Unterrichtseinheit 6:

Netzwerksicherheit mit Hilfe von IPSec

Bei IPSec (Internet Protocol Security) handelt es sich um ein Gerüst offener Standards, um eine sichere, private Kommunikation über IP-Netzwerke (Internetprotokoll) mit Hilfe von kryptographischen Sicherheitsdiensten zu gewährleisten.
IPSec wird benötigt um Computer zu authentifizieren und die Daten zu verschlüsseln.

Anmerkung:
Bislang handelt es sich bei IPSec lediglich um einen Vorschlag und noch nicht um einen Standard.

Häufige Arten von Netzwerkangriffen:

- **Netzwerküberwachung:** durch Verwendung eines Netzwerkmonitors
- **Datenänderung:** während der Übertragung
- **Kennwörter:** stehlen und ändern
- **Adressenspoofing:** Ein Angreifer kann mit Hilfe von speziellen Programmen IP-Pakete erstellen, die scheinbar von gültigen Adressen innerhalb des vertrauten Netzwerkes stammen
- **Anwendungsschicht:** Schwächen im Betriebssystem werden ausgenutzt
- **Man-in-the-Middle:** eine Person erfasst und steuert zwischen den beiden kommunizierenden Computern die Daten aktiv und transparent
- **Denial-of-Service (DoS):** die normale Verwendung von Computern oder Netzwerkressourcen werden versucht zu verhindern

Das Netz muss auf alle Fälle geschützt werden vor:

- Änderungen während der Datenübertragung
- abfangen, anzeigen oder kopieren von Daten
- Zugriff durch unberechtigte Teilnehmer

Untersuchen der Rolle von IPSec in einem Netzwerk

Das Hauptziel von IPSec liegt im Schutz von IP-Paketen. Es basiert auf einem Ende-zu-Ende-Sicherheitsmodell, bei dem der Sender und der Empfänger die einzigen Hosts sind, die über den IPSec-Schutz informiert sein müssen.
Jeder Computer sorgt an seinem Ende für die Sicherheit, wobei davon ausgegangen wird, dass das Medium, über das die Kommunikation erfolgt, nicht sicher ist.
Computer, die Daten lediglich von der Quelle zum Ziel weiterleiten, müssen IPSec nicht unterstützen.

Erweitere Netzwerksicherheit (grober Ablauf):

- Gegenseitige Authentifizierung der Computer vor dem Datenaustausch
- Einrichten einer Sicherheitszone zwischen den beiden Computern
- Verschlüsseln der ausgetauschten Daten

Aktivieren von IPSec

IPSec wird mit Hilfe einer Richtlinienkonfiguration, die in der IP-Sicherheitsrichtlinienverwaltung verwaltet wird, gesteuert.

Anmerkung:
Zur Konfiguration dieser Sicherheitsrichtlinien sind Rechte der Gruppe Administratoren nötig.

Verwalten von IP-Sicherheitsrichtlinien

Durch hinzufügen einer Snap-In IP-Sicherheitsrichtlinienverwaltung zu der Microsoft-Management-Console (MMC) werden diese Richtlinien verwaltet.
Folgende Ebenen können damit verwaltet werden:

Ebenen:

- lokale Computer / Remotecomputer
- eigene Domäne
- fremde Domäne

Nötig sind Administratorrechte auf der betroffenen Ebene!

Verwendung von vordefinierten IP-Sicherheitsrichtlinien

Client: *(nur Antwort)*
(Für Computer, die nicht unbedingt eine sichere Kommunikation erfordern)
Diese Richtlinie ermöglicht es dem Computer, auf Anforderung für gesicherte Kommunikation entsprechend zu reagieren. Die Richtlinie enthält eine Standardantwortregel, die eine Verhandlung mit Computern ermöglicht, die IPSec anfordern.

Server: *(Sicherheit anfordern)*
(Für Computer, die meistens eine sichere Kommunikation benötigen)
Diese Richtlinie ermöglicht es dem Computer unsicheren Datenverkehr anzunehmen. Sie versucht jedoch, weitere Kommunikation zu sichern, indem Sicherheit vom ursprünglichen Sender angefordert wird.

Sicherer Server: *(Sicherheit erforderlich)*
(Für Computer, die immer eine sichere Kommunikation benötigen)
Diese Richtlinie weist unsichere eingehende Übertragungen ab. Der ausgehende Verkehr ist immer sicher.

Aktivieren einer IP-Sicherheitsrichtlinie

*In der IP-Sicherheitsrichtlinienverwaltung auf **IP-Sicherheitsrichtlinien auf lokalem Computer** klicken → im Detailfensterbereich mit der rechten Maustaste auf die zuzuweisende Richtlinie klicken → Zuweisen → OK*

Verwenden von IPSec im Übertragungsmodus

Der Übertragungsmodus (Standardmodus von IPSec) authentifiziert und verschlüsselt Daten, die zwischen zwei beliebigen Computern unter Windows2000 übertragen werden. Er wird folgendermaßen angegeben:
*Öffnen einer Komsole mit dem Snap-In **IP-Sicherheitsrichtlinienverwaltung** → im Detailfensterbereich mit der rechten Maustaste auf die zu ändernde Richtlinie klicken → Eigenschaften → Auf die zu ändernde Regel klicken → Bearbeiten → Tunneleinstellungen → Diese Regel spezifiziert keinen IPSec-Tunnel*

Es existieren zwei Übertragungsarten:

- Übertragungsmodus im gleichen Netzwerk (schlechter)
- Tunnelmodus über einen Router (besser)

Konfigurieren von IPSec für die Sicherheit zwischen Netzwerken

Um eine gesicherte Kommunikation zwischen Remotenetzwerken (über zwei Router) zu erstellen, kann IPSec für den Tunnelmodus konfiguriert werden. Daten zwischen den beiden Enden des Tunnels werden sicher und unabhängig von ihrem Ziel transportiert. Allerdings stellt der Tunnelmodus keine Sicherheit innerhalb der einzelnen Netzwerke bereit.

