Hilde Gruber †

Am 4. März 2006, nur wenige Tage nach ihrem 51. Geburtstag, ist unsere liebe Kollegin Hildegard Gruber nach langer und schwerer Krankheit, die sie vor uns und vor ihrer Familie bis zuletzt vollständig verborgen hat, verstorben. Die Nachricht von ihrem Tod hat uns völlig unerwartet getroffen und bei allen die größte Bestürzung ausgelöst.

Hilde Gruber trat am 1. März 2001 als Angestellte in den Zentralen Informatikdienst ein und kümmerte sich vor allem um die Hardware-Installationen und Software-Konfigurationen am Vienna Internet eXchange (VIX). Wie oft hat sie in diesen fünf Jahren die TechnikerInnen der diversen Internet-Provider in die Maschinenräume im NIG begleitet, um ihnen beim Anschluss ihres Datennetzes an den VIX behilflich zu sein? Wie viele Anfragen hat sie am Telefon oder per eMail in kompetentester Weise beantwortet, wenn VIX-TeilnehmerInnen Auskünfte zu betrieblichen Detailfragen benötigten?

In den letzten Monaten hat Hilde Gruber vom Zentralen Informatikdienst eine kurze Auszeit erbeten und einen Karenzurlaub angetreten. Wir hatten nicht die geringste Ahnung, dass sie längst fest entschlossen war, als Schwerkranke ihren Tod in aller Stille zu erwarten. Hilde Gruber wird uns allen, die mit ihr zusammenarbeiten durften, mit ihrer netten, hilfsbereiten und ruhigen Art für immer als hochgeschätzte Kollegin in Erinnerung bleiben.

Peter Rastl

Inhalt

Aktuelles

PCs & Workstations

Netzwerk- & Infodienste

Anhang

VENI, VIDI – UND TESTETE VISTA!

Das neue Betriebssystem von Microsoft

Microsoft ist im Moment wieder in aller Munde, weil die AnwenderInnen noch ein Weilchen länger warten müssen, bis sie ihr Betriebssystem mit Windows Vista – das übrigens mit der Lernplattform der Universität Wien, WebCT Vista, nur den Namen gemeinsam hat – auf den neuesten Stand bringen dürfen. *Eh schon erwartet*, könnte man bösartigerweise sagen. Aber was entgeht uns wirklich, wenn Windows Vista erst Anfang 2007 (sofern der derzeit angekündigte Auslieferungstermin eingehalten wird) mit einer Entwicklungszeit von satten fünf Jahren unsere Computer heimsucht? Worin liegen die bahnbrechenden Neuerungen, und ist ein sofortiger Umstieg überhaupt empfehlenswert? Der nachfolgende Testbericht soll einen ersten Einblick in die neue Windows-Welt geben und damit vielleicht die eine oder andere Fragestellung beantworten.

Getestet wurde die **Windows Vista Beta 2 Build 5384** (englisch) auf einem AMD Sempron 3000+ Rechner mit 1.80 GHz und 512 MB RAM. Die Installation dieses Betriebssystems läuft folgendermaßen ab: Nach Auswahl der Basisinformationen (z.B. *Installation language*, *Keyboard language*, *Time and currency format*) werde ich aufgefordert, mittels Klick auf *Install now* die Installation zu starten. Nun muss ich den *Product key* eingeben, die *License items* akzeptieren und auswählen, welche Art der Installation vorgenommen werden soll – wobei hier ohnehin nur *Custom (Advanced)* zur Verfügung steht – bzw. auf welchem Laufwerk das Betriebssystem installiert werden soll. Die Installation selbst (aufgrund der Datenmenge via DVD) gestaltet sich reibungslos. Dass Windows Vista vor allem auf verbesserte Sicherheitsmechanismen setzt, fällt bereits im Zuge der Programminstallation auf, denn erstmals muss ich mich schon unmittelbar nach der Installation des Betriebssystems mit Benutzername und Passwort authentifizieren. Hier wird auch gleich nachgefragt, wie ich mit verfügbaren Updates umgehen möchte (die Bandbreite liegt zwischen *Never check for updates* bis hin zu *Install updates automatically*). Dann muss ich noch die *Regional and Language Options* bzw. *Date and Time* festlegen, und anschließend kann es mittels Klick auf *You're ready to start* endlich losgehen. Nach einer guten halben Stunde Installieren, dem erforderlichen Neustart und der Eingabe des korrekten Passworts wird mein Warten belohnt, und Windows Vista begrüßt mich mit dem neuen Welcome Center.

Was mir als eingefleischter Windows-Benutzerin – neben der optischen Neugestaltung der Fenster – auf den ersten Blick ins Auge springt, ist die Übersichtlichkeit: Dort, wo früher mit zum Teil nichts sagenden Icons gespickte Symbolleisten zu finden waren, herrscht nunmehr Ordnung. Navigiert wird wie im Browser mit Vor- und Zurück-Pfeilen; mittels *Deep Linking* hat man exakt den Überblick, wo man sich gerade befindet und welche Navigationswege einem offen stehen. Ein Suchfeld – am rechten oberen Fensterrand positioniert – legt nahe, dass hier nach den gewünschten Einstellungsmöglichkeiten gesucht werden kann. Ausgehend von der Detailansicht meiner Computerspezifikation innerhalb des Welcome Center teste ich die Suche durch Eingabe des Begriffs *monitor* – und siehe da, bereits während des Eintippens werden aus der Masse der zur Verfügung stehenden Einstellungsmöglichkeiten innerhalb des Control Panel (das Welcome Center ist ein Teil davon) nur mehr jene angezeigt, die in Übereinstimmung mit dem gesuchten Begriff stehen. Im Nu kann ich also via *Personalization* unter anderem die Bildschirmauflösung bzw. das Farbmanagement meines Monitors kontrollieren. Alles in allem: Information in kleinen, übersichtlichen Portionen mit intuitiver Bedienbarkeit – und kommt man damit nicht zu Rande, bleibt immer noch die Suchfunktion.

Abb. 1: Windows Vista – Welcome Center

Herzlich willkommen

Aber zurück zum **Welcome Center**, das sich quasi als Einstiegsportal präsentiert (siehe Abb. 1). Es ermöglicht einen raschen Überblick über die Computerspezifikation, und daneben lassen sich hier bereits die wichtigsten Basisaufgaben durchführen: das Hinzufügen von Hardwarekomponenten, die Vista während des Installationsvorganges nicht automatisch erkannt bzw. installiert hat, das Hinzufügen oder Entfernen von Druckern und *last but not least* die persönlichen Windows-Einstellungen wie Bildschirmhintergrund und -auflösung, Bildschirmschoner usw. Hinter dem Punkt *Windows Basics* versteckt sich eine Art Leitfaden für PC-Neu-

linge, die mit dieser Anleitung ihre ersten Windows-Schritte machen sollen. Über das integrierte Hilfesystem wird der Anwender Schritt für Schritt in die Welt der Computer und Peripheriegeräte bzw. in die Windows-Welt eingeführt. Diesen Ansatz gab es auch schon unter Windows XP, allerdings an nicht so prominenter Stelle und bei weitem nicht so ausführlich. Klickt man auf den Eintrag *Show all 12 items*, wird der Inhalt des Welcome Center um acht mehr oder weniger nützliche Tools erweitert. Neben einem Programm mit der Bezeichnung *Windows Easy Transfer* (das laut Beschreibung dem guten alten Migration Wizard entspricht, mit dem sich Daten und Einstellungen des „alten" PCs auf den neuen übertragen lassen) gibt es hier noch die Möglichkeit, über *Add new users* neue Benutzerkonten anzulegen, den PC mit dem Internet zu verbinden, zum Control Panel zu wechseln oder sich über die Windows-Neuigkeiten zu informieren und die installierte Version auch gleich zu registrieren. Und weil's so wichtig ist, kann man hier auch seinen Windows Media Player konfigurieren.

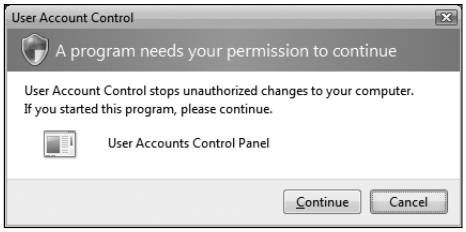


Abb. 2: Windows Vista – Warnung bei Aufruf eines Programms

Beim Versuch, neue Benutzerkonten anzulegen, fällt mir so nebenbei auf, dass Windows Vista hierfür meine Erlaubnis einholt (siehe Abb. 2). Dezent werde ich mittels Warnmeldung darauf hingewiesen, dass die *User Account Control* (UAC) dafür verantwortlich ist, und falls ich diejenige war, die das Programm gestartet hat, soll ich auf den *Continue*-Button klicken. Im Gegensatz zu vorherigen Beta-Versionen werde ich nicht mehr durch Meldungen verunsichert, die mir eine Entscheidung abverlangen, ob ich dem Programmcode vertraue oder nicht. Scheinbar hat auch Microsoft mittlerweile eingesehen oder einsehen müssen, dass es für „unbedarfte" Windows-AnwenderInnen keineswegs einfach ist, solche Entscheidungen zu treffen. Nach einem kurzen In-mich-Hineinhorchen komme ich zu dem Ergebnis, dass ich die Anwendung tatsächlich gerade eben starten wollte, und klicke daher ohne weiteres Zögern auf *Continue*. Gespanntes Warten – dürfte funktioniert haben, das Programm startet ohne Probleme.

Wie bereits ihre Vorgänger konfrontiert mich auch diese Beta-Version im Laufe der weiteren Tests noch unzählige Male mit diesem „Bitte um Erlaubnis"-Spiel. Was ich anfangs noch mit einem gewissen Wohlwollen sehe (schließlich ist man ja doch ein wenig um die Sicherheit seines PCs besorgt), mutiert spätestens nach dem zehnten Mal zum Ärgernis, dann nämlich, wenn das wiederholte Ausführen desselben Programms jedes Mal bestätigt werden muss. Die vielzitierte *Banner-Blindness* mutiert hier zur *Continue-Blindness*: Vor lauter Frust liest man die Meldung gar nicht mehr und denkt auch nicht mehr darüber nach, ob man das Programm wirklich selbst gestartet hat. Ein wenig mehr Merkfähigkeit wäre hier angebracht: Einmal bestätigen und die Aktion mit Programmbezeichnung in eine Liste speichern (somit ist sie wieder abrufbar bzw. nachträglich kontrollier- und editierbar, denn nicht immer bestätigt man solche Abfragen bei vollem Bewusstsein) – mehr verlange ich gar nicht.

Beim verzweifelten Versuch, diesem Treiben Einhalt zu gebieten, stoße ich schließlich auf die Option *Change Security Settings* innerhalb der *User Accounts*. Allerdings bietet sich hier nur die Möglichkeit, dieses Sicherheitsfeature entweder zu verwenden oder nicht. Deaktiviere ich die Option, indem ich das Häkchen wegklicke, muss ich einen Neustart durchführen und kann nun ohne Warnmeldungen arbeiten. Ob es jedoch wirklich schlau ist, dieses Feature generell zu deaktivieren, ist fraglich. Microsoft empfiehlt jedenfalls die Verwendung, und standardmäßig ist die Option auch aktiviert.

Der nächste Test mit dem Welcome Center, das Anlegen von zusätzlichen Benutzerkonten, funktioniert bereits beim ersten Anlauf reibungslos. Ein Klick auf die Option *Add new users*, Name eingeben und Standarduser-Rechte bzw. Administrator-Rechte zuordnen – schon fügt sich der neue User in die Reihe der Benutzerkonten ein. Neben den schon unter Windows XP vorhandenen Optionen wie *Change Name*, *Create a password*, *Change the picture* sowie *Delete the account* stoße ich auf eine interessante Neuerung: *Parental Controls*.

Kindersicher

Hinter der Bezeichnung **Parental Controls** verbirgt sich die Möglichkeit, für jedes Benutzerkonto sehr detaillierte Einschränkungen zu treffen (siehe Abb. 3) – sinnvollerweise allerdings nur mit Administrator-Rechten. Zum einen geht es nach Zeit, indem man ganze Tage oder aber auch nur einzelne Stunden definiert, in denen der PC, bestimmte Programme oder das Internet verwendet werden können bzw. gesperrt sind. Zum anderen kann man die Nutzung nicht altersgemäßer Spiele mit Hilfe so genannter Rating-Systeme unterbinden bzw. Spiele mit bestimmten Inhalten überhaupt blockieren. Das funktioniert auch mit Programmen und Webseiten, indem genau festgelegt werden kann, welche davon ein bestimmter Benutzer verwenden bzw. aufrufen darf und welche für ihn gesperrt sind. Zu guter Letzt bietet Vista in diesem Bereich Eltern die Möglichkeit, einen detaillierten Aktivitätsbericht anzufordern, worin aufgelistet ist, was die lieben Kinder in letzter Zeit auf dem Computer gemacht haben. Auf den ersten Blick handelt es sich hierbei um wirkungsvolle Methoden, um Kinder vor schädlichen Spielen und Webseiten besser zu schützen – fraglich ist nur, ob sich die Elternschaft wirklich die Mühe machen wird, das hierfür nötige Feintuning durchzuführen, oder ob sich dieses Feature nicht als reine Alibiaktion erweist. Wie die Praxis zeigt, ist ein absoluter Schutz (gerade im

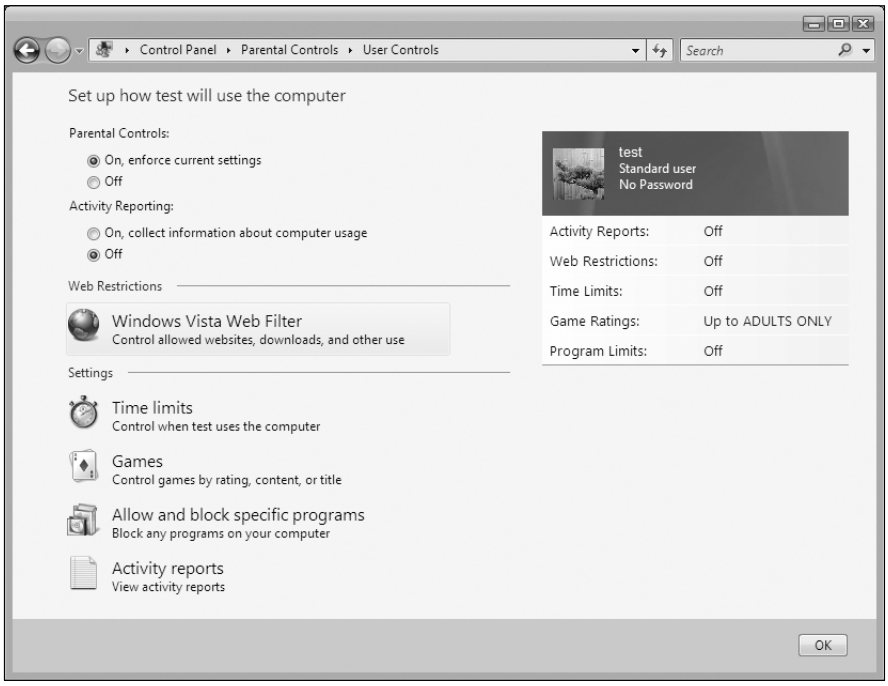


Abb. 3: Windows Vista – Parental Controls

Hinblick auf das Verbieten des Aufrufs von „schädlichen" Webseiten) ein frommer Wunsch, der leider selten von Erfolg gekrönt ist.

Aber zurück zum Benutzerkonto-Konzept, das sich in Benutzer mit Administrator-Rechten und Benutzer mit Standarduser-Rechten unterteilt und im Vergleich zu den Vorgängerversionen mehr Flexibilität verspricht. Spezielle administrative Tätigkeiten wie z.B. die Installation neuer Programme können erst nach erfolgter Bestätigung einer Berechtigungsabfrage ausgeführt werden. Das gestaltet sich so, dass eine Meldung am Bildschirm darauf hinweist, dass nur Personen mit Administrator-Berechtigung die nötigen Privilegien besitzen, um die gewünschte Aktion vorzunehmen. Der Vorteil ist allerdings, dass man als Standarduser nicht mehr ausloggen muss, sondern dass bereits die Eingabe des Administrator-Passworts im entsprechenden Dialogfenster die nötige Berechtigung erteilt. Damit wird effizienter als bisher der Problematik der Administrator-Berechtigungen begegnet.

