der Datenbank wird die Windows-Authentifizierung verwendet. Für die Verbindung wird die Prozessidentität der ASP.NET-Webanwendung verwendet. Die Datenbank vertraut der Webanwendung.
Autorisierung	• Die Webanwendung verwendet eine .NET-rollenbasierte Autorisierung zur Überprüfung, ob der authentifizierte Benutzer (der bei der Formularauthentifizierung durch ein **GenericPrincipal**-Objekt bzw. bei der Standardauthentifizierung durch ein **WindowsPrincipal**-Objekt dargestellt wird) zu einer Partnergruppe gehört.
Sichere Kommunikation	• Zum Sichern der Kommunikation zwischen dem Webbrowser bei den Partnern und der Webanwendung des Verlegers wird SSL verwendet. • Zum Sichern der gesamten Kommunikation zwischen der Webanwendung und der Datenbank wird IPSec verwendet.

Das Ergebnis

Abbildung 6.4 zeigt die empfohlene Sicherheitskonfiguration für dieses Szenario.

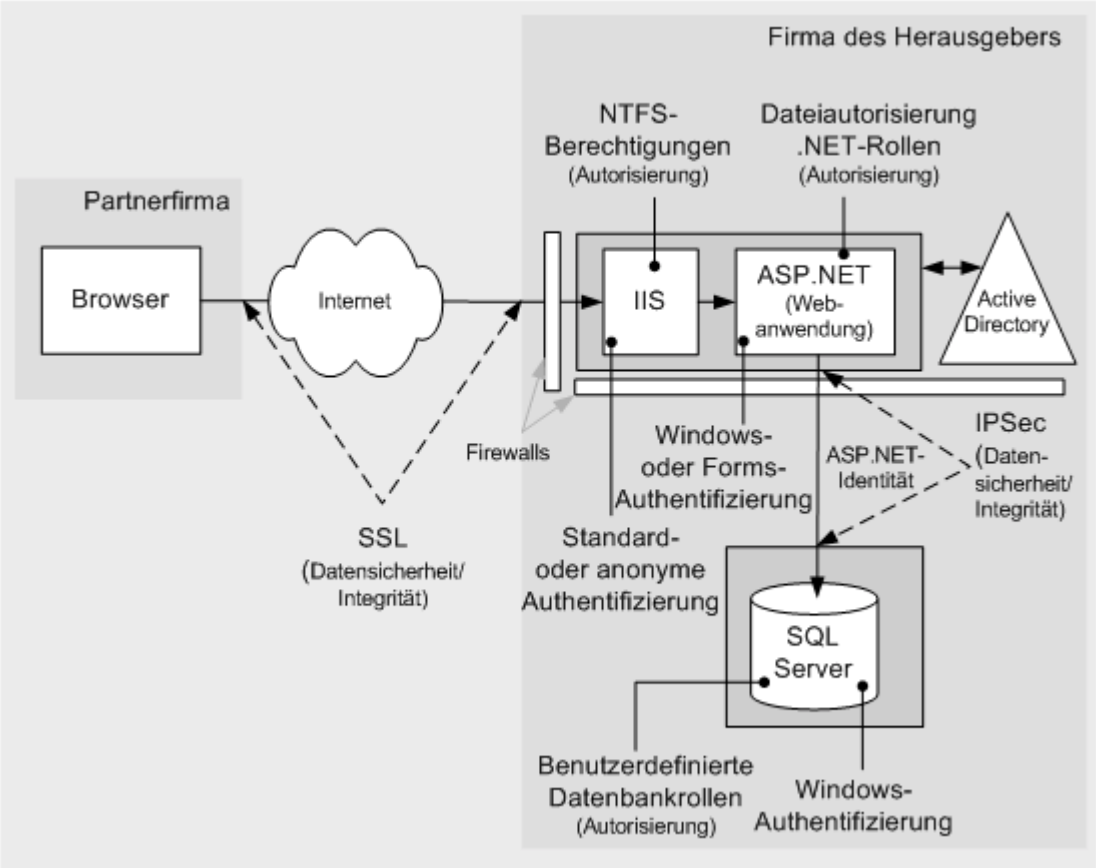

Abbildung 6.4
Empfohlene Sicherheitskonfiguration für das Partnerportalszenario

Konfigurieren des Extranetwebservers

Konfigurieren von IIS	
Schritt	**Weitere Informationen**
Aktivieren des anonymen Zugriffs für das virtuelle Stammverzeichnis der Webanwendung, wenn die Formularauthentifizierung verwendet werden soll – oder – Deaktivieren des anonymen Zugriffs und Auswählen der Standardauthentifizierung, wenn die Standardauthentifizierung verwendet werden soll	

Konfigurieren von Active Directory (Extranet)	
Schritt	**Weitere Informationen**
Einrichten von Active Directory-Konten zur Darstellung der Partnerbenutzer	Für das Extranet wird ein getrenntes Active Directory verwendet, das sich in einer eigenen Gesamtstruktur befindet und vom Active Directory der Firma vollkommen getrennt ist.

