Erstellen sicherer ASP.NET-Anwendungen

Wegweiser

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

Microsoft Corporation

Oktober 2002

Zusammenfassung

In diesem Handbuch finden Sie einen praktischen, szenariogesteuerten Ansatz zum Entwerfen und Erstellen sicherer ASP.NET-Anwendungen für Windows 2000 und der Version 1.0 des .NET Frameworks. Es konzentriert sich dabei auf die Hauptelemente der Authentifizierung, Autorisierung und der sicheren Kommunikation auf und über Ebenen verteilter .NET-Webanwendungen.

Anwendungsbereiche

Die Informationen in diesem Handbuch gelten für Folgendes:

- .NET Framework, Version 1.0
- ASP.NET
- Enterprise Services
- Webdienste
- .NET Remoting
- ADO.NET
- Visual Studio .NET, Version 1.0
- SQL Server
- Windows 2000

Die im Handbuch enthaltenen Empfehlungen und Beispielcodes wurden mit Visual Studio .NET, Version 1.0, erstellt und getestet und auf Servern überprüft, auf denen Windows 2000 Advanced Server SP 3, .NET Framework SP 2 und SQL Server 2000 SP 2 ausgeführt wurde.

Inhalt dieses Handbuchs

Der Inhalt dieses Handbuchs konzentriert sich auf die folgenden Themen:

- Authentifizierung (zum Identifizieren der Clients der Anwendung)
- Autorisierung (zum Bereitstellen der Zugriffssteuerung für diese Clients)
- Sichere Kommunikation (zum Sicherstellen, dass Nachrichten vertraulich bleiben und nicht durch unberechtigte Teilnehmer verändert werden)

Warum Authentifizierung, Autorisierung und sichere Kommunikation?

Sicherheit ist ein weites Thema. Durch Forschungen wurde belegt, dass durch den frühen Entwurf von Authentifizierung und Autorisierung ein hoher Prozentsatz der Verwundbarkeit von Anwendungen beseitigt wird. Die sichere Kommunikation ist ein integraler Bestandteil der Sicherung verteilter Anwendungen zum Schutz vertraulicher Daten, wie z. B. Anmeldeinformationen, die von und zu der Anwendung sowie zwischen den Anwendungsebenen übertragen werden.

Zum Erstellen von .NET-Webanwendungen stehen viele Verfahren zur Verfügung. Damit Sie effektive Authentifizierungs- und Autorisierungsstrategien auf Anwendungsebene erstellen können, müssen Sie wissen, wie die verschiedenen Sicherheitsfunktionen in den einzelnen Produkten und in jedem Technologiebereich optimiert werden und wie diese zusammenarbeiten können, um eine effektive, tief greifende Sicherheitsstrategie bereitzustellen. Dieses Handbuch unterstützt Sie bei diesem Vorhaben.

In Abbildung 1 werden die im Handbuch beschriebenen verschiedenen Technologien zusammengefasst.