Safe – Safer – Security Center

Die mögliche Einschränkung von Benutzerberechtigungen ist jedoch nur ein Ansatz von Microsoft in Richtung verbesserte Sicherheit. Glaubt man Microsoft, so wird in Windows Vista nicht nur die unbemerkte Installation „böser" Software (so genannter *Malware*) verhindert, sondern auch der Suche nach bzw. dem Entfernen von bereits vorhandener Malware besonderes Augenmerk geschenkt. Als zentrale Stelle hierfür präsentiert sich das **Security Center** (siehe Abb. 4), das bis auf wenige Erweiterungen schon unter Windows XP SP2 zur Verfügung stand. Laut der Vista-Produktbeschreibung auf der österreichischen Microsoft-Website habe ich sicherheitstechnisch kaum mehr etwas zu befürchten, denn neben der Möglichkeit, mittels des automatischen **Windows Update** stets auf dem neuesten Stand in puncto Security-Patches zu sein, sorgt die eingebaute **Windows Firewall** für zusätzlichen Schutz vor Hackern, Viren und Würmern, die sich via Internet in den PC einschmuggeln wollen. Mit dem **Windows Defender** zum Schutz vor Spyware und der **Malware protection** zur Erkennung und Entfernung bösartiger Software ist das Security-Quartett komplett. Also alles in Butter in puncto Sicherheit, könnte man meinen, denn immerhin halte ich doch gerade die laut Microsoft-Werbekampagne *„bislang sicherste Version von Windows"* in Händen, die mir *„mit den neuen Features von Windows Vista die benötigte Kontrolle und Sicherheit bietet, um das Optimale aus meinem PC herauszuholen."* Solchen Aussagen stehe ich schon von Berufs wegen skeptisch gegenüber, und nach einem Gespräch mit dem Security Coordinator des ZID steigt die Skepsis weiter – denn im Wesentlichen verbirgt sich hinter den vielgelobten sicherheitstechnischen Neuerungen zum Teil Altbekanntes im neuen Look, und von einem völlig neuartigen Sicherheitskonzept ist in dieser Beta-Version nicht viel erkennbar.

Während die Windows Firewall automatisch und das *Automatic updating* durch mich (im Zuge der Installation) aktiviert wurde, findet sich unter *Malware protection* alles, nur

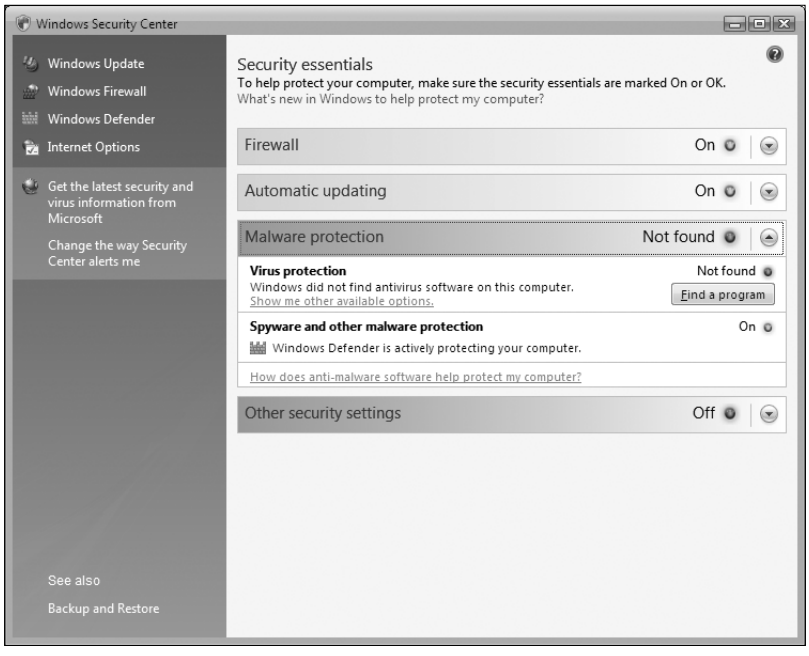


Abb. 4: Windows Vista – Security Center

keine Antivirus-Software. Mit dem Button *Find a program* erhält man jedoch die Chance, ein solches von einem Drittanbieter via Internet downzuloaden. Ich entscheide mich für die u.a. angebotene 30-Tage-Gratisversion der EZ Antivirus Software von Computer Associates – lasse es dann aber doch bleiben, denn ich werde mit einer Pseudorechnung über $ 0.00 beglückt, soll dafür meine Kontaktdaten eingeben, und erst dann funktioniert der Download. Nein danke. Ohne Pseudorechnung lade ich den VirusScan Enterprise 8.0 von McAfee herunter (siehe `www.univie.ac.at/ZID/gratissoftware/`) und installiere ihn. Beleidigt meldet Microsoft, dass zwar eine Antivirus-Software installiert ist, jedoch die Wartung im Hinblick auf verfügbare Updates einzig und allein in meiner Hand liegt.

Neu hinzugekommen ist der Windows Defender, dessen Aufgabe darin besteht, Spyware, Rootkits sowie Keylogger zu erkennen und diese vom Rechner zu verbannen. Die eingebaute Scanfunktion spürt auf dem PC vorhandene Spyware (das sind Programme, die beispielsweise Interneteinstellungen ändern bzw. personenbezogene Daten ohne das Einverständnis der AnwenderInnen nutzen) rasch auf. Alles im grünen Bereich, meldet mir der abgeschlossene Scanvorgang: *No unwanted oder harmful software was detected.* Via *History* erhält man einen Überblick über all die Aktivitäten, die man mittels Windows Defender zugelassen oder in die Quarantänestation geschickt hat. Findet sich in der Liste ein Programm, das nicht ausgeführt wird, weil es versehentlich via Warnmeldung geblockt wurde, kann man diese Blockade durch Klick auf die *Quarantined items* und die Schaltfläche *Restore* wieder funktionstüchtig machen. Unter *Tools* und *Settings* befinden sich die *Options*, die festlegen, wie sensibel der Windows Defender reagieren soll. Hier lassen sich z.B. die Scanfrequenz, aber auch die *Real-time protection options* festlegen. Neben der Möglichkeit, diese *Real-time protection* generell zu deaktivieren, findet sich auch eine Liste möglicher Optionen, die davon ausgenommen werden können. Beispielsweise meldet sich der Windows Defender bei Internet-Downloads und Softwareinstallationen (getestet beim Download von McAfee VirusScan) mit entsprechenden Warnungen, fragt nach, ob ich über diese Vorgänge informiert bin und holt meine Erlaubnis ein, um fortfahren zu dürfen. Zu Testzwecken rufe ich einschlägig bekannte Websites auf und werde mehrmals gewarnt, dass sich das eine oder andere Internet Explorer Add-On installieren möchte – was ich selbstverständlich jedes Mal dankend ablehne. Ob Spyware, die sich unbemerkt auf den Rechner einschleichen möchte, es allerdings tatsächlich nicht schafft, wird wohl erst dann wirklich zu erkennen sein, wenn das Betriebssystem im Echtbetrieb eingesetzt wird.

Der Desktop

Von den Sicherheitsmechanismen nun aber zurück zu augenscheinlicheren Dingen – beispielsweise dem **Desktop**, dessen Grundaufbau sehr ähnlich dem von XP ist. Da finden sich die Taskleiste und das Startmenü wieder, welches allerdings nur mehr durch einen runden Startbutton mit der Windows-Flagge gekennzeichnet ist. Ins Auge springt selbstverständlich das veränderte Design, wobei ich auf den vielgerühmten Glaseffekt beim Aufruf von Dialogfenstern bislang verzichten musste, was wohl auf die vorliegende Beta-Version zurückzuführen ist. Nur ein halbtransparenter Papierkorb und die Verwendung der Sidebar lässt in etwa erahnen, wie es aussehen könnte. Allerdings sollen laut Microsoft-Policy ohnehin nur jene Anwender in den Genuss dieser Oberfläche kommen, die ihr System ordnungsgemäß lizenzieren, also quasi einer Überprüfung standhalten, ob die verwendete Vista-Version nicht vielleicht doch eine Raubkopie ist.

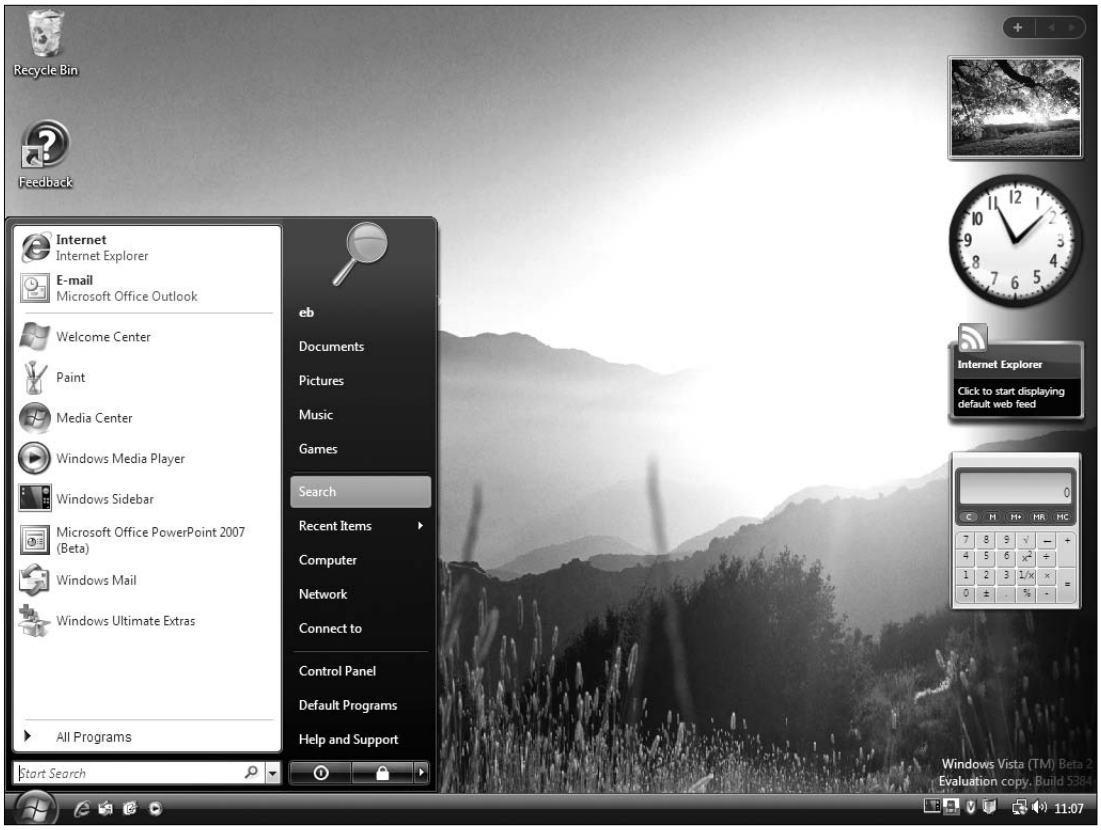


Abb. 5: Windows Vista – Start menu und Sidebar

Abb. 6: Windows Vista – Control Panel

Als Mac-Anwenderin hätte ich beim ersten Anblick der neuen *Aero*-Benutzeroberfläche eine Art Déjà-vu-Erlebnis – präsentiert sich doch das Apple-Betriebssystem ziemlich ähnlich, allerdings unter dem Namen *Aqua*. Generell fällt an einigen Stellen eine nicht nur rein optische Verwandtschaft zu Mac OS X auf. Wer da von wem abkupfert, soll nicht Gegenstand dieses Artikels sein; interessierte LeserInnen können sich aber z.B. unter `www.winsupersite.com/showcase/winvista_beta1_vs_tiger_01.asp` genauer über dieses Thema informieren.

Start menu & Sidebar

Auch das **Start menu** (siehe Abb. 5) wartet mit einem überarbeiteten Layout auf – wobei sich die Frage stellt, ob es wirklich notwendig ist, dass sich das Icon am oberen rechten Rand immer wieder der unterhalb gewählten Option anpasst. Weggefallen ist das Popup-Menü, das aufklappt, sobald die Option *All Programs* ausgewählt wird; stattdessen ist die Programmliste nun direkt im Start menu implementiert und öffnet sich im Bereich der linken Fensterhälfte. Wenn ich daran denke, wie verzweifelt manche TeilnehmerInnen im Windows-Grundkurs versuchen, im aufklappenden Untermenü das richtige Programm zu treffen, zweifle ich nicht daran, dass diese Neuerung zum Bedienungskomfort beitragen wird.

Aber nicht nur das Start menu bietet in Windows Vista Zugriff auf installierte Anwendungen, sondern auch die neue **Sidebar**. Sie fungiert als Ablage für Miniapplikationen (so genannte *Gadgets*), die schnell greifbar sein sollen. Waren in den vorangegangenen Beta-Versionen nur eine Uhr, ein RSS-Reader, ein Startfeld für mehrere Programme, eine Slideshow und ein Mülleimer als Gadgets auswählbar, so ist anhand der vorliegenden Beta-Version bereits erkennbar, dass uns in nicht allzu ferner Zukunft wohl eine Vielzahl von Gadgets überschwemmen wird, mit denen man alle möglichen und unmöglichen Dinge rasch im Zugriff hat. Ob man die Sidebar überhaupt verwenden bzw. mit wie vielen Gadgets man diese bestücken möchte, lässt sich in den zugehörigen Einstellungen festlegen.

Control Panel

Einen sehr wesentlichen Bestandteil des Betriebssystems stellt nach wie vor das **Control Panel** (die Systemsteuerung) dar, dessen klassische Ansicht bereits unter Windows XP unübersichtlich war. In Windows Vista sind noch ein paar Einstellungsmöglichkeiten hinzugekommen, und dem Anwender eröffnet sich in der klassischen Ansicht nun eine schier unüberschaubare Zahl verschiedener Icons. Selbst ich als langjährige Windows-Kennerin bin damit ein wenig überfordert. Um des Problems Herr zu werden und die AnwenderInnen nicht unnötig in die Irre laufen zu lassen, wartet Vista mit einer verbesserten Gliederung in Kategorien auf, erweitert um die zum Teil sehr aufschlussreichen Beschreibungen der Aufgaben, die mit den jeweiligen Programmen erledigt werden können (siehe Abb. 6). Wer sich trotzdem nicht zurechtfindet, kann auf die integrierte Suchfunktion zurückgreifen, die bereits während der Eingabe des Begriffs nur noch die passenden Optionen anzeigt.

Ein interessantes Werkzeug namens *Performance Rating and Tools* (siehe Abb. 7) ist innerhalb des Control Panel im

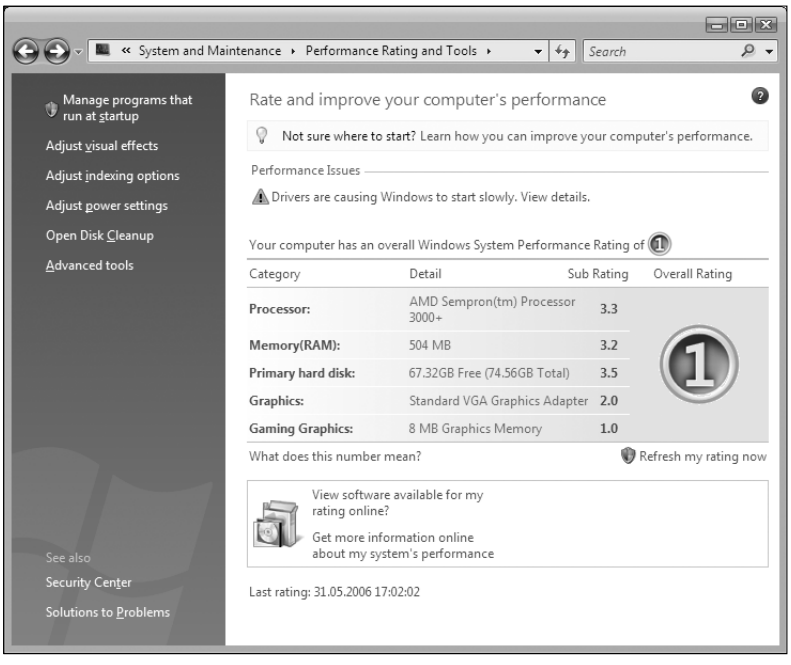


Abb. 7: Windows Vista – Performance Rating and Tools

Bereich *System and Maintenance* zu finden. Anhand der Prozessorleistung, des vorhandenen Arbeitsspeichers, des Speichervolumens der Festplatte sowie der Spezifikation der Grafikkarte vergibt Windows Vista Noten. Ich kann mich glücklich schätzen, denn mein Test-PC bekommt eine glatte Eins. Also gibt es zumindest von der PC-Seite her keinerlei Ausrede dafür, dass Arbeiten nicht zügig und rasch erledigt werden können. Für all jene PCs, die nicht mit Spitzennoten aufwarten können, finden sich hier die nötige Hilfestellung, die nötigen Programme (z.B. *Disk Cleanup*) bzw. auch diverse Einstellungsmöglichkeiten (z.B. *Adjust visual effects* oder *Adjust power settings*), um die Leistungsfähigkeit des Computersystems zu verbessern. Über die so genannten *Advanced tools* kommt man zur *Performance Diagnostic Console*, die beispielsweise mit einem *Performance Monitor* aufwartet, der die CPU-Auslastung grafisch darstellt (startet man z.B. den Internet Explorer, erhält Vista einen Adrenalinstoß, und die CPU-Auslastung beträgt kurzfristig 100%). Daneben finden sich hier etliche Diagnosetools, die Auskunft über ausgeführte Tätigkeiten bzw. über Fehlermeldungen und -behebungen geben.