Verwenden von IPSec im Tunnelmodus

Windows2000 benötigt Routing und RAS, um den Tunnelmodus für IPSec zu implementieren. IPSec benötigt für den Tunnelmodus eine IP-Adresse für jedes Ende des Tunnels. Der IPSec-Tunnel wird folgendermaßen angegeben:
*Öffnen einer Komsole mit dem Snap-In **IP-Sicherheitsrichtlinienverwaltung** → im Detailfensterbereich mit der rechten Maustaste auf die zu ändernde Richtlinie klicken → Eigenschaften → Auf die zu ändernde Regel klicken → Bearbeiten → Tunneleinstellungen → Der Tunnelendpunkt wird durch diese IP-Adresse spezifiziert*

Windows2000 unterstützt zwar mehrere Verbindungen im Tunnelmodus, jedoch nicht mehrere Tunnel gleichzeitig. Jede Tunnelverbindung benötigt eine eigenständige Regel.

Regelkomponenten

Eine Regel besteht aus den folgenden Komponenten:

- Tunnelendpunkt
- Netzwerktyp
    - Alle Netzwerkverbindungen
    - LAN
    - RAS
- Authentifizierungsmethode
    - Windows2000-Standard (Kerberos V5-Protokoll)
    - Verwenden eines Zertifikats von dieser Zertifizierungsstelle
    - Diese Zeichenkette zum Schutz des Schlüsselaustauschs verwenden
- IP-Filterliste
    - All ICMP-Verkehr (ping...)
    - Gesamter IP-Verkehr
- Filteraktion

Standardantwortregel

Ein Computer verwendet diese Regel, um auf Anfragen für eine sichere Kommunikation zu antworten.

Die Standardrichtlinien wird folgendermaßen wieder hergestellt:
*Öffnen einer Komsole mit dem Snap-In **IP-Sicherheitsrichtlinienverwaltung** → im Detailfensterbereich mit der rechten Maustaste auf **IP-Sicherheitsrichtlinien auf lokalem Computer** klicken → Alle Tasks → Standardrichtlinien wiederherstellen → Ja*

Auswählen eines IPSec-Verschlüsselungsschemas

(**DES** – **D**ata **E**ncryption **S**tandard)

- **Authentifizierungsverschlüsselung**
  SHA (**S**ecure **H**ash **A**lgorithm) - 160-Bit-Schlüssel (höherwertig)
  MD5 (**M**essage **D**igest **5**) - 128-Bit-Schlüssel
- **Paketverschlüsselung (Datenverschlüsselung)**
  56-Bit DES - für die meisten exportierten Anwendungen
  40-Bit DES - nicht RFC-kompatibel
  3DES - sicherste Methode durch Verwendung von drei 56-Bit-Schlüssel

Überprüfung einer Zuweisung von IP-Sicherheitsrichtlinien

Mit dem Befehl „PING“ kann Gültigkeit einer Netzwerkverbindung überprüft werden. IPSec blockiert den Befehl PING nicht, wenn die Standardrichtlinien unverändert verwendet werden.

Wichtig:
Werden benutzerdefinierte Richtlinien erstellt, welche nicht ICMP (Internet Control Message Protocol) unterliegen, kann der Befehl PING falsche Ergebnisse anzeigen.

Verwenden der IP-Sicherheitsüberwachung zum Überprüfen der Zuweisung einer Richtlinie

Die IP-Sicherheitsüberwachung wird folgendermaßen gestartet:
Start → Ausführen → ipsecmon <Computername>
Um IPSec zu aktivieren muss eine Richtlinie zugewiesen werden.

Optimieren der IPSec-Leistung

Bevor IPSec im Netzwerk implementiert wird, sollten folgende Leistungsaspekte bedacht werden:

- **Erforderliche Sicherheitsebene:**
  Wird IPSec aktiviert, so erhöhen sich die Prozessorauslastung, der IP-Paketverkehr und die IP-Paketgröße.

Anmerkung:
Einige Hersteller bieten Netzwerkadapter an, welche die IPSec-Verschlüsselungstasks auf dem Netzwerkadapter durchführen. Das Durchführen der IPSec-Verschlüsselung mit Hilfe einer dediziert Hardware kann die Leistung erheblich steigern.

- **Sicherheitsanforderungen des Computers**
- **Anzahl der Einträge für IP-Sicherheitsrichtlinienfilter**

Konfigurieren von TCP/IP für die Serversicherheit

Die IP-Sicherheit für TCP/IP (Transmission Control Protocol) wird aktiviert, indem die Richtlinie **Sicherer Server** (standardmäßig deaktiviert) zugewiesen wird.

*Öffnen einer Komsole mit dem Snap-In **IP-Sicherheitsrichtlinienverwaltung** → im Detailfensterbereich mit der rechten Maustaste auf **IP-Sicherheitsrichtlinien auf lokalem Computer** klicken → Sicherer Server (Sicherheit erforderlich) → Zuweisen*

Überprüfen der IP-Sicherheitsrichtlinie bei Auftreten von Problemen

- Überprüfen der System- und Sicherheitsprotokolle auf Fehlermeldungen
- Überprüfen der IP-Sicherheitsüberwachung
- Überprüfen, ob die Richtlinien beiden Computern zugewiesen wurden
- die Richtlinien müssen miteinander kompatibel sein
- Neustart der IP-Sicherheitsüberwachung