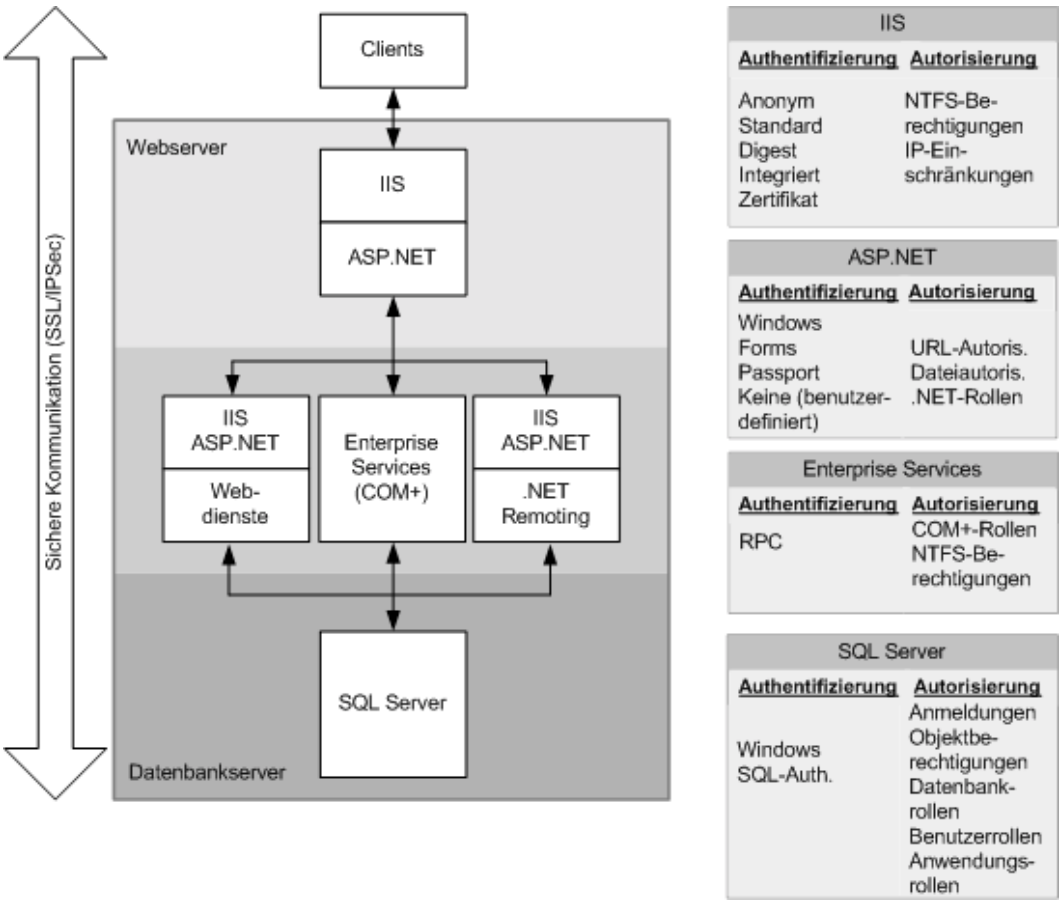

Abbildung 1
.NET Web-Anwendungssicherheit

Dieses Handbuch ist in vier Teile unterteilt. Ziel ist eine logische Aufteilung, damit Sie die Inhalte leichter auswählen können.

Teil I, Sicherheitsmodelle

In Teil I des Handbuchs werden die Grundlagen für den Rest des Handbuchs gelegt. Wenn Sie mit den Konzepten, Grundsätzen und Technologien vertraut sind, die in Teil I vorgestellt werden, können Sie aus dem Rest des Handbuchs maximalen Nutzen ziehen. Teil I enthält die folgenden Kapitel:

- **Kapitel 1 – Einführung**
  In diesem Kapitel werden die Ziele dieses Handbuchs erläutert, die grundelegende Terminologie vorgestellt und mehrere wichtige Richtlinien beschrieben, die für die in den späteren Kapiteln dargestellten Informationen gelten.
- **Kapitel 2 – Sicherheitsmodell für ASP.NET-Anwendungen**
  Dieses Kapitel beschreibt die allgemeinen Merkmale von .NET-Webanwendungen im Hinblick auf die Sicherheit und stellt das Sicherheitsmodell von .NET-Webanwendungen vor. Darüber hinaus werden die Kernimplementierungstechnologien vorgestellt, mit denen sichere .NET-Webanwendungen erstellt werden.
- **Kapitel 3 – Authentifizierung und Autorisierung**
  Der Entwurf einer zusammenhängenden Authentifizierungs- und Autorisierungsstrategie in allen Ebenen der Anwendung bildet eine anspruchsvolle Aufgabe. Dieses Kapitel enthält hilfreiche Informationen für die Entwicklung einer geeigneten Strategie für das jeweilige Anwendungsszenario. Sie erhalten Hilfestellungen bei der Auswahl der geeignetesten Authentifizierungs- und Autorisierungstechnik und der Anwendung dieser Technik an den richtigen Stellen in der Anwendung.
- **Kapitel 4 – Sichere Kommunikation**
  In diesem Kapitel werden die beiden Kerntechnologien vorgestellt, mit denen die Vertraulichkeit und Integrität von Datennachrichten bereitgestellt wird, die im Netzwerk zwischen den Clients und Servern im Internet und im Firmenintranet übertragen werden: SSL und IPSec. Darüber hinaus wird die RPC-Verschlüsselung erläutert, mit der die Kommunikation mit Remote-Serviced Components gesichert werden kann.

Teil II, Anwendungsszenarien

Die meisten Anwendungen können als Intranet-, Extranet- oder Internetanwendungen kategorisiert werden. Dieser Teil des Handbuchs stellt einige gebräuchliche Anwendungsszenarien da, die jeweils in diese Kategorien fallen. Die Schlüsselmerkmale der einzelnen Szenarien werden beschrieben, und die möglichen Sicherheitsrisiken werden analysiert.

Anschließend wird das Konfigurieren und Implementieren der geeignetesten Strategie für Authentifizierung, Autorisierung und sichere Kommunikation im jeweiligen Anwendungsszenario gezeigt.

- **Kapitel 5 – Intranetsicherheit**
  In diesem Kapitel wird beschrieben, wie häufige Intranetanwendungsszenarien gesichert werden.
- **Kapitel 6 – Extranetsicherheit**
  In diesem Kapitel wird beschrieben, wie häufige Extranetanwendungsszenarien gesichert werden.
- **Kapitel 7 – Internetsicherheit**
  In diesem Kapitel wird beschrieben, wie häufige Internetanwendungsszenarien gesichert werden.