Surfen mit dem Internet Explorer 7

Microsoft hat dem **Internet Explorer 7** ein vollkommen neues Gesicht verpasst, und auch hier wird Übersichtlichkeit groß geschrieben: Die Mehrzahl der Icons wurde durch ein paar zielgerichtete Hinweise (z.B. *Page* oder *Tools*) ersetzt, die bei Anklicken die dazu passenden Optionen wie *Send this Page*, *Save as* oder aber *Pop-up Blocker*, *Toolbars*, *Internet Options* usw. freigeben. Vorbei ist nun auch die „Never-ending-Window-Story" – anstelle unzähliger Browserfenster hält jetzt endlich auch im Internet Explorer 7 das so genannte *Tabbed Browsing* Einzug, was bedeutet, dass mehrere Webseiten gleichzeitig mittels Registerkarten-System im selben Fenster angezeigt werden können.

Selbst dem relativ neuen Thema Newsfeeds – bekannt auch unter der Bezeichnung RSS (siehe Artikel *RSS Enterprise* in *Comment 06/1*, Seite 46 bzw. unter `www.univie.ac.at/comment/06-1/061_46.html`) – wird Rechnung getragen. Newsfeeds können mit dem IE7 rasch und einfach bezogen werden: Sobald via IE7 eine Seite aufgerufen wird, die einen Newsfeed enthält, wird in einem gelben Meldungskästchen darauf hingewiesen (siehe Abb. 8). Um diesen zu abonnieren, genügt es, auf *Subscribe to this feed* zu klicken und den gewünschten Namen und Speicherort anzugeben – schon ist man dabei. Sortier- und Gruppiermöglichkeiten runden die einfache Nutzung von Newsfeeds ab.

Auch in puncto Sicherheit hat der IE7 angeblich einiges dazugelernt, beispielsweise sollen Schäden durch Phishing und gefälschte Websites nun der Vergangenheit angehören (siehe Abb. 9; mehr zum Thema Phishing finden Sie auf Seite 37). Mangels entsprechender, noch existenter Phishing-Webseiten kann ich die Treffsicherheit und Qualität dieses Features leider nicht austesten. Nur soviel sei gesagt: Auf fragwürdige Webseiten wird laut Microsoft-Beschreibung mittels Warnmeldung hingewiesen bzw. erscheint innerhalb der Adresszeile ein entsprechender Hinweis. Basis dafür soll einerseits eine so genannte *Whitelist* von mehreren tausend Websites sein, die Microsoft als sicher einstuft, anderseits das Erkennen typischer Charakteristika, die Phishing-Websites gemeinhin auszeichnen. Dass dabei Kontakt zu Microsoft-Servern aufgenommen werden muss und ob vielleicht nebenbei andere Informationen mitgeschickt werden könnten, möchte ich nicht näher kommentieren. Scheinbar hat aber auch Microsoft ein verstärktes Problembewusstsein im Hinblick auf den Schutz der Privatsphäre seiner KundInnen entwickelt und Jefferson Wells (ein auf die Überprüfung von Technologien spezialisiertes Unternehmen) beauftragt, die Anti-Phishing-Funktion des IE7 unter diesem Gesichtspunkt zu kontrollieren. Als Ergebnis stellte Jefferson Wells fest, dass diese keine persönlichen Benutzerdaten übermittelt und auch die versendeten Daten keinen Rückschluss auf den Anwender geben. Wer es genau wissen möchte, sei auf den Report verwiesen, der als PDF-Datei abrufbar ist (`www.jeffersonwells.com/Client_Audit_Reports/Microsoft_PF_IE7_IEToolbarAddin_Privacy_Audit.pdf`).

Wenn wir schon beim Thema Phishing sind, ein kleiner Schwenk zum integrierten Mailing-Programm: Nach Outlook Express als Mail-Client sucht man unter Windows Vista vergeblich. Fündig wird man allerdings unter dem Namen **Windows Mail**, und wie erwartet gibt es hier keine bahnbrechenden Neuerungen. Allerdings ist ein via Windows Mail empfangener Newsletter als potentielle Phishing-Mail eingestuft und mit einem roten Warn-Icon markiert. Ruft man die so gekennzeichnete Nachricht auf, finden sich nähere Informationen unterhalb des Mail-Headers. Wahlweise kann man nach den ausführlichen Phishing-Erläuterungen die Nachricht löschen oder freischalten. Ein sehr löblicher Beitrag Microsofts zum Thema Phishing. Von „Filterung" kann allerdings nicht die Rede sein, wenn die Treffsicherheit

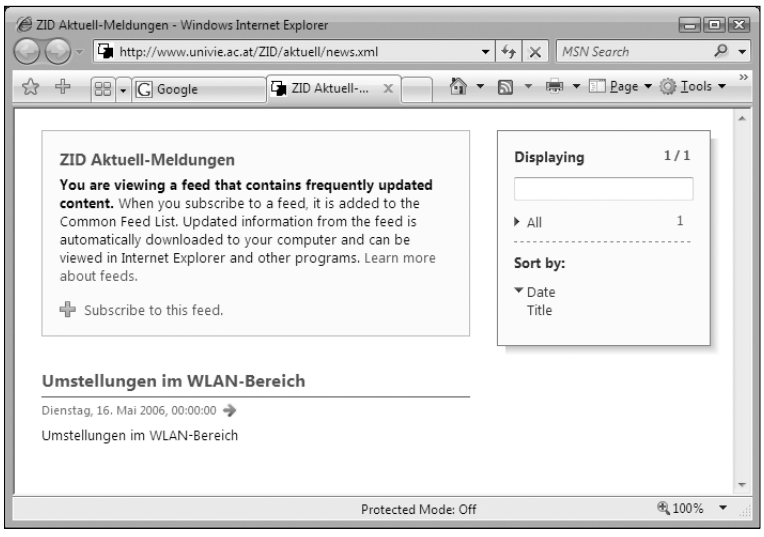


Abb. 8: Windows Vista – Internet Explorer 7

nicht noch erhöht wird: Mir graut bei dem Gedanken, dass in Zukunft womöglich bei vielen meiner abonnierten Newsletters ein solcher Fehlalarm gegeben wird und ich mir neben meiner *Continue-Blindness* auch noch eine *Phishing-Reminder-Blindness* zuziehe.

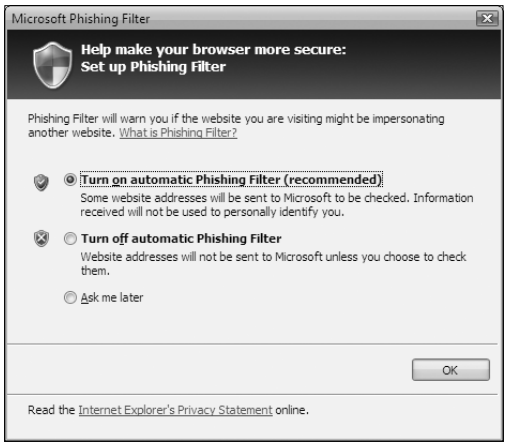


Abb. 9: Windows Vista – Phishing Filter

Kleine Helferlein

Selbstverständlich sind auch wieder verschiedene, zum Teil sehr brauchbare Zusatzprogramme mit von der Partie: Neben den schon erwähnten Programmen Internet Explorer 7 und Windows Mail findet sich auch der **Media Player** mit der nächst höheren Versionsnummer 11 im Lieferumfang von Vista. **MovieMaker** und **Paint** sind ebenfalls enthalten. Neu hinzugekommen ist der **Windows Calendar**, mit dem sich Termine und Aufgaben planen lassen und der auch im Internet publiziert werden kann, um KollegInnen, FreundInnen und Verwandten die Terminkoordination zu erleichtern. Mittels **Windows Contacts** lassen sich bequem Adressinformationen von einzelnen Personen wie auch Firmendaten verwalten. Dieses Tool wird auch von Windows Mail als Adressbuch genützt und ermöglicht somit den Zugriff auf gespeicherte Kontaktdaten – mit dem Vorteil, dass die doppelte Adresswartung wegfällt. Unter *Accessories* finden sich noch einige weitere nützliche Zusatzprogramme, beispielsweise die Möglichkeit DVDs zu brennen.

Mit der **Windows Photo Gallery** trägt Microsoft der zunehmenden Beliebtheit digitaler Medien Rechnung. Die Photo Gallery zeigt gespeicherte Bilder und Videos (nach dem Datum der Aufnahme sortiert) übersichtlich an und ermöglicht es, die Metadaten derselben zu bearbeiten. Mit Hilfe von Assistenten wird das korrekte Drucken und Versenden von Bildern per eMail zum Kinderspiel, und auch eine vereinfachte Bearbeitungsmöglichkeit für Bilder steht hier zur Verfügung.

Neu ist auch das **Sync Center**, ein Tool, welches den einfachen Datenabgleich zwischen verschiedenen Geräten ermöglicht. Im Vordergrund steht hierbei die Synchronisation mit mobilen Endgeräten wie Telefonen oder PDAs – wobei Microsoft schon jetzt darauf hinweist, dass die bei diversen mobilen Geräten mitgelieferten Synchronisationstools mitunter besser funktionieren als sein Sync Center.

Mit dem **Ease of Access Center** – was wohl wieder mit „Eingabehilfen" übersetzt werden wird – lässt sich unter anderem ein Narrator aktivieren, dessen Funktion darin besteht, vorzulesen, was auf dem Bildschirm zu sehen ist, wenn man mittels Tastatur navigiert. Nach Auswahl einer Stimme – derzeit steht nur eine Dame mit dem Vornamen *Anna* und dem Nachnamen *Microsoft* zur Verfügung – geht's auch schon los. Sobald man mit der Tastatur arbeitet, sieht man nicht nur, was man angerichtet hat, sondern hört es auch noch: Anna gibt dezentes *„Delete"* von sich und schon ist die Datei futsch – gelöscht! Als weitere Hilfestellungen für AnwenderInnen mit körperlichen Einschränkungen bietet dieser Bereich ein Vergrößerungstool, mit dem Bildschirmbereiche vergrößert dargestellt werden können, und eine Bildschirmtastatur, die mittels Maus zu bedienen ist.

Zu erwähnen ist weiters noch die **BitLocker Drive Encryption**, ein neues Sicherheitsfeature, das vor allem Notebook-BesitzerInnen interessieren wird: Es soll bewirken, dass im Falle eines Diebstahls weder vertrauliche Daten noch das Betriebssystem des Rechners missbraucht werden können. Allerdings scheitere ich hier bereits bei den Grundvoraussetzungen, denn ich kann meine Festplatte mangels geeigneter Software nicht partitionieren. BitLocker Drive Encryption benötigt jedoch zumindest zwei Partitionen: Auf der einen Partition befindet sich das Betriebssystem, das via BitLocker verschlüsselt werden soll; die zweite Partition muss unverschlüsselt bleiben, damit der Computer überhaupt hochgefahren werden kann. Im Gegensatz zu den vorangegangenen Beta-Versionen bietet das integrierte Hilfsprogramm aber jetzt die nötigen Informationen, wie man mit dem BitLocker-Verschlüsselungssystem umzugehen hat, damit es wie gewünscht funktioniert.

Superfetch

Laut Microsoft-Produktbeschreibung verbirgt sich hinter der **Superfetch**-Funktion die Möglichkeit, ungenutzte Bereiche des Arbeitsspeichers als Cache für Programme und Dateien zu verwenden (*Caching* bedeutet, dass oft benötigte Daten auf einem schnelleren Medium „zwischengelagert" werden, damit sie rascher abgerufen werden können). Dadurch sollen die vergleichsweise langsamen Festplattenzugriffe minimiert werden. Auch USB-Sticks können zum Cachen der Programme genutzt werden, was natürlich getestet werden muss. Ich stecke also einen USB-Stick an. Das *Autostart*-Fenster bietet daraufhin – wie von Windows XP gewohnt – an, diesen als externen Datenträger zu verwenden, zeigt aber auch noch einen neuen Eintrag: *Speed up your system*. Klickt man darauf, so landet man im Dialogfenster *Properties* und kann dort zusätzlichen Speicher freigeben, was die Performance deutlich verbessern soll.

Aber egal welche Speicherkapazität der USB-Stick aufweist, mehr als 110 MB für die Systembeschleunigung werden – so scheint es – nicht akzeptiert. Es soll auch nicht verschwiegen werden, dass in meinen Tests mehrere Versuche mit einer Vielzahl von USB-Sticks nötig sind, bis die Systembeschleunigung überhaupt funktioniert. Von zu wenig freiem Speicher auf dem USB-Stick (obwohl es laut Beschreibung

bereits ab 64 MB funktionieren sollte und ausreichend Platz vorhanden ist) bis hin zur fehlenden Registerkarte, um die erforderlichen Einstellungen zu treffen, reichen die Steine, die mir Windows Vista in den Weg legt. Aber gut Ding braucht eben Weile: Letztendlich funktioniert es doch, und ich darf Vista anweisen, einen Teil des Speichers des USB-Sticks für das Auslagern von Dateien zu nutzen und damit den Systemspeicher zu erweitern.

Gesucht – Gefunden?

Wie habe ich diese Datei nur benannt und wo zum Teufel habe ich sie hingespeichert? Geht es nach Microsoft, soll ich mir nie wieder diese Frage stellen müssen – und wenn doch, gibt es eine rasche Antwort mit Hilfe der neu konzipierten Suchfunktionalität. Neuerdings reicht es durchaus, sich nur noch eine dateibezogene Information zu merken (z.B. ein Schlüsselwort, einen Teil des Dateinamens oder das Datum, an dem ein Foto gemacht wurde). Einzugeben ist der Suchbegriff in die neuen Desktop-Suchfunktionen, und wie es richtig heißt, findet sich nahezu alles auf dem Computer wieder. Hier wurde im Vergleich zu den vorangegangenen Beta-Versionen Entscheidendes verbessert, denn mittlerweile erhalte ich tatsächlich ein Suchergebnis. Während eine in der Beta-Version 5308 mittels Notepad erstellte Datei (abgespeichert unter *Documents*, also beileibe kein exotischer Aufbewahrungsort) nicht mehr gefunden werden konnte, wartet die Beta 2 Build 5384 mit einem prompten Suchergebnis auf. Egal ob ich mit dem Dateinamen, einem Teil des Inhalts oder der Dateierweiterung suche: Das Ergebnis wird in allen Fällen sofort geliefert, wobei ich vor Suchbeginn noch definieren muss, ob im Internet oder auf dem Computer nach dem Begriff gefahndet werden soll. Auch mit den mitgelieferten Beispielbildern funktioniert es wie am Schnürchen: Eingabe der Dateierweiterung `jpg`, Klick auf die Option *Search the computer* – schon erhalte ich eine Liste aller JPG-Dateien, die sich auf dem Rechner befinden, mitsamt ihren Speicherorten und sonstigen Details.

Während meiner Such-Odysee stoße ich auch auf die neue Funktion, so genannte *Searches* zu definieren. Hinter diesem Begriff verbirgt sich schlicht und einfach ein gespeicherter Suchvorgang, der durch Öffnen der jeweiligen *Searches* unmittelbar ausgeführt wird. Auch dieses Feature funktioniert reibungslos und ist allen AnwenderInnen ans Herz zu legen, die immer wieder dieselben Suchanfragen an das Computersystem stellen (müssen).

Shut down

Erstaunlich, wie schnell Wünsche in Erfüllung gehen können: Beim ersten Testdurchgang mit der Windows Vista Beta 5308 scheiterte ich daran, den PC ordnungsgemäß herunterzufahren – hinter dem vermeintlichen Aus-Schalter verbarg sich der neue Betriebsmodus, der sich *Sleep* nennt, und ich wartete daher vergeblich darauf, dass der PC herunterfährt. Um das zu erreichen, musste ich mich in das Untermenü begeben und dort den Befehl *Shut Down* auswählen. Damals dachte ich mir im Stillen, dass Microsoft zumindest ein Gadget hierfür implementieren könnte, denn drei Klicks zum Ausschalten tragen nicht gerade zum erhöhten Bedienungskomfort bei. Aber siehe da – in der neuen Beta 2 Build 5384 ist der Aus-Schalter wieder an der gewohnten Stelle, mit einem Klick über das Start menu erreichbar und fährt den PC prompt herunter.

