# Sicherheit im Internet mit Microsoft Windows 2000

Werner Illsinger

## Sicherheit bei E-Mail

Das Internet Protokoll SMTP (*Simple Mail Transfer Protocol*), das zum Versenden von Mails im Internet verwendet wird hat einen großen Vorteil: es ist simpel, wie der Name schon sagt. Ein Beispiel dafür ist, dass die SMTP-Server nicht prüfen, wer die Nachricht abschickt. So könnte theoretisch jedermann eine Mail als bill.clinton@whitehouse.gov abschicken.

Eine zweite Möglichkeit wäre, eine Mail die zwar vom richtigen Absender kommt, auf dem Wege zu verfälschen. Zusätzlich wird E-Mail im Internet im Klartext übertragen. Theoretisch kann die Nachricht auf dem Weg vom Absender zum Empfänger abgehört werden.

Um E-Mail als Kommunikationsmedium für wichtige Kommunikation einsetzen zu können, benötigt man zusätzlich:

- Eine Methode um festzustellen, ob die Nachricht tatsächlich vom Absender stammt.
- Eine Methode um sicherzustellen, dass der Inhalt der Nachricht nicht verändert wurde.
- Eine Methode um das Abhören einer Nachricht zu verhindern.

## Digitale Signatur


Die elektronische Unterschrift löst gleich zwei Probleme. Sie stellt sicher, dass die Nachricht vom Absender stammt, der behauptet sie abgesendet zu haben. Zusätzlich stellt die digitale Signatur sicher, dass die Nachricht auf dem Weg von Absender zu Empfänger nicht verändert wurde.

Seit 1. Jänner gibt es in Österreich das „Signaturgesetz". Das Signaturgesetz regelt die Gleichstellung der elektronischen Unterschrift mit einer Unterschrift auf einem Vertrag. Sowohl Microsoft Outlook (Express 5 und 2000) unterstützen die digitale Signatur. Was man dazu benötigt und wie man sie anwendet, zeigen wir am ***Technet-Clubabend***.

## Verschlüsselung (Encryption)


Verschlüsselung ist ein Verfahren, bei dem es einem Mithörer (zufällig oder beabsichtigt) unmöglich (möglichst schwer) gemacht werden soll, den Inhalt einer Nachricht zu verstehen. Wichtig ist das vor allem, wenn man E-Mail dazu verwenden möchte, sensible Daten (Geschäftsdaten, Bestellungen, persönliche Daten, etc.) über das Internet zu übertragen. Seit Anfang des Jahres hat die US Regierung das Exportgesetz gelockert und es dürfen jetzt auch starke Verschlüsselungsverfahren in die meisten Länder der Erde (damit auch nach Österreich) exportiert werden.

## Sicherheit im Web

Woher weiß man, dass wenn man im Browser www.ccc.at eintippt, dass man wirklich bei unserem Club-Server landet? Es wäre theoretisch nicht sehr schwierig, jemanden einfach auf einen anderen Server umzuleiten. Bei unserem Club-Server ist das sicher kein Problem – aber stellen Sie sich vor, das macht jemand beim Telebanking-Server einer Bank.

Aus diesem Grund ist es wichtig, dass sich der Server gegenüber dem Benutzer ausweist. Zusätzlich möchte man natürlich auch seine Bankgeschäfte nicht unbedingt in der Öffentlichkeit abwickeln. Daher ist es auch besonders wichtig, dass die Daten auch hier verschlüsselt über das Internet übertragen werden. Die Methode, die in diesem Fall angewendet wird heißt SSL (*Secure Socket Layer*). Sowohl der Internet-Information-Server als auch der Internet-Explorer verstehen SSL. Wie einfach es ist, mit den Internet Information Services 5.0, die in Windows 2000 Server enthalten sind, einen SSL-Server einzurichten und was man dazu benötigt, zeigen wir am Technet-Clubabend.

## Verschlüsseltes Dateisystem

Ein Administrator in einem Netzwerk kann alle Daten aller Benutzer lesen? Nicht mehr seit Windows 2000. Windows 2000 unterstützt das sogenannte *Encrypted Filesystem* (EFS), das dem Benutzer die Möglichkeit gibt, seine Daten vor dem Zugriff anderer zu schützen. Dies geschieht, indem alle Daten auf der Festplatte (lokal oder am Server) verschlüsselt abgelegt werden. Damit ist gewährleistet, dass nur noch der entsprechende Anwender selbst seine Daten lesen kann. Wie einfach es ist, mit Windows 2000 seine Daten verschlüsselt abzulegen, zeigen wir am **Technet-Clubabend**.

## Smartcards

Windows 2000 unterstützt sogenannte Smartcards. Smartcards sind Scheckkartengroße Geräte. Was ist der Unterschied zwischen einer Chipkarte und einer Smartcard? Auf einer Smartcard befindet sich ein ganz winziger Computer – aber mit allem was dazugehört (Prozessor, RAM, ROM, PROM). Smartcards haben die Möglichkeit, sensitive Daten auf dieser Karte abzulegen – damit kann sie der Benutzer immer mit sich herumtragen (statt am Netzwerk abzulegen). Dieser Computer hat auch die Möglichkeit, Daten zu verschlüsseln. Diese Fähigkeit kann zum Unterschreiben und verschlüsseln von E-Mail, zum Anmelden an den Computer usw. verwendet werden. Wenn man eine Smartcard verwendet, benötigt man kein Passwort mehr – und das macht die Sache noch sicherer. Nähere Informationen zu Smartcards gibt es auf http://www.microsoft.com/security/tech/smartcards/ und am **Technet-Clubabend**.

## IPSEC

IPSEC ist die Möglichkeit, alle Daten, die von einem Server oder einer Workstation über das Netzwerk gesendet werden, zu verschlüsseln. Dazu muss sowohl der Server als auch die Workstation dies können. Sowohl Windows 2000 Server als auch Windows 2000 Professional unterstützen IPSEC (die Möglichkeit Datenverkehr auf einem TCP/IP-basierenden Netzwerk zu verschlüsseln).

http://www.ccc.at/clubabend/