Teil III, Sichern der Ebenen

Dieser Teil des Handbuchs enthält detaillierte Informationen in Bezug auf die einzelnen Ebenen und Technologien sicherer .NET-Webanwendungen. Teil III enthält die folgenden Kapitel:

- **Kapitel 8 – ASP.NET-Sicherheit**
  Dieses Kapitel enthält Empfehlungen für eine tiefreichende Sicherheit von ASP.NET-Webanwendungen. Es wird beschrieben, wie die Formular- und Windows-Authentifizierung implementiert und die Autorisierung mithilfe verschiedener von ASP.NET unterstützter Gatekeeper durchgeführt wird. Unter anderem wird auch beschrieben, wie vertrauliche Daten gespeichert, die richtige Prozessidentität verwendet und wie auf Netzwerkressourcen unter Verwendung der Windows-Authentifizierung zugegriffen wird, z. B. auf Remotedatenbanken.
- **Kapitel 9 – Enterprise Services-Sicherheit**
  In diesem Kapitel wird erläutert, wie die Geschäftsfunktionalität in Service Components innerhalb von Enterprise Services-Anwendungen gesichert wird. Es wird gezeigt, wie und wann die Enterprise Services (COM+)-Rollen für die Autorisierung verwendet und wie die RPC-Authentifizierung und der Identitätswechsel konfiguriert werden. Des Weiteren wird beschrieben, wie Serviced Components über eine ASP.NET-Webanwendung sicher aufgerufen und wie der Sicherheitskontext des ursprünglichen Aufrufers über eine Serviced Component der mittleren Ebene identifiziert und übermittelt wird.
- **Kapitel 10 – Webdienstsicherheit**
  In diesem Kapitel wird hauptsächlich die Sicherheit auf Plattformebene für Webdienste unter Verwendung der zugrunde liegenden Features von IIS und ASP.NET behandelt. Für die Sicherheit auf Nachrichtenebene entwickelt Microsoft das Web Services Development Kit, mit dem Sie sichere Lösungen erstellen können, die die WS-Security-Spezifikation, ein Bestandteil der GXA-Initiative (Global XML Architecture), erfüllen.
- **Kapitel 11 – .NET Remoting-Sicherheit**
  Das .NET Framework stellt eine Remoteinfrastruktur bereit, die Clients die Kommunikation mit Objekten ermöglicht, die sich in Remoteanwendungsdomänen und -prozessen oder auf Remotecomputern befinden. In diesem Kapitel wird gezeigt, wie sichere .NET Remoting-Lösungen implementiert werden.
- **Kapitel 12 – Datenzugriffssicherheit**
  In diesem Kapitel werden Empfehlungen und Anleitungen behandelt, die beim Entwickeln einer sicheren Datenzugriffsstrategie hilfreich sind. Die behandelten Themen umfassen die Verwendung der Windows-Authentifizierung von ASP.NET für Datenbanken, das Sichern von Verbindungszeichenfolgen, das sichere Speichern von Anmeldeinformationen in einer Datenbank, das Schützen vor SQL Injection-Angriffen sowie das Verwenden von Datenbankrollen.

Teil IV, Referenz

Dieser Referenzteil des Handbuchs beinhaltet ergänzende Informationen, die Ihnen beim besseren Verstehen der Techniken, Strategien und Sicherheitslösungen helfen, die in den vorangehenden Kapiteln erläutert wurden.

- **Kapitel 13 – Problembehandlung bei der Sicherheit**
  In diesem Kapitel werden eine Reihe von Tipps zur Problembehandlung sowie Verfahren und Tools erläutert, die bei der Diagnose von sicherheitsbezogenen Themen hilfreich sind.
- **Vorgehensweisen**
  In diesem Abschnitt sind eine Reihe von Artikeln zur schrittweisen Vorgehensweise enthalten, die Sie durch viele, in vorherigen Kapiteln beschriebene Lösungsverfahren führen.
- **Grundkonfiguration**
  In diesem Abschnitt wird die während der Entwicklung und dem Test für dieses Handbuch verwendete Hardware und Software aufgeführt.
- **Konfigurationsspeicher und -tools**
  In diesem Abschnitt sind die von verschiedenen Authentifizierungs-, Autorisierungs- und sicheren Kommunikationsdiensten verwendeten Konfigurationsspeicher zusammengefasst und die zugehörigen Wartungstools aufgeführt.
- **Referenzliste**
  Dieser Abschnitt bietet eine Reihe von Hyperlinks zu hilfreichen Artikeln und Websites, die zusätzliche Hintergrundinformationen zu den im Handbuch erläuterten Hauptthemen bereitstellen.
- **Die technischen Grundlagen**
  In diesem Abschnitt werden ergänzende Informationen bereitgestellt, die ausführlich beschreiben, wie bestimmte Technologien funktionieren.
- **ASP.NET-Identitätsmatrix**
  In diesem Abschnitt werden die für ASP.NET-Webanwendungen, Webdienste und Remotekomponenten verfügbaren Variablen (mit Beispielen) zusammengefasst, die in ASP.NET verwaltet werden und Informationen über den Aufrufer, den Thread sowie die Prozessebenenidentität bereitstellen.
- **Kryptographie und Zertifikate**
  In diesem Abschnitt sind ergänzende Hintergrundinformationen zur Kryptographie und zu Zertifikaten enthalten.
- **ASP.NET-Sicherheitsmodell**
  Dieser Abschnitt bietet ein Diagramm, das die Authentifizierungs-, Autorisierungs- und sicheren Kommunikationsdienste darstellt, die über die verschiedenen Ebenen einer ASP.NET-Anwendung hinweg zur Verfügung stehen.
- **Glossar**
  Ein Glossar mit Begriffen zur Sicherheit, die in diesem Handbuch verwendet werden.