Darf's ein bisschen mehr sein?

Damit die BenutzerInnen mit Jahresbeginn 2007 nicht vollkommen verwirrt im Geschäft und ratlos vor der Qual der Wahl stehen, welche Vista-Version die für sie am besten geeignete ist, hat Microsoft bereits im Februar 2006 via Pressebericht verlautbart, dass Windows Vista in mehreren Versionen auf den Markt kommen wird. Private AnwenderInnen können zwischen drei Versionen wählen: Windows Vista Home Basic, Windows Vista Home Premium und Windows Vista Ultimate. Zwei Versionen sind für Unternehmen gedacht: Windows Vista Business und Windows Vista Enterprise. Der Unterschied liegt vor allem im Funktionsumfang – die Basisprodukte enthalten deutlich weniger Features. Wer sich detaillierter damit auseinandersetzen möchte, sei auf die Microsoft Homepage verwiesen: Unter dem URL `www.microsoft.com/germany/presseservice/service/pressemappen/windows-vista.mspx` findet sich dort im Artikel *Microsoft präsentiert Editionen für Windows Vista (27.02.2006)* alles Wissenswerte.

Fazit

Obwohl Geschmäcker bekanntlich ja verschieden sind, kann das optische Erscheinungsbild der Windows Vista Beta 2 Build 5384 im Vergleich zum Teletubbie-Outfit von Windows XP durchaus als gelungen bezeichnet werden (all diejenigen, die sich dieser Meinung nicht anschließen können oder möchten, haben nach wie vor die Möglichkeit, zur altbewährten klassischen Ansicht zu wechseln). Die integrierten Applikationen zeichnen sich durch Übersichtlichkeit und erhöhten Bedienkomfort aus, der vor allem durch wirksame Hilfestellungen bzw. Querverlinkungen zu weiterführenden Applikationen erzielt wird. Und im Vergleich zur vorhergehenden Beta Build 5308 ist die nunmehr getestete Version nicht nur *Feature-complete*, sondern die Features funktionieren auch im Großen und Ganzen wie erwartet. Microsoft hat zwischenzeitlich sichtlich einiges an Arbeit geleistet, wobei mich die vielgerühmten Sicherheitsfunktionen noch nicht wirklich überzeugen. Da gilt es, noch an dem einen oder anderen Feature Hand anzulegen, denn schließlich will Microsoft mit Vista doch die bislang sicherste Windows-Version verkaufen. Gerade in diesem Bereich gibt es allerdings noch einiges zu überdenken, will man „Otto Normalverbraucher" nicht mit allzu vielen, zum Teil sehr komplexen Sicherheitsoptionen überfordern. Aber die nächste Betaversion kommt bestimmt – *Hasta la vista!*

Eva Birnbacher ■

SCHRÖDINGER-NEWS

Offiziell ist das Supercomputer-Projekt „Schrödinger“ seit der letzten Ausbaustufe (siehe *Comment 05/2*; `www.univie.ac.at/comment/05-2/052_20.html`) beendet. Dennoch gibt es laufend kleinere Ausbauten:

- Viele Applikationen, z.B. Gaussian 03, haben praktisch unbeschränkten Bedarf an Hauptspeicher. Daher wurden 16 Knoten mit 4 GB (statt 2 GB) Hauptspeicher ausgerüstet. Für diese Knoten wurde eine eigene Batch-Queue `bigmem` eingerichtet, in der Paralleljobs maximal vier Knoten verwenden können.

- Es ist nicht einfach, die Ressourcen gerecht aufzuteilen und einen Scheduling-Algorithmus zu finden, der allen Anforderungen gerecht wird. Da es bei Paralleljobs manchmal zu unakzeptabel langen Wartezeiten kam, wurde dafür die Batch-Queue `parallel` eingerichtet, für die 64 Knoten reserviert sind.

- Die Software wird laufend aktualisiert und erweitert: GaussView 3.0 ist nun am Login-Server verfügbar, und folgende Pakete wurden auf den neuesten Stand gebracht: Gaussian 03 (Rev. D2), Matlab (R2006a), Portland Group Compiler (6.1) und die dazugehörige Parallelsoftware mpich (1.2.7p1).

Peter Marksteiner ■

Neue Standardsoftware

Neue Produkte (Stand: 1. Juni 2006)

- Adobe After Effects Prof. 7.0 für Win./Mac
- Adobe Audition 2.0 für Win.
- Adobe Encore DVD 2.0 für Win.
- Adobe Premiere Elements 2.0 für Win.
- Adobe Premiere Pro 2.0 für Win.
- IDL 6.2 für Win./Unix (Datenanalyse/-visualisierung)
- ProCite 5 für Win./Mac (Bibliographieprogramm)
- RedHat Linux Enterprise Server
- Reference Manager 11 für Win. (Bibliographieprogramm)
- RefViz 2.1 für Win./Mac (Textanalyse/-visualisierung)
- Roxio Toast 7 Titanium für Mac (CDs/DVDs brennen)
- SPSS 14 für Win.

Updates (Stand: 1. Juni 2006)

- MATLAB 7.2 R2006a für Win./Mac/Unix (bisher 7.0 R14)
- Apple Mac OS X 10.4.3 (bisher 10.4)

Alle Informationen zur Standardsoftware finden Sie unter `www.univie.ac.at/ZID/standardsoftware/`.

Peter Wienerroither

EINE FÜR ALLE, ALLES IN EINER:

Services und Projekte der Abteilung *PC-Systeme & Fakultätsunterstützung*

Als im Mai 2005 die Abteilung *PC-Systeme & Fakultätsunterstützung* durch Zusammenfassung mehrerer PC-orientierter Aufgabenbereiche des ZID gegründet wurde, war dies in erster Linie von einem tragischen Ereignis induziert,[1] die Idee hingegen, durch diese Zusammenlegung mögliche Synergien zu nutzen und die EDV-Unterstützung für die Fakultäten der Uni Wien neu zu gestalten, war bereits seit längerem gegenwärtig. Heute, ein Jahr später, umfasst die Abteilung folgende Tätigkeitsgebiete:

- die Entwicklung und Administration des EDV-Systems, das in den vom ZID betreuten PC-Räumen der Universität Wien zum Einsatz kommt,
- den Support in den PC-Räumen der Universitätsstandorte NIG/1. Stock, AAKH und UZA durch PC-RaumBetreuerInnen,
- die Entwicklung und den Support der Verwaltungs- und Instituts-PCs,
- die Support-Gruppe für Hardware und Kaufberatung,
- die Betreuung der für die genannten Dienste erforderlichen zentralen Server (Windows-Server und RedHat-Cluster) sowie
- den gesamten Bereich der Standardsoftware für Universitäts-MitarbeiterInnen.

Aus den genannten Bereichen ersieht man die Ausrichtung der Abteilung: Hier werden für den jeweiligen „Kundenkreis" (Studierende, MitarbeiterInnen, so genannte „Organisationseinheiten" von Fakultäten bis zu Arbeitsgruppen) speziell zugeschnittene Lösungen angeboten und dabei Entwicklungen und Support für die verschiedenen Bereiche eng miteinander verknüpft.

Fakultätsunterstützung

Die zentrale Herausforderung, der sich die Abteilung zu stellen hat, war und ist wohl die Reorganisation der Fakultätsunterstützung: Das Projekt Juridicum[2] zeigte ob seines Erfolges, dass in den Organisationseinheiten (kurz OE) der Uni Wien großes Interesse an einer zentralen Unterstützung der PC-Systeme durch den ZID besteht. Unabdingbare Voraussetzung für eine solche Unterstützung (diese umfasst im Wesentlichen das zentral gesteuerte Einspielen von Betriebssystem-Updates und neuesten Virendefinitionen sowie die Verfügbarkeit eines breit gefächerten Software-Angebots, das sich auf Wunsch der jeweiligen OE unter Berücksichtigung möglicher Lizenzpflichten auf den einzelnen PCs installieren lässt) sind Flexibilität in der Konfiguration sowie lokale Administrierbarkeit durch EDV-Verantwortliche und FakultätsbetreuerInnen.

Die bereits für das Projekt Juridicum erarbeiteten „Paradigmen" einer Fakultätsunterstützung (siehe Kasten *Anforderungen an ein Konzept zur Instituts-PC-Betreuung*) sind mittlerweile in einem neuen, vollständig vom ZID entwickelten, so genannten „Deployment-System" zur Ferninstallation und -wartung von PCs realisiert und um einige Aspekte erweitert worden, die teils unter Mitarbeit von BenutzerInnen und EDV-Verantwortlichen vorgeschlagen wurden bzw. sich als notwendige Erweiterungen erwiesen. So wird es unter anderem auch Deployments und Support

Anforderungen an ein Konzept zur Instituts-PC-Betreuung

Quelle: *Comment 05/1*, Seite 3
(www.univie.ac.at/comment/05-1/051_3.html)

- Zentrale Verteilung und Installation von Betriebssystemen, Security-Patches, Virenscanner-Updates und so genannter Standardsoftware durch den ZID;
- Implementierung eines Netzwerk-Sicherheitskonzepts (VLANs, Instituts-Firewalls, Datentankstellen für ungewartete Notebooks etc.), um den Security-Problemen der Vergangenheit entgegentreten zu können;
- Ablage der Dateien auf zentralen Fileservern (Samba) in selbst verwalteten Verzeichnissen, die entweder nur für den jeweiligen Benutzer persönlich zugänglich sind oder von Instituten bzw. Arbeitsgruppen gemeinsam genutzt werden können;
- lokale Administrierbarkeit der PCs durch die EDV-Verantwortlichen der Institute und die EDV-Beauftragten der Fakultät, da im universitären Alltag zusätzlich zur Basis-Konfiguration oft verschiedenste Programme installiert und deinstalliert werden müssen, was im Zeitrahmen einer zentral organisierten Wartung nicht möglich ist.

1) siehe *Personalnachrichten* in *Comment 05/2*, Seite 3 bzw. unter www.univie.ac.at/comment/05-2/052_3.html

2) siehe Artikel *Anmerkungen zur EDV-Sanierung des Juridicums* in *Comment 05/1*, Seite 3 bzw. unter www.univie.ac.at/comment/05-1/051_3.html

für Mac OS und Linux geben, die freilich personell an der realen Verteilung dieser Systeme in den Organisationseinheiten orientiert bleiben müssen.

PC-Deployment

Nach erfolgreicher Initiierung an der Rechtswissenschaftlichen Fakultät (und weiteren Installationen an den Fakultäten für Physik und für Philosophie, in Hörsälen, in der Universitätsverwaltung, am ZID und in einigen kleineren Bereichen) kann das PC-Deployment nun also für die gesamte Universität Wien angeboten werden. Seit Mitte Mai dieses Jahres laufen weitere Umstellungen an, die von den FakultätsbetreuerInnen und den EDV-Verantwortlichen vorbereitet sein müssen.

Diese Umstellungen erfolgen nach der Reihung, die sich aus den Vereinbarungen der jeweiligen Fakultäten mit dem Rektorat ergeben haben. Die früheren Leistungen der Außenstellen des ZID werden damit in skalierbarer, nachvollziehbarer und kommunizierter Form allen Bereichen der Universität zugänglich und damit deutlich effizienter, die Unterstützung damit auch transparenter für die Organisationseinheiten.

Unbedingte Voraussetzungen, um in den Genuss der Fakultätsunterstützung zu kommen, sind:

- Die Benennung eines ***EDV-Verantwortlichen*** durch die Organisationseinheit, der in Übereinkunft mit deren LeiterIn „politische", vom ZID unbeantwortbare Entscheidungen fällt (z.B. *Wer darf sich an welchem PC einloggen? Wer hat welche Zugriffe auf Verzeichnisse am Instituts-Share?*) sowie

- die Benennung eines ***Technical Staff*** (z.B. Fakultätsbetreuer), der den Vollzug des Deployments vor Ort überwacht, mögliche Problemlagen analysiert und die lokale Administration übernimmt. Letzteres umfasst
  - das Initiieren von Garantieabwicklungen durch Hersteller bei Hardware-Defekten,
  - das Aufstellen neuer Geräte und
  - die Installation oder das Skripten von Spezial-Software, die nicht vom ZID zentral eingespielt werden kann.

Im Falle von Zweifeln bei der Beurteilung von Hardware-Problemen steht den Fakultäten der neu geschaffene *Service Desk Hardware* des ZID zur Seite, der auch bei Fragen zu Neuanschaffungen von PCs, Notebooks, Monitoren und Druckern konsultiert werden kann (siehe `www.univie.ac.at/ZID/hardware/`).

Die Arbeitsgruppe Fakultätsunterstützung des ZID und die FakultätsbetreuerInnen, die den jeweiligen Fakultäten unterstellt bleiben, bilden ein kommunikatives Netzwerk, das die Entwicklung des Systems im Sinne der BenutzerInnen vorantreibt. Ein genaues Verständnis des Deployment-Systems ist dafür unerlässlich, deshalb müssen bereits auf dem Anmeldeformular zum PC-Deployment (erhältlich unter `www.univie.ac.at/ZID/formulare/#fu`) die entsprechenden Verantwortlichen der OE namentlich genannt werden.

Groupware-Service

Zusätzlich zu (und unabhängig von) der Ferninstallation und -wartung der PCs bietet die Fakultätsunterstützung des ZID den Organisationseinheiten der Universität Wien die Verwendung einer Groupware an. Diese Groupware (MS-Exchange) ermöglicht die Nutzung gemeinsam verwalteter Kalender, Aufgaben, Notizen, Adressen oder beliebiger Ressourcen und erlaubt via MS-Outlook die einfache Synchronisation mit einer Vielzahl von Handhelds. Der Zugriff auf die Groupware ist via OWA (*Outlook Web Access*) von allen Betriebssystemen aus möglich. Mit Evolution steht zudem ein leistungsstarker eMail-Client unter Linux zur Verfügung, der problemlos mit dem Exchange-Cluster zu „sprechen" vermag.

Diese Groupware-Lösung ist per definitionem (*group*) nur Organisationseinheiten zugänglich und nicht einzelnen BenutzerInnen, da sie kein (!) Ersatz für das zentrale Mailing ist und an dieses vollständig gekoppelt bleibt. Das bedeutet auch, dass die Nutzung der Groupware keinen Einfluss auf die Geschwindigkeit der Mailzustellung hat, und auch die Spam-Problematik bleibt weiterhin die des zentralen Mailings (siehe dazu auch den Artikel *Wenn der Postmann zweimal klingelt* auf Seite 13).

Die Fakultätsunterstützung stellt jeder Organisationseinheit auf Wunsch einen eigenen Exchange-Bereich zur Verfügung. Die Rechtestruktur innerhalb von Exchange (*Wer darf welche Daten einsehen oder ändern?*) wird dabei ausschließlich von der OE selbst verwaltet; der ZID nimmt hierauf keinen Einfluss. Das Anmeldeformular zum Groupware-Service finden Sie ebenfalls unter `www.univie.ac.at/ZID/formulare/#fu` (Groupware-Service und PC-Deployment können getrennt voneinander bezogen werden).

Software-Projekte

Neben dem Schwerpunkt „Aufbau einer effektiven, kollaborativen Fakultätsunterstützung" verfolgt die neue Abteilung derzeit auch noch andere Projekte. Darunter fällt die **Reorganisation des Software-Bestellwesens**, das in eine Art elektronischen Warenkorb umgewandelt werden soll. Der jeweiligen Organisationseinheit wird es dann möglich sein, auch online die Lizenzzahlen, die Ablaufdaten von Mietlizenzen sowie die Verteilung der Software innerhalb der OE abzufragen. Bei Ausscheiden von MitarbeiterInnen kann die Organisationseinheit deren Lizenzen in einem Pool „zwischenparken" und bei Bedarf an andere MitarbeiterInnen vergeben. Zudem werden die Lizenzbedingungen übersichtlich zusammengefasst sein. Mit der Konsolidierung im Storage-Bereich wird das gesamte am Software-Distributionsserver notierte Software-Sortiment so-

wohl als ISO-Images zum Selbstbrennen als auch als Installations-Images für das PC-Deployment verfügbar gemacht werden.

In einem weiteren Projekt versuchen wir, günstige Konditionen für **Studenten-Software** zu verhandeln. Die besondere Schwierigkeit an der Uni Wien liegt hier zum einen an der großen Zahl von Studierenden, die Campus-Verträge für Studierende zumeist unfinanzierbar macht, und zum anderen an der (im Gegensatz zu einer Technischen Universität) hohen Diversifikation der Fachrichtungen, die einem einigermaßen einheitlichen Portfolio zuwiderläuft. Sollten wir trotz dieser Hürden zu einem positiven Abschluss und einem ansprechenden Portfolio gelangen, werden wir einen geeigneten Distributionsweg finden, um die Software den Studierenden zur Verfügung zu stellen.