Konfigurieren von ASP.NET	
Schritt	**Weitere Informationen**

Konfigurieren der ASP.NET-Webanwendung, sodass die Windows-Authentifizierung (für IIS: Standardauthentifizierung) verwendet wird
– oder –
Konfigurieren von ASP.NET, sodass die Formularauthentifizierung verwendet wird
	Bearbeiten Sie **Web.config** im virtuellen Stammverzeichnis des Webdienstes.
	Legen Sie das <**authentication**>-Element fest auf:
	`<authentication mode="Windows" />`
	– oder –
	`<authentication mode="Forms" />`

Zurücksetzen des Kennworts des Kontos **ASPNET** (unter dem ASP.NET ausgeführt wird) auf ein bekanntes starkes Kennwort	Dadurch können Sie ein doppeltes lokales Konto (mit demselben Benutzernamen und demselben Kennwort) auf dem Datenbankserver erstellen. Dies ist erforderlich, damit das Konto **ASPNET** Authentifizierungsanforderungen des Datenbankservers über das Netzwerk beantworten kann, wenn die Verbindung mit der Windows-Authentifizierung hergestellt wird. Als Alternative kann hier ein Domänenkonto mit möglichst geringen Rechten verwendet werden (falls eine Windows-Authentifizierung durch den Firewall zulässig ist). Weitere Informationen finden Sie unter "Prozessidentität für ASP.NET" in Kapitel 8, "ASP.NET-Sicherheit". Bearbeiten Sie **Machine.config** in **%windir%\Microsoft.NET\Framework\v1.0.3705\CONFIG**. Legen Sie die Attribute für den Benutzernamen und das Kennwort des benutzerdefinierten Kontos im <**processModel**>-Element fest.

	Die Standardeinstellung
	
	`<!-- userName="machine" password="AutoGenerate" -->`
	
	wird geändert in
	
	`<!-- userName="machine"`
	`password="YourStrongPassword" -->`

Konfigurieren von SQL Server

Schritt	Weitere Informationen
Erstellen eines Windows-Kontos auf dem Computer mit Microsoft SQL Server™, das dem ASP.NET-Prozesskonto entspricht, mit dem der Webdienst ausgeführt wird (standardmäßig **ASPNET**)	Benutzername und Kennwort müssen mit dem ASP.NET-Prozesskonto übereinstimmen. Erteilen Sie dem Konto die folgenden Rechte: - Auf diesen Computer vom Netzwerk aus zugreifen - Lokale Anmeldung verweigern - Anmelden als Stapelverarbeitungsauftrag
Konfigurieren von SQL Server für die Windows-Authentifizierung	
Erstelen eines SQL Server-Benutzernamens für das Konto **ASPNET**	Dadurch wird der Zugriff auf SQL Server gewährt.
Erstellen eines neuen Datenbankbenutzers und Zuordnen des Benutzernamens zum Datenbankbenutzer	Dadurch wird der Zugriff auf die angegebene Datenbank gewährt.
Erstellen einer neuen benutzerdefinierten Datenbankrolle in der Datenbank und Einfügen des Datenbankbenutzers in die Rolle	
Einrichten der Datenbankberechtigungen für die Datenbankrolle	Gewähren Sie minimale Rechte. Siehe Kapitel 12, "Datenzugriffssicherheit".

Konfigurieren der sicheren Kommunikation

Schritt	Weitere Informationen
Konfigurieren der Website auf dem Webserver für SSL	Siehe "Vorgehensweise: Einrichten von SSL auf einem Webserver" im Abschnitt "Referenz" dieses Handbuchs.
Konfigurieren von IPSec zwischen Webserver und Datenbankserver	Siehe "Vorgehensweise: Verwenden von IPSec zum Sichern der Kommunikation zwischen zwei Servern" im Abschnitt "Referenz" dieses Handbuchs.

Analyse

- ASP.NET wird auf dem Webserver als lokales Konto mit möglichst geringen Rechten (dem Standardkonto **ASPNET**) ausgeführt, sodass ein mögliches Risiko einer Offenlegung gemindert wird.
- Zwischen Browser und Webanwendung wird SLL verwendet, um die Anmeldeinformationen für die Formular- oder Standardauthentifizierung zu schützen (die jeweils unverschlüsselt übertragen werden, obwohl bei der Standardauthentifizierung die Base64-Codierung verwendet wird). SSL schützt außerdem die anwendungsspezifischen Daten, die von der Webanwendung zurückgegeben werden.
- Bei der Formularauthentifizierung wird SSL auf allen Seiten verwendet (nicht nur der Anmeldeseite), um das Authentifizierungscookie zu schützen, das nach der ersten Authentifizierung bei allen Webanforderungen übertragen wird.
- Wenn SSL nur auf der ersten Anmeldeseite verwendet wird, um die zur Authentifizierung übergebenen Anmeldeinformationen zu verschlüsseln, sollten Sie sicherstellen, dass das Formularauthentifizierungsticket (das in einem Cookie enthalten ist) geschützt wird, da es bei allen nachfolgenden Webanforderungen zwischen Client und Server übertragen wird. Konfigurieren Sie zum Verschlüsseln des Formularauthentifizierungstickets das **protection**-Attribut des <**forms**>-Elements wie unten gezeigt, und verschlüsseln Sie das Ticket mit der **Encrypt**-Methode der **FormsAuthentication**-Klasse.

```
<authentication mode="Forms">
  <forms name="MyAppFormsAuth"
       loginUrl="login.aspx"
       protection="All"
       timeout="20"
       path="/" >
  </forms>
</authentication>
```

