Sicherheit im Internet mit 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 beim Web

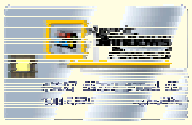
Woher weiß man, dass wenn man im Browser www.ccc.at eintippt, dass man wirklich bei unserem Club-Server landet? Es wäre theoretisch nicht sehr schwierig, jemanden einfach auf einen anderen Server umzuleiten. Bei unserem Club Server ist das sicher kein Problem – aber stellen Sie sich vor, das macht jemand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

Technet - Clubabend

Sicherheit im Internet mit Windows 2000

Mittwoch, **12. April 2000** ab 18:00

Exner-Saal TGM
Wexstraße 19-23
1200 Wien

Voranmeldung erforderlich unter
http://www.ccc.at/clubabend/

ein Buffet wird wie immer für Sie vorbereitet

VPL-CS1

Michael Kugler

Der Videoprojektor VPL-CS1 von SONY, mit 2,9 kg einer der leichtesten und mit seiner Notebookgröße auch einer der kleinsten.

Ausgeliefert wird der Projektor mit einem umfangreichen Kabelsortiment. Die mitgelieferte Tragtasche ist zweigeteilt. In hinteren Teil hat der Projektor seine Platz, der vordere Teil ist für die mitgelieferten Kabel bestimmt. Ein Klettverschluss verschließt die Tasche. Aufgestellt ist Projektor sehr einfach. Vorne die Klappe öffnen, und hinstellen. Damit ist gleichzeitig für die Luftzufuhr unterhalb des Projektors gesorgt. Der für die Kühlung zuständige Ventilator saugt von unten die Luft an. Selbstverständlich ist ein Ersatzluftfilter beigelegt.

Vorne wird das Netzkabel angesteckt, damit ist der Projektor bereits im Stand-by-Betrieb, die Datenkabel werden hinten angesteckt.

Im Computerbetrieb kennt der VPL-CS1 insgesamt 38 vordefinierte Modi. Die von den 1.44 Millionen Pixel dargestellte Auflösung beträgt 800x600. Der Input kann aber bis zu einer Auflösung von 1280 x 1024 bei 85 Hz gehen. Die Umwandlung auf die niedrigere Auflösung erfolgt ausgezeichnet. Mit der Taste APA sucht der Projektor eigenständig die beste Darstellungsmöglichkeit.

Im Videobereich ist es neben der Möglichkeit eines normalen Videosignals (eine Chinch-Buchse nimmt das FBAS-Videosignal auf) auch möglich, S-VHS Signale anzulegen. Die 600 Zeilen des SVHS Signals werden auch wirklich angezeigt. Der Begriff des Heimkinos erfährt eine neue Bedeutung. Der eingebaute Audioverstärker ist dagegen etwas kümmerlich (2 x 0.5 W). Über den Maus-Anschluss lässt sich die mitgelieferte Fernbedienung als Computer verwenden. Falls der Computer einen USB Anschluss hat, lässt sich der Projektor über den Computer steuern. Ebenfalls lassen sich USB-Geräte direkt an den Projektor anschließen.

Der Projektor verfügt über ein Menu für die verschiedenen Einstell- und Anpassungsoptionen. Im Menu können neben den standardmäßigen Einstellungen wie Helligkeit und Kontrast auch die Farbtemperatur oder der Gammawert eingestellt werden.

Das Menü EING-EINST liefert je nach der Art des Eingangsignals die Möglichkeit eine eigene Signalquelle zu definieren. Das folgende Menu EINSTELLUNGEN liefert die interessantesten Optionen. Eine Korrektur einer trapezförmigen Verzerrung (nur bei Computer-Signalen) und die Gesamtanzahl der Stunden, die die Lampe in Betrieb war, sind nur zwei der Möglichkeiten.

Für den Schulbetrieb eignet sich der Projektor ausgezeichnet. Mit seinen 600 Ansi-Lumen ist er durchaus in der Lage (bis auf wenige wirklich helle Sonnentage) das Klassenzimmer hervorragend auszuleuchten. Mit dem 2,9 kg schweren Projektor und einem Laptop bekommt das Wort Präsentation eine neue Bedeutung. Weitere Daten siehe:
http://www.sony.at/projection/pro/1/VPL-CS1.html

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).

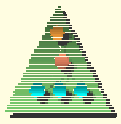
Authenticode und warum Sie Office 2000 vor Viren schützt

Woher wissen Sie, dass eine Datei, die Sie aus dem Internet herunterladen frei von Viren ist? Dann, wenn der Softwareentwickler dafür garantiert, dass sie Virenfrei ist. Aber wie kann der Softwareentwickler garantieren, dass eine Software nicht von einem Virus befallen wurde? Hier wird die gleiche Methode angewendet, wie beim Unterschreiben von E-Mails. In diesem Fall wird die Software vom Entwickler unterschrieben. Damit kann der Anwender davon ausgehen, dass die Software ihn so erreicht, wie der Entwickler das wollte.

Die gleiche Technik kann seit Office 2000 auch für Office-Makros angewendet werden. Als Anwender oder Administrator kann man die Ausführung von Makros, die nicht aus dem eigenen (oder vertrauenswürdigen) Unternehmen stammen, verhindern. Makros, die unerwünscht an Dokumenten hängen, werden einfach ignoriert. Das hilft sehr bei der Bekämpfen der sehr lästigen und teilweise auch sehr gefährlichen Makroviren. Nähere Informationen zu diesem Thema unter *http://www.microsoft.com/security/tech/authenticode/* und am nächsten **Technet-Clubabend**.

Active Directory in Windows 2000

Active Directory ist der Grundstein aller sicherheitsrelevanten Funktionen in Windows 2000. *Active Directory* dient als zentrale Ablage aller benutzerspezifischer Daten. Am Technet-Clubabend erfahren Sie, warum sich *Smartcards* (als privater Datenspeicher) und das *Active Directory* (als zentrales Verzeichnis) ideal ergänzen und zusammen ein unschlagbares Team bilden.



Weiterführende Informationen

Auf der Windows 2000 Website unter *http://www.microsoft.com/windows2000/library/planning/walkthroughs/* finden sich ausgezeichnete „*Step by Step Guides*“ für Windows 2000, (auch über Sicherheitsrelevante Themen) in denen die Konfiguration der einzelnen Sicherheitsfunktionen von Windows 2000 Schritt für Schritt erklärt werden. Allgemeine Informationen über Windows 2000 finden sich unter
http://www.microsoft.com/windows/.

Microsoft und Sicherheit

Microsoft nimmt Sicherheit sehr ernst. Aus diesem Grund gibt es eine Website mit vielen Informationen zum Thema Sicherheit. Diese Website finden Sie unter *http://www.microsoft.com/security/*.