Über die Fortschritte dieser und anderer Projekte werden wir in den nächsten Ausgaben des *Comment* informieren.

Christian Marzluf ■

Fakultätsunterstützung – Hilfe & Kontakt

- Allgemeine **Informationen zur Fakultätsunterstützung** (kurz FU) sowie einen Überblick über das umfangreiche Software-Portfolio finden Sie unter:

  www.univie.ac.at/ZID/fu/

- Etliche EDV-Verantwortliche und/oder FakultätsbetreuerInnen haben sich das Deployment-System des ZID auf eigenen Wunsch hin bereits vorführen lassen, um die Vorarbeiten für die Umstellungen beschleunigen zu können. Falls auch Sie eine **Präsentation des PC-Deployments** wünschen, setzen Sie sich bitte mit uns in Verbindung:

  Christian Marzluf, Tel.: 4277-141 20, eMail: christian.marzluf@univie.ac.at

- Das so genannte ***Organon*** (die Verwaltungs- und Informationswebseite für PCs, die bereits im Deployment erfasst sind) finden Sie unter:

  https://organon.univie.ac.at/

  Sie können dort – nach Eingabe Ihrer Mailbox-UserID und Ihres Mailbox-Passworts – jederzeit Einblick in die zu Ihrem PC erfassten Daten nehmen. Den EDV-Verantwortlichen und den FakultätsbetreuerInnen dient diese Webseite zum Verwalten der ihrem Bereich zugeordneten PCs, Netzwerkdrucker und BenutzerInnen (Viren- und Updatekontrolle, Zuweisen von Druckern sowie zentralen und lokalen BenutzerInnen, Verwalten von File-Shares, Zugriff auf Exchange-Services etc.).

- Über den ***ZID-Agent***, der im *Systemtray* (das ist der Infobereich rechts unten in der Windows-Taskleiste) installiert ist, erfahren Sie, falls Probleme mit zentralen Services oder lokale Problemlagen einen nicht vollständigen Betrieb bedingen. Der ZID-Agent informiert Sie auch über anstehende Updates oder neue Softwarepakete.

- Die Fakultätsunterstützung des Zentralen Informatikdienstes ist **Montag – Freitag von 08:00 – 18:00 Uhr** unter der Telefonnummer **4277-141 40** für Sie erreichbar. Denken Sie aber bitte daran, dass der Weg zur Problemlösung in der Regel zuerst über Ihren zuständigen EDV-Verantwortlichen oder Fakultätsbetreuer und nur bei dessen Nichtverfügbarkeit oder bei Unlösbarkeit des Problems über die Fakultätsunterstützung des ZID führen sollte.

  Eine Kontrolle über Ihre Anfrage erhalten Sie am besten, wenn Sie diese via eMail an **fu.zid@univie.ac.at** senden. Sie erhalten unmittelbar nach Versenden der Nachricht eine Bestätigung vom Ticketsystem des ZID und können über den an Sie zurückgesandten Link die Bearbeitung Ihrer Anfrage verfolgen.

Bei allgemeinen Anfragen wenden Sie sich bitte direkt an den Helpdesk des Zentralen Informatikdienstes (siehe www.univie.ac.at/ZID/helpdesk/).

An Anfragen, Vorschlägen, Anregungen und Kritik zu den einzelnen Projekten der Fakultätsunterstützung ist uns sehr gelegen. Bitte nutzen Sie dazu die unter www.univie.ac.at/ZID/staff/ veröffentlichten eMail-Adressen der jeweiligen Teilbereiche.

UNIorientiert:
Ganz und gar nicht orientierungslos

Wie schon im Vorjahr beteiligte sich der Zentrale Informatikdienst auch heuer wieder an der von *Student Point* organisierten Beratungs- und Informationswoche *UNIorientiert* (siehe `www.univie.ac.at/bologna-lab/uniorientiert/`). Im Rahmen dieser Veranstaltung wurde StudieninteressentInnen die Möglichkeit geboten, sich bereits vorab über das umfangreiche Studien- und Serviceangebot der Universität Wien zu informieren. Die Veranstaltungsreihe stieß dabei auch dieses Jahr wieder auf positive Resonanz bei den potentiellen StudienkandidatInnen.

Ratsuchende konnten sich am Informationsstand des ZID ausführlich über die EDV-Services der Universität Wien informieren sowie technische Fragen stellen (siehe Foto). Zudem gab es für sie jede Menge Infomaterialien und natürlich eine Gratisausgabe unserer Zeitschrift *Comment*. Neben diesem Beratungsangebot veranstaltete der Zentrale Informatikdienst am ersten Tag der Veranstaltungsreihe einen Workshop, der den angehenden Studierenden Gelegenheit bot, in die diversen Services auch gleich praktisch „hineinzuschnuppern". Inhalte des Workshops waren u.a. die Anmeldung zum Unet-Service, ein Überblick über die Einrichtungen und Servicestellen des ZID sowie über die wichtigsten EDV-Services (eMail, Webspace, Fileservices, PC-Räume, vergünstigter Internetzugang von daheim, …) und Informationssysteme (*UNIVIS online*, Account-Info, …) für Studierende. Im Rahmen der Veranstaltung standen den TeilnehmerInnen auch PCs zur Verfügung, um sich aktiv am Workshop zu beteiligen. Zudem bot der kleine aber feine TeilnehmerInnenkreis optimale Bedingungen für eine persönliche Betreuung durch die Vortragenden.

Michaela Bociurko ■

***UNIorientiert*: Beratungsgespräch am Infostand des ZID**

Personalnachrichten

Auch in dieser *Comment*-Ausgabe ist wieder über etliche Veränderungen in unserem Personalstand zu berichten: Unserem langjährigen Datenbank-Administrator **Lukas Ertl** ist trotz seiner wichtigen Aufgaben am ZID die Einberufung zum Zivildienst nicht erspart geblieben, und so wird er ab Juli 2006 statt am ZID bei einer steirischen Feuerwehr ausrücken, wenn es wo brennt. Um die Administration unserer Oracle-Datenbanken wird sich an seiner Stelle ein alter Bekannter kümmern: **Robert Brunnthaler**, der bereits von 1998 bis 2001 am ZID angestellt war, kehrt nach fünf Jahren einschlägiger Tätigkeiten in einem anderen großen Rechenzentrum wieder an den ZID zurück. Auch in unserem eLearning-Team verlieren wir eine wichtige Mitarbeiterin, die drei Jahre lang entscheidend zum Aufbau der eLearning-Services an der Uni Wien beigetragen hat: **Birgit Zens** hat ein attraktives Angebot als Wissenschaftlerin an der Donau-Universität Krems angenommen und verlässt uns mit Ende Juni 2006. Herzlichen Dank für die gute Arbeit am ZID!

Im Referat *UNIVIS-Produktionsbetrieb* unserer Abteilung *Universitätsverwaltung*, dessen Leiter Dejan Vidovic kürzlich den ZID verlassen hat, wurde mit Juni 2006 **Martin Huxhold** als neuer Mitarbeiter aufgenommen; im Referat *Projekt- und Changemanagement* verstärkt **Karin Englhart** seit Mitte Juni 2006 unser Analytiker-Team. In der Abteilung *PC-Systeme & Fakultätsunterstützung* freuen wir uns seit Mitte April 2006 über die Mitarbeit von **Tibor Rudas**, der davor etliche Jahre lang die Computersysteme am Institut für Biomolekulare Strukturchemie betreut hat.

Gerade rechtzeitig, um noch tatkräftig bei der Erneuerung unserer Klimaanlage im NIG mitarbeiten zu können, wurde Mitte März 2006 **Eva Rubasch** in der Abteilung *Datennetze & Infrastruktur* angestellt. Die Aufgaben im Bereich des Vienna Internet eXchange, die durch den Tod von **Hilde Gruber** so plötzlich verwaist waren, übernimmt seit Juni 2006 **Tina Stadlmann**, die Schwester von Uwe Stadlmann, dem langjährigen Systembetreuer unserer Bibliotheks-Services. Da dürfen auch wir als seine Kolleginnen und Kollegen mit Befriedigung die Vermutung anstellen, dass der große Bruder im Familienkreis immer nur das Allerbeste über seinen Arbeitsplatz am ZID berichtet hat.

Zwei Mitarbeiterinnen haben innerhalb des ZID neue Aufgaben übernommen: **Susanne Kriszta** ist Ende März 2006 vom Helpdesk in das Referat *IT-Security* übersiedelt, und **Christine Dworak** wechselt nach dem erfolgreichen Abschluss ihres Fachhochschul-Studiums von ihrem Praktikums-Arbeitsplatz im Referat *Datenleitungs-Infrastruktur* in das Referat *ACOnet & VIX*.

Last but not least müssen wir uns bei unserer Direktionssekretärin **Claudia Eitler-Buchner** seit ihrer Hochzeit nicht nur an den Doppelnamen gewöhnen, sondern auch an ihre Abwesenheit während der nächsten Monate: Mitte Mai 2006 hat sie ihre Mutterschutz-Karenz angetreten. Wir wünschen ihr und ihrer Familie alles Gute! Aber auch allen anderen ZID-Mitarbeiterinnen und -Mitarbeitern wünschen wir das Beste für ihre Zukunft, vor allem viel Freude und Erfolg mit ihren jeweiligen neuen Tätigkeiten!

Peter Rastl ■

UNIVIS: ANMELDESYSTEME
PILOTEN IST NICHTS VERBOTEN

Im letzten *Comment*-Artikel zum Thema UNIVIS[1)] wurde bereits kurz über Arbeiten an einem Prototyp eines Lehrveranstaltungs-Anmeldesystems für die Studienrichtung Politikwissenschaft berichtet. Der im Rahmen dieses *Pilotprojekts Politikwissenschaft* entwickelte Prototyp ist mittlerweile seit zwei Semestern im Einsatz – Zeit also für ein Resümee.

Wie es in diesem Bereich zu einem – für das Projekt UNIVIS durchaus untypischen – Verzug von mittlerweile mehreren Jahren gekommen ist, warum man sich für die – ebenfalls untypische – Durchführung eines Pilotprojekts ohne vorherige breit angelegte Planung und Entscheidungsfindung entschieden hat und was das Thema *Lehrveranstaltungs-Anmeldesysteme* ausreichend komplex macht, um eine universitätsweite Lösung nachhaltig zu verzögern, obwohl doch vermeintlich schon der Begriff allein den Leistungsumfang eines solchen Systems recht umfassend beschreibt – auch diesen Fragen soll im Rahmen dieses Artikels nachgegangen werden.

Lehr- und Prüfungsverwaltung in UNIVIS

Die Einführung eines Anmeldesystems für Lehrveranstaltungen und Prüfungen ist im Rahmen des Projektes UNIVIS im Teilprojekt Studienwesen angesiedelt.[2)] In diesem Teilprojekt werden die Bereiche Studierendenverwaltung, Lehrverwaltung und Prüfungsverwaltung unterschieden. Während die Studierendenverwaltung und die Lehrverwaltung weitgehend planmäßig in Betrieb genommen werden konnten, zeichneten sich bei der Prüfungsverwaltung bald Probleme ab, die die Aufspaltung in zwei Teilbereiche erforderlich machten, nämlich die *Prüfungsergebnisverwaltung* einerseits und die *umfassende Prüfungsverwaltung* andererseits.

Im Rahmen der Prüfungsergebnisverwaltung wurden mit hoher Priorität jene Funktionen umgesetzt, die zur Erfüllung des gesetzlichen Auftrags rasch benötigt wurden, also im Wesentlichen eine zentrale Prüfungsevidenz mit angeschlossenen Funktionen (z.B. Zeugnisausfertigung). Die darüber hinausgehenden Funktionen wurden in der umfassenden Prüfungsverwaltung zusammengefasst – und aus Zeitgründen auf später verschoben.

Der gesamte Bereich Anmeldesysteme (inklusive Lehrveranstaltungs-Anmeldesysteme) wurde der umfassenden Prüfungsverwaltung zugerechnet. Diese auf den ersten Blick widersprüchliche Zuordnung ist bei einer näheren Betrachtung eher verständlich: Es ist prinzipiell zu unterscheiden zwischen Anmeldungen zu Lehrveranstaltungen und Anmeldungen zu Prüfungen. Bei den Lehrveranstaltungen ist weiters zu unterscheiden zwischen

- Lehrveranstaltungen **mit** immanentem Prüfungscharakter (auch *prüfungsimmanente Lehrveranstaltungen* genannt): Bei diesen Lehrveranstaltungen (z.B. Übungen, Proseminare) erfolgt die Beurteilung während der gesamten Dauer der Lehrveranstaltung. Die Anmeldung zur Lehrveranstaltung ist daher zugleich auch die Anmeldung zur Prüfung.

- Lehrveranstaltungen **ohne** immanenten Prüfungscharakter: Bei diesen Lehrveranstaltungen (z.B. Vorlesungen) erfolgt die Beurteilung im Rahmen eines eigenständigen Prüfungsaktes, in der Regel am Ende des Semesters und in weiteren Prüfungsterminen danach. Zusätzlich zur Anmeldung zur Lehrveranstaltung (sofern eine solche vorgesehen ist), wird eine gesonderte Anmeldung zu einem der Prüfungstermine erforderlich sein, zumal ja mit der Teilnahme an der Lehrveranstaltung noch keine Verpflichtung zur Ablegung der entsprechenden Prüfung entsteht.

Prüfungsimmanente Lehrveranstaltungen haben im Normalfall eine beschränkte TeilnehmerInnenzahl, und dies führt – vor allem dann, wenn die Nachfrage größer ist als das Angebot – zumeist unmittelbar zur Notwendigkeit einer „Anmeldung" im weitesten Sinne. Bei entsprechend großen Studierendenzahlen wird eine Anmeldung durch persönliches Vorsprechen oder handschriftliches Eintragen in einer Liste nicht mehr administrierbar sein, und ein EDV-unterstütztes Anmeldesystem wird erforderlich. Der Hauptbeweggrund für die Einführung eines Lehrveranstaltungs-Anmeldesystems ist somit die Verteilung der beschränkt verfügbaren Plätze in prüfungsimmanenten Lehrveranstaltungen.

Ein weiterer Umstand intensiviert den Zusammenhang zwischen Lehrveranstaltungsanmeldung und Prüfungsverwaltung: Neben dem beschränkten Platzangebot sind bei der Anmeldung zu Lehrveranstaltungen auch studienrechtliche Rahmenbedingungen zu beachten. Im *Curriculum* (vor dem UG2002: *Studienplan*) kann festgelegt werden, dass für die Teilnahme an einer Lehrveranstaltung bestimmte Voraussetzungen (z.B. die positive Absolvierung von Prüfungen) zu erfüllen sind (§ 54(7) UG2002). Wenn ein Anmeldesystem derartige Nebenbedingungen prüfen soll, so

1) siehe *Comment 05/2*, Seite 10 bzw. unter `www.univie.ac.at/comment/05-2/052_10.html`

2) siehe *Comment 04/3*, Seite 4 bzw. unter `www.univie.ac.at/comment/04-3/043_4.html`

ist das jeweilige Curriculum im System in geeigneter Weise abzubilden. Eine entsprechende Curriculum-Verwaltung ist eines der Ziele der umfassenden Prüfungsverwaltung.

Ein Problem – viele Lösungen

Die Erfahrungen im Projekt UNIVIS haben gezeigt, dass die universitätsweit einheitliche Unterstützung von Abläufen durch Informationstechnologie dann vergleichsweise reibungslos umgesetzt werden kann, wenn zumindest einer der folgenden Umstände zutrifft:

- Der Ablauf ist durch gesetzliche Vorgaben relativ genau geregelt.
- Der Ablauf wird von einer zentralen Stelle der Universität durchgeführt oder zumindest koordiniert und damit an der gesamten Universität weitgehend einheitlich abgewickelt.
- Der Ablauf wird bereits durch ein zumindest in weiten Teilen der Universität eingesetztes System unterstützt, das somit den kleinsten gemeinsamen Nenner der unter Umständen unterschiedlichen Ansprüche darstellt und als Basis für eine Neuentwicklung geeignet ist.