Das **protection="All"**-Attribut gibt an, dass das Ticket überprüft (Integritätsprüfung) und verschlüsselt werden soll, wenn die Anwendung **FormsAuthentication.Encrypt** aufruft. Rufen Sie diese Methode auf, wenn Sie das Authentifizierungsticket erstellen, normalerweise im Ereignishandler für die Anmeldeschaltfläche der Anwendung.

```
string encryptedTicket = FormsAuthentication.Encrypt(authTicket);
```

Weitere Informationen zur Formularauthentifizierung und Ticketverschlüsselung finden Sie in Kapitel 8, "ASP.NET-Sicherheit".

- Gleicherweise wird SSL bei der Standardauthentifizierung auf allen Seiten verwendet, da die Anmeldeinformationen der Standardauthentifizierung bei allen Anforderungen von Webseiten übertragen werden und nicht nur bei der ersten Anforderung, bei der die Anmeldeinformationen der Standardauthentifizierung vom Benutzer eingegeben werden.
- Bei der Standardauthentifizierung erstellt ASP.NET automatisch ein **WindowsPrincipal**-Objekt, das den authentifizierten Benutzer darstellt, und ordnet es der aktuellen Webanforderung zu (**HttpContext.User**), bei der es von der .NET-Autorisierung sowie **PrincipalPermission**-Forderungen und .NET-Rollen verwendet wird.
- Bei der Formularauthentifizierung müssen Sie Code entwickeln, um die bereitgestellten Anmeldeinformationen anhand Active Directory zu überprüfen, und ein **GenericPrincipal**-Objekt erstellen, das den authentifizierten Benutzer darstellt.

- Durch die Windows-Authentifizierung gegenüber SQL Server wird das Speichern der Anmeldeinformationen auf dem Webserver sowie das Senden der Anmeldeinformationen über das interne Netzwerk an den SQL Server-Computer vermieden.
- IPSec zwischen Webdienst und Datenbank schützt die im Firmennetzwerk von und zu der Datenbank übertragenen Daten.

Fallstricke

- Die Verwendung eines duplizierten lokalen Windows-Kontos im Datenbankserver (das mit dem IIS-lokalen ASP.NET-Prozesskonto übereinstimmt) führt zu einem gesteigerten Verwaltungsaufwand. Die Kennwörter sollten regelmäßig von Hand aktualisiert und synchronisiert werden.
- Bei der Standardauthentifizierung wird im Browser ein Popup-Dialogfeld angezeigt. Verwenden Sie die Formularauthentifizierung, um eine reibungslosere Anmeldung zu ermöglichen.

Verwandte Szenarien

Keine Verbindung vom Extranet zum Firmennetzwerk

Um eine höhere Sicherheit zu erreichen, kann die Extranetanwendung so aufgebaut werden, dass keine Verbindung zurück zum Firmennetzwerk erforderlich ist. In diesem Szenario gilt:

- Im Extranet befindet sich eine separate SQL Server-Datenbank, und die Daten werden von der internen Datenbank in die Extranetdatenbank repliziert.
- Mithilfe von Routern werden Verbindungen vom Extranet zum Firmennetzwerk zurückgewiesen. Verbindungen in die andere Richtung können mithilfe von speziellen Ports im hohen Bereich hergestellt werden.
- Verbindungen vom Firmennetzwerk zum Extranet sollten immer über einen dedizierten Server mit einer strengen Überwachung und Protokollierung durchgeführt werden, über den sich die Benutzer vor dem Zugriff auf das Extranet authentifizieren müssen.

Weitere Informationen

- Weitere Informationen finden Sie in den folgenden Microsoft TechNet-Artikeln:
  - "Extending Your Network to Business Partners" (nur auf Englisch verfügbar)
  - "Deploying SharePoint Portal Server in an Extranet Environment" (nur auf Englisch verfügbar)
- Weitere Informationen zum Verwenden der Formularauthentifizierung mit Active Directory finden Sie unter "Vorgehensweise: Verwenden der Formularauthentifizierung mit Active Directory" im Abschnitt "Referenz" dieses Handbuchs.

Zusammenfassung

In diesem Kapitel wird beschrieben, wie zwei häufige Extranetanwendungsszenarien gesichert werden.

Informationen bezüglich Intranet- und Internetanwendungsszenarien finden Sie in Kapitel 5, "Intranetsicherheit", und Kapitel 7, "Internetsicherheit".