Zielgruppe dieses Handbuchs

Wenn Sie Middlewareentwickler oder -architekt sind und planen, .NET-Webanwendungen mithilfe einer oder mehrerer der folgenden Technologien zu erstellen oder wenn Sie sich bereits in einem solchen Erstellungsprozess befinden, sollten Sie dieses Handbuch lesen.

- ASP.NET
- Webdienste
- Enterprise Services
- Remoting
- ADO.NET

Vorbedingungen

Sie sollten bereits mit Verfahren und Technologien der .NET-Entwicklung vertraut sein und gewisse Erfahrungen besitzen, damit Sie dieses Handbuch effektiv zum Entwerfen und Erstellen sicherer .NET-Webanwendungen verwenden können. Sie sollten mit verteilten Anwendungsarchitekturen vertraut sein und Ihr eigenes Anwendungsarchitektur- und Entwicklungsverhalten kennen, wenn Sie bereits .NET-Webanwendungslösungen implementiert haben.

Feedback und Support

Fragen? Anmerkungen? Vorschläge? Senden Sie Ihr Feedback zu diesem Sicherheitshandbuch bitte als E-Mail an secguide@microsoft.com.

Dieses Sicherheitshandbuch ist dazu gedacht, Sie beim Erstellen sicherer, verteilter .NET-Anwendungen zu unterstützen. Der Beispielcode und die Anhaltspunkte werden ohne jegliche Gewährleistung bereitgestellt. Obwohl diese Materialien Tests unterzogen wurden und als stabile Sammlung von Prozeduren und Empfehlungen betrachtet werden können, werden sie nicht wie ein normales Microsoft Produkt unterstützt.

Mitwirkende

Den zahlreichen Mitwirkenden und Rezensenten gilt unserer besonderer Dank:

Manish Prabhu, Jesus Ruiz-Scougall, Jonathan Hawkins and Doug Purdy, Keith Ballinger, Yann Christensen and Alexei Vopilov, Laura Barsan, Greg Fee, Greg Singleton, Sebastian Lange, Tarik Soulami, Erik Olson, Caesar Samsi, Riyaz Pishori, Shannon Pahl, Ron Jacobs, Dave McPherson, Christopher Brown, John Banes, Joel Scambray, Girish Chander, William Zentmayer, Shantanu Sarkar, Carl Nolan, Samuel Melendez, Jacquelyn Schmidt, Steve Busby, Len Cardinal, Monica DeZulueta, Paula Paul, Ed Draper, Sean Finnegan, David Alberto, Kenny Jones, Doug Orange, Alexey Yeltsov, Martin Kohlleppel, Joel Yoker, Nanduri, Ilia Fortunov, Aaron Margosis (MCS), Venkat Chilakala, John Allen, Jeremy Bostron, Martin Petersen-Frey, Karl Westerholm, Jayaprakasam Siddian Thirunavukkarasu, Wade Mascia, Ryan Kivett, Sarath Mallavarapu, Jerry Bryant, Peter Kyte, Philip Teale, Ram Sunkara, Shaun Hayes, Eric Schmidt, Michael Howard, Rich Benack, Carlos Lyons, Ted Kehl, Peter Dampier, Mike Sherrill, Devendra Tiwari, Tavi Siochi, Per Vonge Nielsen, Andrew Mason, Edward Jezierski, Sandy Khaund, Edward Lafferty, Peter M. Clift, John Munyon, Chris Sfanos, Mohammad Al-Sabt, Anandha Murukan (Satyam), Keith Brown (DevelopMentor), Andy Eunson, John Langley (KANA Software), Kurt Dillard, Christof Sprenger, J.K.Meadows, David Alberto, Bernard Chen (Sapient)