Leider trifft für den Bereich Anmeldesysteme keiner dieser Umstände zu. Die entsprechende gesetzliche Regelung findet sich im § 54(8) UG2002:

> *Im Curriculum ist für Lehrveranstaltungen mit einer beschränkten Zahl von Teilnehmerinnen und Teilnehmern die Anzahl der möglichen Teilnehmerinnen und Teilnehmer sowie das Verfahren zur Vergabe der Plätze festzulegen. Dabei ist zu beachten, dass den bei einer Anmeldung zurückgestellten Studierenden daraus keine Verlängerung der Studienzeit erwächst.*

Es hat sich herausgestellt, dass der zweite Teil dieser Regelung zwar schwierig zu erfüllen ist, aber insgesamt kaum konkrete Hinweise enthalten sind, wie dies zu bewerkstelligen sei. Die Anmeldung zu Lehrveranstaltungen (und Prüfungen) wird an der Uni Wien weder zentral abgewickelt noch koordiniert, und es gibt auch keine universitätsweit einheitlichen Vorgaben. Der massiv vorhandene Bedarf an Anmeldesystemen in Verbindung mit dem Fehlen eines zentralen Serviceangebots hat daher seit etwa 1985 zur Entwicklung von zahlreichen individuellen Anmeldesystemen geführt, die von Fakultäten, Instituten und mitunter einzelnen LehrveranstaltungsleiterInnen betrieben wurden und werden. Der *Student Point* führt eine Liste von Anmeldesystemen unter `http://studentpoint.univie.ac.at/index.php?id=325`; der dort enthaltene Aufruf, neu entdeckte Anmeldesysteme doch bitte der Redaktion zu melden, verdeutlicht die Situation recht plastisch.

Abgesehen vom Funktionsumfang und dem äußeren Erscheinungsbild unterscheiden sich die bestehenden Anmeldesysteme vor allem hinsichtlich der Vorgangsweise bei der Vergabe der Plätze. Im Wesentlichen sind hier drei Varianten zu unterscheiden:

- Vergabe der Plätze **in der Reihenfolge der Anmeldung**: Diese Strategie simuliert die früher übliche Warteschlange. Neben der Grundidee wurde dabei auch die überdurchschnittlich häufige mediale Präsenz aufgrund der mitunter unerfreulichen Begleitumstände (menschliche Zusammenbrüche einst, Serverzusammenbrüche jetzt) übernommen.
- Vergabe der Plätze **durch Zufall/Losentscheid**
- Vergabe der Plätze **auf individueller Basis**: Als Kriterien werden hier Präferenzen der Studierenden (z.B. mit Hilfe so genannter Auktionssysteme), eine Bewertung des Studienfortschritts oder andere individuelle Faktoren herangezogen.

Gemeinsam ist den meisten Systemen, dass sie schon länger im Einsatz und daher recht gut auf die jeweiligen Bedürfnisse abgestimmt sind. Die Ablösung durch ein einheitliches System wird daher verständlicherweise nur dann auf Akzeptanz stoßen, wenn durch das neue System zumindest keine Verschlechterung der Situation eintritt. Vor allem auch die Art der Platzvergabe stellt für die meisten BetreiberInnen solcher Systeme ein Kriterium dar, auf das nicht verzichtet werden kann. Für ein universitätsweites System ist es jedoch, nicht zuletzt im Sinne der Bedienbarkeit, ein wesentlicher Erfolgsfaktor, dass man sich – wenn schon nicht auf eine – auf einige wenige Vergabevarianten einigt, die darüber hinaus auch miteinander verträglich sein müssen (was leider auf die meisten im Einsatz befindlichen Varianten nicht zutrifft).

Auch die grundsätzlich sinnvolle Verknüpfung des universitätsweiten Anmeldesystems mit der Curriculum-Verwaltung hat sich als ein der raschen Umsetzbarkeit nicht eben zuträgliches Ziel erwiesen. Zwar ist praktisch jedes Curriculum für sich genommen in einem solchen System abbildbar, indem im Extremfall alle Vorschriften des Curriculums „ausprogrammiert“ werden; dies wird in einigen der bestehenden Anmeldesysteme auch erfolgreich umgesetzt. Angesichts der Vielzahl von Curricula der Uni Wien würde dies bei einem universitätsweiten Anmeldesystem aber einen weder zeit- noch kostenmäßig vertretbaren Aufwand bedeuten, der zudem nicht nur bei der Einführung des Systems anfällt, sondern bei jeder Neuerstellung oder Änderung eines Curriculums. Die technische Herausforderung besteht also darin, ein System zu entwickeln, in dem mittels Konfiguration (also ohne Eingriff in das eigentliche System) alle Curricula abgebildet werden können und das im Idealfall von den fachlich für die Erstellung und Pflege der Curricula zuständigen Personen selbst bedient werden kann.

Es gab im Laufe des Projektes UNIVIS einige zeitintensive Bemühungen in diesem Zusammenhang, die im Wesentlichen ergaben, dass ein Formalismus, der ausreichend mächtig ist, um zumindest einen großen Teil der an der Uni-

versität Wien gültigen Curricula (bzw. damals Studienpläne) in hinreichender Genauigkeit abzubilden, einen so hohen Grad an Komplexität aufweist, dass der Einsatz eines darauf aufbauenden Systems gegenüber der individuellen Ausprogrammierung jedes einzelnen Curriculums praktisch keinen Vorteil hat. Es war daher bald klar,[3] dass eine universitätsweite Abbildung von Curricula nur dann erfolgreich sein kann, wenn die Curricula nach einheitlichen Konstruktionsprinzipien aufgebaut sind. Ein Formalismus, der diese Konstruktionsprinzipien unterstützt, kann dann in Folge zur Abbildung aller Curricula benutzt werden, die diesen Prinzipien gehorchen. Selbstverständlich ist bei der Festlegung derartiger Prinzipien darauf zu achten, dass die dadurch zwangsläufig definierten Einschränkungen ausschließlich struktureller und keinesfalls inhaltlicher Natur sind. Aus diesem Grund kann die Festlegung solcher Prinzipien auch nicht durch den ZID erfolgen, sondern nur durch die für die Entwicklung von Curricula zuständigen Organe der Universität Wien.

Ein Pilotprojekt …

Die im Zuge von UNIVIS im Bereich Studienwesen eingesetzte Software i3v verfügte bereits bei der Einführung über eine Komponente zur Modellierung von Studienplänen. Um Erfahrungen zu sammeln, wurde diese Komponente von der Firma GINIT um ein Online-Anmeldesystem erweitert und im Rahmen des Pilotprojekts *[mcw]150* im Wintersemester 2001 an der damaligen Medizinischen Fakultät eingesetzt.[4] Mit dem Inkrafttreten des neuen medizinischen Studienplanes im Wintersemester 2002 wurde das System auf die gesamte Fakultät ausgedehnt; an der heutigen Medizinischen Universität Wien ist es nach wie vor im Einsatz. Das Online-Anmeldesystem stellte sich jedoch bald als Schwachstelle heraus und wurde daher von der Universität Wien völlig neu entwickelt und in *UNIVIS online* (siehe Kasten auf Seite 9) integriert.

Die Erfahrungen an der Medizinischen Fakultät zeigten, dass die Modellierungsmöglichkeiten von i3v für den medizinischen Studienplan recht gut geeignet sind. Es zeigte sich allerdings auch, dass dies zu einem wesentlichen Teil auf die spezifischen Eigenheiten dieses Studienplanes zurückzuführen ist und die Erkenntnisse daher nicht ohne weiteres für andere Studienpläne verallgemeinert werden konnten (aus heutiger Sicht mag daher die Wahl der Medizinischen Fakultät als Versuchsgelände ein wenig unglücklich erscheinen).

Noch ein weiterer Aspekt war dem Einsatz an der Medizinischen Fakultät förderlich, einem Einsatz an der gesamten Uni Wien jedoch hinderlich: Das System beruht auf der Voraussetzung, dass nur Studierende teilnehmen, deren Studienplan im System abgebildet ist. Das war für die Medizinische Fakultät (und danach für die Medizinische Universität) aufgrund der überschaubaren Anzahl von Studienrichtungen mit vertretbarem Aufwand umsetzbar. Für die gesamte Universität Wien bedeutet dies aber, dass für den Einsatz des Systems die Abbildung aller aktuell gültigen Studienpläne erforderlich ist, was aufgrund der großen Anzahl von Studien für viele Jahre – wenn nicht überhaupt auf Dauer – unrealistisch ist.

… und noch eines

Im Juni 2005 wurde ein neuerlicher Anlauf zur Entwicklung eines Anmeldesystems im Rahmen von UNIVIS unternommen. Im Rahmen einer Machbarkeitsstudie sollte *UNIVIS online* bis zum Beginn des Wintersemesters 2005 um ein Anmeldesystem erweitert werden (genau genommen um ein *weiteres* Anmeldesystem, denn das Anmeldesystem für die Medizinische Universität war ja bereits integriert). Als Zugeständnis an diesen ehrgeizigen Zeitplan wurden – den bisherigen Erfahrungen Rechnung tragend – folgende Rahmenbedingungen festgelegt:

- Um weltanschauliche Diskussionen in Bezug auf die Modalitäten der Platzvergabe zu vermeiden und auch sonst den Bedarf an zeitaufwendigen Abstimmungen auf ein Minimum zu reduzieren, sollte das Projekt vorerst auf eine Studienprogrammleitung (SPL) beschränkt bleiben (somit konnte die betroffene SPL autonom entscheiden) und alle erforderlichen Abstimmungen direkt zwischen der SPL und dem ZID erfolgen.

- Da einerseits die Entwicklung einer allgemein verwendbaren Komponente zur Abbildung von Curricula im vorgesehenen Zeitrahmen nicht realisierbar schien (nicht zuletzt aufgrund der Tatsache, dass einheitliche Konstruktionsprinzipien nach wie vor nicht vorlagen), und andererseits im Sinne einer späteren Ausdehnung des Projekts auf andere Studienprogrammleitungen die Entwicklung einer speziell auf die Bedürfnisse der teilnehmenden SPL abgestimmten Komponente zu vermeiden war, wurde auf eine Integration des Curriculums vorerst überhaupt verzichtet.

Als Projektpartner konnte die Studienprogrammleitung Politikwissenschaft gewonnen werden,[5] die bereits erste Erfahrungen mit einem selbst entwickelten Anmeldesystem gesammelt hatte, das seit dem Studienjahr 2002/2003 für einen Teil der vom Institut für Politikwissenschaft angebotenen Lehrveranstaltungen eingesetzt worden war. Dieses System sollte nun durch ein Nachfolgesystem abgelöst werden, das

3) siehe z.B. *Comment 01/2*, Seite 2 bzw. unter `www.univie.ac.at/comment/01-2/012_2.html`

4) siehe *Comment 02/1*, Seite 6 bzw. unter `www.univie.ac.at/comment/02-1/021_6.html`

5) Besonderer Dank gebührt an dieser Stelle den MitarbeiterInnen des Instituts für Politikwissenschaft, des Instituts für Staatswissenschaft und der Studienprogrammleitung Politikwissenschaft, insbesondere Mag. Marion Löffler und Michael Mühlböck, deren unermüdlicher Einsatz den Erfolg des Pilotprojektes erst ermöglicht hat, sowie den Studierenden der politikwissenschaftlichen Studienrichtungen.

einerseits für alle Lehrveranstaltungen der SPL zum Einsatz kommen und zudem auch für die Prüfungsanmeldung geeignet sein sollte.

Im Juli 2005 begannen intensive Gespräche zwischen VertreterInnen der SPL und dem ZID, die aufgrund der bereits recht konkreten Vorstellungen der SPL rasch vorankamen. Planmäßig ab 3. 10. 2005 erfolgte die Anmeldung zu den Lehrveranstaltungen des Instituts für Politikwissenschaft über *UNIVIS online*. Die Anmeldephase verlief technisch reibungslos, lediglich die gewohnt spartanische Benutzeroberfläche von *UNIVIS online* bereitete vereinzelt Probleme bei der Bedienung.

Für die Anmeldungen des Sommersemesters 2006 wurden die Erfahrungen aus dem Wintersemester 2005 berücksichtigt und das System um einige Funktionen erweitert. Außerdem wurden nunmehr auch die Lehrveranstaltungen des Instituts für Staatswissenschaft in das System aufgenommen. Im Wintersemester 2005 war (wie in den Semestern davor) die Anmeldung zu diesen Lehrveranstaltungen noch im Anmeldesystem ISWI abgewickelt worden, und zwar im Wesentlichen deshalb, weil die entsprechenden Vorarbeiten am Institut (Erfassung der Lehrveranstaltungen, Festlegung der Anmeldefristen, Information der Studierenden usw.) längst abgeschlossen waren, als das *Pilotprojekt Politikwissenschaft* ins Leben gerufen wurde.

Zur Charakterisierung des im Rahmen des Pilotprojektes entwickelten Prototyps soll im Folgenden auf einige **Eigenschaften** desselben eingegangen werden:

- Das Anmeldesystem ist Bestandteil des Universitätsverwaltungssystems **i3v** und arbeitet daher mit dem zentralen Datenbestand der Universität Wien. Folglich entfällt etwaige Mehrarbeit durch mehrfaches Erfassen von Daten, und auch der aufwendige Betrieb fehleranfälliger Systemschnittstellen ist nicht erforderlich.

- Die Bedienung des Systems erfolgt für Studierende (z.B. zum An- und Abmelden) und Lehrende (z.B. zum Zugriff auf Anmeldelisten) über ***UNIVIS online*** – also über einen beliebigen Webbrowser. Die Verwaltung des Systems (z.B. die Festlegung der Anmeldefristen oder die Erfassung von Noten) erfolgt über i3v. Da die zugrunde liegenden Daten (Lehrveranstaltungsdaten, Studierendendaten usw.) ohnehin bereits in i3v verfügbar sind, ist der für die Konfiguration der Anmeldung erforderliche Zusatzaufwand minimal.

- Das System unterscheidet hinsichtlich der **Lehrveranstaltungsanmeldung** zwischen Lehrveranstaltungen mit beschränkter TeilnehmerInnenzahl (in der Regel prüfungsimmanente Lehrveranstaltungen) und solchen ohne Zugangsbeschränkung (klassischer Vertreter dieser Kategorie ist die Vorlesung). Die – nicht in allen Systemen übliche – Anmeldung zu Vorlesungen dient zum einen der SPL als Information über die Nachfrage nach den einzelnen Veranstaltungen, um z.B. eine Veranstaltung bei Bedarf in einen größeren Hörsaal zu verlegen (wobei die Reaktionsmöglichkeiten in Anbetracht der Hörsaalsituation der Universität in der Regel beschränkt sind). Zum anderen können die TeilnehmerInnen einer Veranstaltung künftig per eMail mit relevanten Informationen (z.B. kurzfristigen Änderungen) versorgt werden.

- Die Aufnahme in Veranstaltungen mit Platzbeschränkung erfolgt nach einem so genannten **Präferenzsystem**; der Zeitpunkt der Anmeldung ist dabei nicht relevant. Die Studierenden melden sich zu einem beliebigen Zeitpunkt innerhalb der Anmeldefrist (diese dauert in der Regel eine Woche) zu den gewünschten Lehrveranstaltungen an und reihen diese nach persönlicher „Wichtig-

UNIVIS online

UNIVIS online (`www.univie.ac.at/uvo/`) ist der Online-Zugang zum zentralen Universitätsverwaltungssystem der Universität Wien und bietet Studierenden die Möglichkeit, persönliche Daten einzusehen, die Heimat- und Zustelladresse zu ändern, den Studienstatus zu überprüfen und Studien online fortzusetzen (dies ist erforderlich, wenn der Studienbeitrag an einer anderen Universität eingezahlt wurde), das Studienbeitragskonto und Prüfungsergebnisse abzufragen sowie über die Zweckwidmung der Studienbeiträge abzustimmen.

UNIVIS online ging im Jänner 2004 als Prototyp in Betrieb und wurde sukzessive erweitert, zuletzt um ein Lehrveranstaltungs- und Prüfungsanmeldesystem und ein kommentiertes Vorlesungsverzeichnis.

Der Prototyp wurde auf Basis der J2EE-Technologie implementiert, als *Application Server* kommt der Open Source-Server JBoss (`www.jboss.com`) mit eingebettetem Apache Tomcat (`http://tomcat.apache.org/`) zum Einsatz. Der JBoss Application Server läuft auf einem HP DL380-Server unter dem Betriebssystem RedHat AS 3.0. Die SSL-gesicherte Kommunikation wird über einen Apache-Webserver (`http://httpd.apache.org/`) abgewickelt. An Web-Technologien werden derzeit ausschließlich HTML und CSS eingesetzt, was zwar die Möglichkeiten der Benutzeroberfläche und der Client-Server-Kommunikation einschränkt, aber eine möglichst gute Verträglichkeit mit einer Vielzahl von Browsern gewährleistet.

UNIVIS online wird täglich von durchschnittlich 5 000 Personen benutzt; dieser Wert steigt zu Semesterbeginn und -ende auf über 12 000. Ende 2006 soll der Prototyp von einem regulären Nachfolger abgelöst werden.

keit“, beginnend mit 1 für die subjektiv wichtigste Lehrveranstaltung. Diese Wunschliste wird bei der Vergabe der Plätze insofern berücksichtigt, als die Aufnahme in die Veranstaltungen in der Reihenfolge der Wunschliste erfolgt. In eine konkrete Lehrveranstaltung werden also zuerst alle Studierenden aufgenommen, die diese auf Platz 1 der Wunschliste haben, danach folgen jene, die sie auf Platz 2 haben usw., bis die Veranstaltung ausgebucht ist.

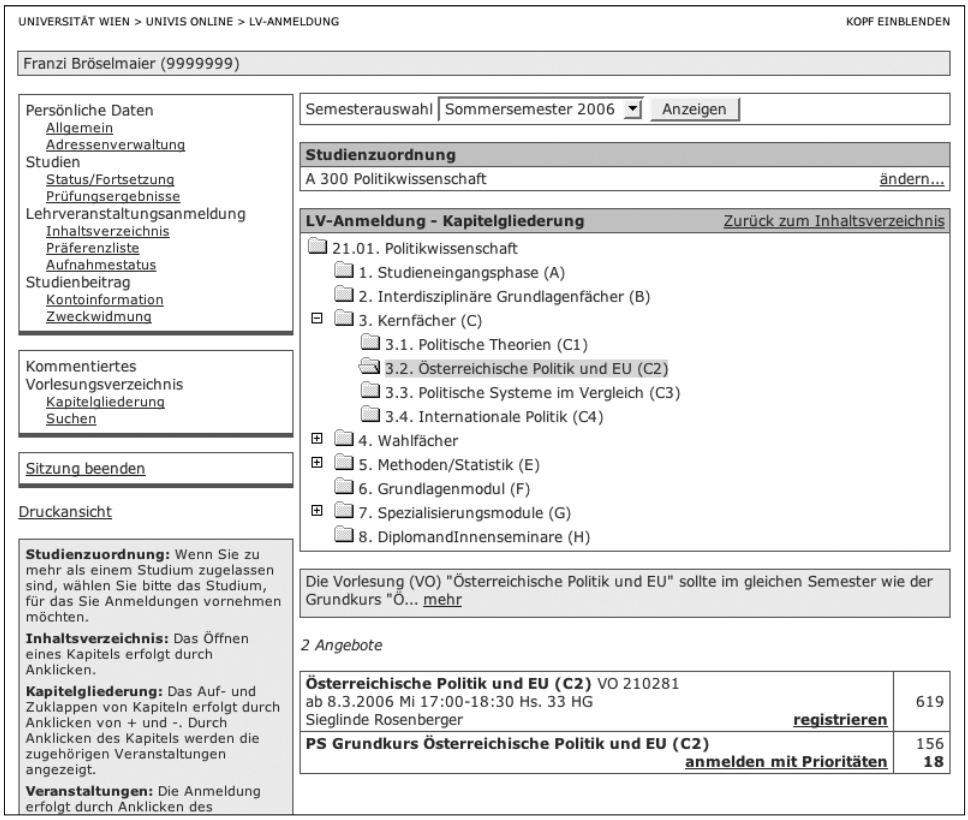


Abb. 1: Prototyp des Anmeldesystems in *UNIVIS online* (Ausschnitt)

- Lehrveranstaltungen, die mehrfach angeboten werden (**Parallelveranstaltungen**), können nur einmal besucht werden (d.h. man kann nicht zwei inhaltlich gleiche Parallelveranstaltungen im selben Semester besuchen). Es ist jedoch möglich, sich für mehrere davon anzumelden und die persönlichen Präferenzen in Form einer Reihung anzugeben, die bei der Zuteilung nach Maßgabe verfügbarer Plätze berücksichtigt wird.

- Nach der Anmeldefrist erfolgt die **Zuteilung** der Plätze aufgrund der festgelegten Kriterien. Die Studierenden können online eruieren, in welche Veranstaltungen sie aufgenommen wurden. Nach der Zuteilung erfolgt eine zweite Anmeldephase für Restplätze und etwaige infolge der Nachfrage zusätzlich angebotenen Lehrveranstaltungen. Die Anmeldung und Zuteilung in dieser Nachfrist erfolgt nach denselben Kriterien wie im ersten Durchgang. Die Listen der aufgenommenen Studierenden stehen den LehrveranstaltungsleiterInnen sowohl in *UNIVIS online* als auch in i3v zur Verfügung.

- Da die Studierenden bei der Anmeldung noch nicht wissen können, in welche Veranstaltungen sie letztlich aufgenommen werden, besteht prinzipiell die Gefahr, in Lehrveranstaltungen aufgenommen zu werden, die sich teilweise oder zur Gänze zeitlich überschneiden und daher nicht besucht werden können. Um die Anmeldung flexibler zu gestalten, erlaubt das System zwar eine Anmeldung zu **kollidierenden Veranstaltungen**, teilt jedoch nur Veranstaltungen zu, die auch besucht werden können (eine minimale Überschneidung wird toleriert).

- Damit alle für die Auswahl von Lehrveranstaltungen hilfreichen Informationen an einer Stelle zugänglich sind, wurde auch ein **Kommentiertes Vorlesungsverzeichnis** in *UNIVIS online* integriert. Die entsprechenden Daten werden (wie auch alle anderen) in i3v gepflegt.

- Auch die Anmeldung zu **Lehrveranstaltungsprüfungen** kann über *UNIVIS online* abgewickelt werden. Die Listen der aufgenommenen Studierenden stehen den PrüferInnen auch hier sowohl in *UNIVIS online* als auch in i3v zur Verfügung. Die Erfassung der Beurteilungen (Noteneingabe) erfolgt vorerst nur über i3v.

Ausblick

Das Projekt *Lehre XXI – Services* (Näheres siehe `http://lehrexxi-services.univie.ac.at/`) beschäftigt sich im Rahmen des universitätsweiten Projekts *Lehre XXI* mit der operativen Planung, Umstellung und Neuorientierung der Administration des Studienbetriebs und gliedert sich in verschiedene Teilprojekte (u.a. Anmeldesysteme, Elektronisches Curriculum, Lehrcontrolling, Prozessdokumentation).

Im Rahmen einer Präsentation am 14. 3. 2006 im Kleinen Festsaal der Universität Wien wurde das Pilotprojekt Politikwissenschaft als Vorarbeit zu *Lehre XXI – Services* vorgestellt und die Einführung eines auf diesem Pilotprojekt aufbauenden Systems für weitere Studienrichtungen im Rahmen des Teilprojekts Anmeldesysteme angekündigt. Dadurch ist gewährleistet, dass die Erfahrungen aus dem Pilotprojekt in die Konzipierung eines universitätsweiten Anmeldesystems einfließen, und darüber hinaus ist eine reibungslose Zusammenarbeit mit den anderen Teilprojekten von *Lehre XXI – Services* (insbesondere mit dem Teilprojekt Elektronisches Curriculum) sichergestellt.

Martin Polaschek ■

Das Postamt zieht um:

Ein neues Mailsystem für die Uni Wien

Warum ein neues Mailsystem?

Seit im *Comment 94/2* das „Mailbox-Service“ zum ersten Mal vorgestellt wurde (siehe `www.univie.ac.at/comment/94-2.pdf`), haben sich die Anforderungen an ein Mailsystem vervielfacht. Heute gehört Electronic Mail zur grundlegenden Kommunikations-Infrastruktur – ein zuverlässiges Mailsystem wird genauso als selbstverständlich vorausgesetzt wie die Wasserversorgung.

Um den wachsenden Ansprüchen gerecht zu werden, musste das Mailsystem der Universität Wien ständig weiterentwickelt werden: In fast jeder Ausgabe des *Comment* gab es mindestens einen Artikel zum Thema Mailing, und laufend wurde über Neuerungen berichtet. Schon mehrmals war von einem „neuen Mailbox-Rechner“ zu lesen; inzwischen gibt es schon lange keinen Mailbox-Rechner mehr, stattdessen sorgt rund ein Dutzend Server für die reibungslose Abwicklung des Mailverkehrs. Vor acht Jahren wurde im *Comment 98/2* noch die Frage gestellt: *Viren über eMail – Gefahr oder Gerücht?* Heute ist klar, dass die Gefahren real sind, und verlässliche Maßnahmen zur Abwehr von Viren sind unumgänglich, ebenso wie eine effiziente Spambekämpfung.

Trotz aller Erneuerungen, Erweiterungen und Umbauten des universitären Mailsystems wurde dessen grundlegende Achitektur unverändert beibehalten. Dabei haben sich im Laufe der Jahre einige Altlasten angesammelt. Wenn ein Haus zu klein wird und auch sonst nicht mehr den Anforderungen der Zeit genügt, kann man sich lange Zeit mit Um- und Ausbauten behelfen: Aus dem Dienstbotenzimmer wird ein Bad, der Dachboden wird ausgebaut, ein Schuppen wird zur Garage usw. Irgendwann nützt aber alles nichts mehr, und ein Neubau ist erforderlich. Das Mailsystem der Uni Wien ist an diesem Punkt angelangt: Alle Komponenten – Architektur, Hardware, Software – wurden erneuert.

Nach außen sollte von der Umstellung möglichst wenig zu merken sein: Alles, was bisher funktioniert hat, sollte – ohne Änderungen an Einstellungen in Mailprogrammen – auch weiter funktionieren.[1)] Deshalb wurde so verfahren, wie es manchmal beim Umbau von denkmalgeschützten Häusern geschieht: Die Fassade wurde stehengelassen, aber dahinter blieb kaum ein Stein auf dem anderen.

Eine so radikale Umstellung erfordert selbstredend eine gründliche Vorbereitung. Das neue Mailsystem wurde daher im Laufe von mehreren Monaten parallel zum bestehenden aufgebaut und gründlich getestet. Eine schrittweise Inbetriebnahme war hier nicht möglich; das System wurde vielmehr am Vormittag des 16. Juni 2006 durch die Änderung der entsprechenden Nameserver-Einträge aktiviert, die nur wenige Minuten in Anspruch nahm. Nach einigen kleinen Nachbesserungen läuft das System seither ohne Probleme.

Was ist anders?

Wie das neue Mailing technisch funktioniert, wird im Kasten *Das neue „Postverteilerzentrum“ der Universität Wien* vom Architekten des Systems, Wolfgang Breyha, beschrieben (siehe Seite 12). Im Folgenden ist kurz zusammengefasst, welche Erweiterungen und Features das System bietet:

Neuer Spamfilter

Dem komplett erneuerten Spamfilter ist ein eigener Artikel gewidmet (siehe Seite 13).

Verschlüsselte Übertragung

Als die im Mailing verwendeten Übertragungsprotokolle[2)] erfunden wurden, dachte noch niemand daran, eine Verschlüsselung vorzusehen. Es stellte sich jedoch bald heraus, dass dies problematisch ist, besonders dort, wo Passwörter übertragen werden. Deshalb wurden nachträglich verschlüsselte Erweiterungen definiert, von denen es zwei Varianten gibt:

- Das gesamte Protokoll wird verschlüsselt. Für verschlüsselte Übertragungen wird ein anderer Port verwendet als für unverschlüsselte.

- Die beiden „Gesprächspartner“ (Client und Server) beginnen ihren Dialog unverschlüsselt, können sich aber darauf einigen, verschlüsselt fortzufahren. Dies geschieht mit Hilfe des Befehls `STARTTLS`, weshalb diese Variante in vielen Mailprogrammen *TLS* genannt wird, während die durchgehend verschlüsselte als *SSL* bezeichnet wird (siehe Abb. 1 auf Seite 13) – eine reichlich verwirrende Nomenklatur, da TLS eigentlich ein Synonym für neuere Varianten von SSL ist (mehr über *Transport Layer Security* und *Secure Sockets Layer* erfahren Sie auf Seite 43).

---

1) Ausnahmen sind lediglich einige Altlasten, die im Zuge der Umstellung bereinigt wurden. Dazu gehören Mailadressen der Form *username*`@pcserv.univie.ac.at` und *username*`@rs6000.univie.ac.at` – mehrere Jahre nach Einstellung der „alten“ PC-Räume und des RS6000-Clusters wurden auch die dazugehörigen Mailadressen aufgelassen. Auch die vor der Mailbox-Umstellung im Sommer 1999 üblichen Mailbox-IDs (z.B. `a4711max`) funktionieren auf dem neuen System nicht mehr.

2) SMTP (*Simple Mail Transfer Protocol*), POP (*Post Office Protocol*) und IMAP (*Internet Message Access Protocol*)

Das neue „Postverteilerzentrum“ der Universität Wien

Die große Herausforderung und Chance, am Neudesign des Mailsystems der Uni Wien (mehr dazu siehe Seite 11) mitzuwirken, lockte mich vor etwa neun Monaten an den ZID. Seither wurde eine komplett neue „Postleitstelle“ geplant, gebaut und getestet – parallel zum laufenden Mail-Betrieb, der bis zum Tag der Umstellung über das bisherige System lief, und stets unter Rücksichtnahme auf die bestehenden organisatorischen Strukturen und Notwendigkeiten. Selbstverständlich flossen auch Elemente und Ideen des bisherigen Mailsystems (das technisch gesehen noch lange nicht zum „alten Eisen“ gehört) in das neue System ein. Nun ist der Zeitpunkt gekommen, dieses vorzustellen:

- Als Hardware werden derzeit 10 Server der Type **HP Proliant DL380 G4** eingesetzt.

- Beim Betriebssystem fiel die Entscheidung zugunsten von Linux (**Fedora Core 4**), nicht zuletzt aufgrund langjähriger guter Erfahrungen mit RedHat/Fedora auf eben dieser Hardware.

- Als *Mail Transfer Agent* (MTA) kommt **Exim** (`www.exim.org`) anstelle von sendmail (`www.sendmail.org`) zum Einsatz: Obwohl ich sendmail ebenfalls sehr schätze – vor allem auch aufgrund des Milter-API zur Einbindung externer Programme wie Virenscanner oder Spamfilter –, hat Exim in meinen Augen doch einige Vorteile. Dazu zählen unter anderem die gute Dokumentation, die vergleichsweise leicht verständliche Konfiguration, die exzellente Unterstützung von LDAP und ein ausgefeiltes Queue-Handling. Auch die Anbindung von Viren- und Spamfiltern ist in den letzten Jahren stetig verbessert worden.

- Ein wesentlicher Unterschied zum bisherigen Mailsystem ist die Verwendung von LDAP (*Lightweight Directory Access Protocol*). Dadurch werden Änderungen bzw. Neuanschaltungen von eMail-Adressen, Forwards etc. deutlich schneller aktiv: Anstatt alle Daten periodisch auf den Mailservern selbst zu aktualisieren, werden Änderungen inkrementell im LDAP-Verzeichnis durchgeführt. Das Mailsystem befragt für jede Transaktion neuerlich die LDAP-Server und hat somit unmittelbar Zugriff auf veränderte Daten (es ist eine der besonderen Eigenschaften von LDAP, die immense Anzahl von Anfragen, die dabei entstehen, zu bewältigen). Sowohl server- als auch clientseitig wird dabei das Open Source-Produkt **OpenLDAP** (`www.openldap.org`) verwendet.

- Im Bereich der Virenscanner setzen wir nun ebenfalls auf Open Source und wechseln von McAfee zu **ClamAV** (`www.clamav.net`). Zwar entstehen auch durch die Verwendung von McAfee keine Kosten, die Unix-Unterstützung dieses Scanners ist aber aufgrund des fehlenden Daemons nach wie vor äußerst mangelhaft. ClamAV bietet neben einer hoch performanten Scan-Engine auch guten Schutz gegen die meisten Phishing-Attacken; die Reaktionszeiten bei neuen Bedrohungen liegen im Spitzenfeld, weit vor Symantec oder McAfee. Der Nachteil dieser Lösung ist, dass ältere Viren nicht immer erkannt werden. Da es aber nach wie vor unerlässlich ist, jeden Computer zusätzlich mit einem lokalen Virenscanner zu schützen, sollte dies keine ernsthafte Bedrohung darstellen.

- Der Spamfilter wurde vollständig neu entwickelt; mehr dazu erfahren Sie im Artikel *Wenn der Postmann zweimal klingelt* auf Seite 13.

Die Mailserver sind in den Arbeitsgruppen MX, MSA, DCC und RELAY zusammengefasst und für folgende Aufgabengebiete zuständig:

- **MX** (*Mail eXchanger*): Diese Server empfangen Mails aus dem Internet. Hier sind alle Filterkomponenten – wie Greylisting, Virenfilter und Spamfilter – aktiv.

- **MSA** (*Mail Submission Agent*): Die MSA-Server – besser bekannt als MAIL.UNIVIE.AC.AT – übernehmen Mails aus dem Bereich der Universität Wien und beherbergen die POP3- und IMAP4-Proxies. Aktiv sind nur die Virenfilter.

- **DCC** (*Distributed Checksum Clearinghouse*): Hier laufen die DCC- und Greylisting-Services sowie lokal gespiegelte Blacklists (Näheres dazu finden Sie im Artikel *Wenn der Postmann zweimal klingelt* auf Seite 13).

- **RELAY**: Diese Gruppe dient als *Smarthost*, d.h. sie übernimmt die Zustellung aller Mails an externe Systeme.

Alle Server des neuen Mailsystems können prinzipiell jede beliebige Rolle übernehmen. Die Zuteilung zu einer Gruppe erfolgt zentral von einem Management-Server.

Wolfgang Breyha

Teilweise konnten die verschlüsselten Protokolle schon bisher verwendet werden. Mit dem neuen Mailsystem wird nun aber eine flächendeckende Unterstützung für verschlüsselte Übertragung angeboten:

- Der SMTP-Server **MAIL.UNIVIE.AC.AT** unterstützt TLS. Dieser Server dient im neuen Mailsystem allen Universitätsangehörigen – auch Studierenden – als Server für ausgehende Mail. (Der bisherige SMTP-Server für Studierende, MAIL.UNET.UNIVIE.AC.AT, kann weiterhin verwendet werden, unterstützt jedoch keine Verschlüsselung und Authentifizierung.)

- Die Server für eingehende Mail – **IMAP.UNIVIE.AC.AT** (für UniversitätsmitarbeiterInnen) und **IMAP.UNET.UNIVIE.AC.AT** (für Studierende) – unterstützen die verschlüsselte Variante des IMAP-Protokolls und, sofern gewünscht, auch des POP-Protokolls.

Zu beachten ist, dass die Verschlüsselung in allen Fällen nur den Transport betrifft – am Mailserver werden die Nachrichten unverschlüsselt gespeichert. Soll die Nachricht selbst kryptisiert werden, benötigt man spezielle Programme wie z.B. PGP (die selbstverständlich verwendet werden können, für die der Zentrale Informatikdienst aber derzeit keinen Support bietet).

Abb. 1: Aktivieren der SMTP-Authentifizierung in Thunderbird

Authentifizierung beim Mailversand

Zum Versenden von eMail ist, anders als beim Abholen, meist keine Authentifizierung (d.h. kein „Identitätsnachweis" mittels Username und Passwort) erforderlich. Um Missbrauch – vor allem durch Spammer – zu unterbinden, akzeptierten die Mailserver für ausgehende Mail (MAIL.UNIVIE.AC.AT und MAIL.UNET.UNIVIE.AC.AT) daher bislang nur Verbindungen aus dem Datennetz der Uni Wien. Wenn man sich aber authentifiziert (was, wie erwähnt, nur vom Server MAIL.UNIVIE.AC.AT unterstützt wird und bei den meisten Mailprogrammen durch einfaches Ankreuzen der entsprechenden Option geschieht, siehe Abb. 1), ist diese Einschränkung nicht nötig: Damit ist es z.B. möglich, bei einem Gastaufenthalt im Ausland ein Notebook einfach ans Netzwerk anzustecken und das Mailprogramm ohne jede Konfigurationsänderung weiter zu verwenden.

Authentifizierung und Verschlüsselung sind zwar im Prinzip voneinander unabhängig, der Server ist jedoch so konfiguriert, dass er Authentifizierung nur bei gleichzeitiger Verschlüsselung akzeptiert. Aktivieren Sie daher bitte die entsprechende Option ***TLS*** in Ihrem Mailprogramm (bei Thunderbird z.B. mittels ***Extras – Konten – Postausgang-Server (SMTP) – Bearbeiten***; siehe Abb. 1).

Peter Marksteiner ■

WENN DER POSTMANN ZWEIMAL KLINGELT:

Der neue Spamfilter der Uni Wien

Noch immer Spam?

Seit Sommer 2003 bietet der Zentrale Informatikdienst einen Spamfilter auf seinen Mailservern an. Dieser wurde im *Comment 03/1* vorgestellt, wo im Artikel *Forever Spam!? – Warum Spam nicht schon längst abgeschafft wurde* eine ausführliche Diskussion zum Thema Spam und zur Problematik der Spambekämpfung zu finden ist.[1)]

Die wichtigsten Punkte sind im Folgenden kurz zusammengefasst:

- Als „Spam" werden unerwünschte eMail-Nachrichten bezeichnet, die massenweise – oft millionenfach – verschickt werden. Zweck dieser Massensendungen ist fast immer schlicht und einfach das Geldverdienen; man spricht dann von *Unsolicited Commercial E-Mail* (UCE, unerwünschte Werbemail). Massensendungen zu anderen Zwecken – z.B. politische Propaganda – kommen seltener vor und werden allgemein als *Unsolicited Bulk E-Mail* (UBE, unerwünschte Massenmail) bezeichnet.

- Manche Formen von Spam sind nicht nur leicht anrüchige Methoden des Geschäftemachens, sondern eindeutig kriminell. Dazu gehören Phishing-Mails, das sind gefälschte Nachrichten von Banken, Online-Versandhäusern usw., die auf ebenfalls gefälschten Webseiten zur Preisgabe von Konto- und Kreditkartennummern, Passwörtern, TANs[2)] usw. verleiten (Näheres siehe Seite 37). Beim *Nigeria-* oder *419-Scam*[3)] wird um Unterstützung beim Transfer fabelhafter Summen von einem Land in ein anderes gebeten. Auch wenn manche dieser Geschäftsangebote durchaus seriös und verlockend wirken: Bitte lassen Sie davon unbedingt die Finger!

---

1) siehe *Comment 03/1*, Seite 2 bzw. unter `www.univie.ac.at/comment/03-1/031_2.html`

2) TAN steht für *Transaktionsnummer*; damit werden die im Online-Banking verwendeten Einmalpasswörter bezeichnet.

3) Benannt nach § 419 des nigerianischen Strafgesetzbuches, weil diese Art des Betrugs in Nigeria besonders beliebt ist (Näheres siehe `http://de.wikipedia.org/wiki/Scam`).

Ausschnitt aus einer Spam-Mail: Kopfzeilen und Inhalt

```
Date: Wed, 31 May 2006 02:05:21 +0600
From: "Charles Dupree" <FRDYJN@msn.com>
To: pugilistik@univie.ac.at
Subject:  Best Pharmacy r56
X-DCC-Univie-Metrics: ray.univie.ac.at 32722; Body=1 Fuz1=1 Fuz2=8300035
X-Univie-Virus-Scan: scanned by ClamAV on ray.univie.ac.at
X-Univie-Spam-Score: 29.3
X-Univie-Spam-Score-Int: 293
X-Univie-Spam-Level: ++++++++++++++++++++++++++++++
X-Univie-Spam-Checker-Version: SpamAssassin 3.1.1 (2006-03-10) on ray.univie.ac.at
X-Univie-Spam-Status: Yes, score=29.3, required=8.0, tests=DNS_FROM_RFC_ABUSE,
       DNS_FROM_RFC_POST,FUZZY_GUARANTEE,FUZZY_PHARMACY,FUZZY_VLIUM,
       FUZZY_VPILL,FUZZY_XPILL,SPF_SOFTFAIL,UNPARSEABLE_RELAY,URIBL_AB_SURBL,
       URIBL_JP_SURBL,URIBL_OB_SURBL,URIBL_SC_SURBL,URIBL_WS_SURBL,ZIDDCC_ONE
X-Univie-Spam-Languages: en
X-Univie-Spam-Report: Content analysis details:   (29.3 points, 8.0 required)
       *  1.5 SPF_SOFTFAIL SPF: sender does not match SPF record (softfail)
       *      [SPF failed: Please see http://www.openspf.org/why.html?sender=frdyjn%40msn.com&
       *      ip=194.152.96.145&receiver=ray.univie.ac.at]
       *  0.0 UNPARSEABLE_RELAY Informational: message has unparseable relay lines
       *  3.0 FUZZY_GUARANTEE BODY: Attempt to obfuscate words in spam
       *  0.6 FUZZY_VLIUM BODY: Attempt to obfuscate words in spam
       *  2.6 FUZZY_XPILL BODY: Attempt to obfuscate words in spam
       *  2.6 FUZZY_PHARMACY BODY: Attempt to obfuscate words in spam
       *  0.7 FUZZY_VPILL BODY: Attempt to obfuscate words in spam
       *  0.5 DNS_FROM_RFC_ABUSE RBL: Envelope sender in abuse.rfc-ignorant.org
       *  1.4 DNS_FROM_RFC_POST RBL: Envelope sender in postmaster.rfc-ignorant.org
       *  3.6 URIBL_SC_SURBL Contains an URL listed in the SC SURBL blocklist
       *      [URIs: bestproofonline.com]
       *  3.4 URIBL_JP_SURBL Contains an URL listed in the JP SURBL blocklist
       *      [URIs: bestproofonline.com]
       *  3.3 URIBL_AB_SURBL Contains an URL listed in the AB SURBL blocklist
       *      [URIs: bestproofonline.com]
       *  1.5 URIBL_WS_SURBL Contains an URL listed in the WS SURBL blocklist
       *      [URIs: bestproofonline.com]
       *  2.6 URIBL_OB_SURBL Contains an URL listed in the OB SURBL blocklist
       *      [URIs: bestproofonline.com]
       *  2.0 ZIDDCC_ONE reached threshold in one DCC category
X-Univie-Spam-Flag: YES

The most complete Phar macy Online
We carry all major medds at bargain price
Viggra, Ci ialis, VaIium, Xa naax
Phantermiine, Ulltraam and etc...
SatiisfactIon Gua ranteeed

http://bestproofonline.com/?4l6l
```

Beim neuen Spamfilter der Uni Wien beginnen alle von SpamAssassin erzeugten Kopfzeilen mit `X-Univie-Spam`. Für die hier abgebildete Nachricht wurden 29.3 Schlechtpunkte vergeben (das ist ein sehr hoher Wert). Diese Zahl wird in mehreren Formaten ausgegeben (`X-Univie-Spam-Score`, `X-Univie-Spam-Score-Int`, `X-Univie-Spam-Level`), um ein automatisches Verarbeiten durch Filterprogramme zu erleichtern. Unter `X-Univie-Spam-Report` ist detailliert aufgelistet, aufgrund welcher Tests die Punkte vergeben wurden. Das abschließende Urteil ist unter `X-Univie-Spam-Flag` zu finden: `YES` – es ist eindeutig Spam.

- Eine automatisierte, fehlerfreie Spam-Erkennung ist unmöglich: Das entscheidende Kriterium ist „unerwünscht", und das ist ein subjektives Kriterium. Bei jeder Form der automatisierten Spambekämpfung besteht daher die Gefahr so genannter *False Positives*: Es kann vorkommen, dass legitime und vom Empfänger gewünschte Nachrichten fälschlicherweise als Spam klassifiziert werden.

- In Österreich ist das Versenden von Massenmail im § 107 des Telekommunikationsgesetzes 2003 geregelt. Bei unerwünschter elektronischer Post aus Österreich ist eine Beschwerde beim jeweiligen örtlich zuständigen Fernmeldebüro möglich und sinnvoll (Näheres siehe `www.bmvit.gv.at/telekommunikation/spam/`). Fast alles an Spam kommt jedoch aus dem Ausland, und die Aussichten auf Erfolg sind bei einer gerichtlichen Verfolgung außerhalb Österreichs bzw. der EU sehr gering.

Bei der Implementierung des Spamfilters vor drei Jahren wurde größter Wert auf die Vermeidung von False Positives gelegt. In dieser Hinsicht war er auch außerordentlich erfolgreich: Es ist uns kein einziger derartiger Fall bekannt. Trotz des ehrgeizigen Zieles *„keine False Positives"* konnte nach einigen Anlaufschwierigkeiten eine respektable Trefferquote erzielt werden. Leider ist diese im Lauf der Jahre wieder gesunken: Form und Inhalt von Spam sowie die Methoden von Spammern ändern sich andauernd, was laufende Anpassungen am Spamfilter erforderlich macht. Diese konnten nicht immer schnell genug durchgeführt werden.

Nicht nur der Spam hat sich in den letzten drei Jahren verändert, sondern auch die Maßnahmen zur Spambekämpfung: Heute stehen ganz andere Werkzeuge zur Verfügung als noch vor drei Jahren. Deshalb hat der ZID beschlossen, im Zuge der Erneuerung des Mailsystems (siehe Seite 11) auch einen vollständig neuen Spamfilter zu entwickeln, wobei möglichst viele der bisher gewonnenen Erfahrungen in das neue System einfließen sollten.

Die Tricks der Spammer ...

Nachdem sie einem unsauberen und in fast allen Ländern der Welt illegalen Gewerbe nachgehen, müssen Spammer große Anstrengungen unternehmen, um ihre Spuren zu verwischen. Auch müssen sie sich immer wieder etwas Neues einfallen lassen, um die Gegenmaßnahmen der Internet-Provider und Software-Hersteller zu umgehen. Vor einigen Jahren wurde Spam hauptsächlich über ungenügend geschützte Mailserver, so genannte „offene Relays", versendet.[4] Inzwischen sind die meisten dieser offenen Relays abgedichtet, und die verbliebenen stehen auf Schwarzen Listen (siehe weiter unten). Deshalb verbünden sich viele Spammer kurzerhand mit den Urhebern von Viren und Trojanern (siehe dazu auch den Artikel *Ferngesteuerte Spam-Armeen* im *c't-Magazin 5/04*, Seite 18). Einerseits fungieren die von solchen Schädlingen infizierten Rechner als ferngesteuerte Spambots[5] und verschicken – von ihren ahnungslosen BenutzerInnen unbemerkt – große Mengen an Spam. Andererseits durchforsten die ungebetenen Gäste auf dem Wirtssystem etliche Dateien nach eMail-Adressen. So verschicken z.B. einige Varianten des Sobig-Wurms nichts als eMail-Adressen, um die Adresslisten anderer Systeme zu füttern. Auf diesem Weg kommen die Spammer auch an die bestgehüteten Adressen, die nur im privaten Bereich verwendet werden.[6]

... und die Waffen der Spamjäger

Die meisten der nachfolgend beschriebenen Methoden liefern nur Indizien, ob es sich bei einer Mail um Spam handelt oder nicht. Zur erfolgreichen Spambekämpfung ist daher immer eine Kombination möglichst vieler Methoden erforderlich. Die Aufzählung erhebt keinen Anspruch auf Vollständigkeit, beinhaltet jedoch die wichtigsten der Verfahren, die im neuen Spamfilter der Uni Wien eingesetzt werden.

Die Masse macht's

Eine Eigenschaft hat Spam immer: Er wird in Massen versandt. Zwar gibt es auch legitime Massenmails, aber in jedem Fall ist das massenhafte Vorkommen von Nachrichten gleichen oder ähnlichen Inhalts verdächtig. Das ***Distributed Checksum Clearinghouse*** (DCC, `www.rhyolite.com/anti-spam/dcc/`) bietet die Möglichkeit, Prüfsummen zu bilden, die Prüfsumme bei einer zentralen Stelle zu registrieren und festzustellen, wie oft weltweit eine Nachricht mit derselben Prüfsumme schon registriert wurde. Auch *Spamtraps* lassen sich in Verbindung mit DCC erfolgreich einsetzen: Das sind Mailadressen, deren einziger Zweck es ist, von automatischen Suchprogrammen (so genannten *Harvestern*) gefunden zu werden. Mail an solche Adressen ist ausschließlich Spam und kann beim Clearinghouse wesenlich höher gewichtet werden.

Schwarze, weiße und graue Listen

Zahlreiche Organisationen und Firmen pflegen ***Blacklists*** – „Schwarze Listen", auf denen üblicherweise IP-Adressen stehen, von denen aus Spam versandt wurde. Details dazu sind im Artikel *Spammer vs. Blacklists: Ein ewiges Wett-*

---

4) siehe Artikel *We do not relay* in *Comment 98/2*, Seite 28 bzw. unter `www.univie.ac.at/comment/98-2/982_28.html`

5) Als Bot (abgekürzt für *Robot*) wird ein Computerprogramm bezeichnet, das weitgehend autonom und unbeaufsichtigt simple, aber arbeitsintensive Aufgaben erledigt – wie z. B. das Versenden von Spam.

6) Spammer erhalten Adressen auf vielen Wegen, u.a. auch durch systematisches Probieren. Es wird immer wieder diskutiert, wie sehr das Publizieren von Adressen (z.B. auf Webseiten oder in Newsgruppen) zu einer „Verseuchung" durch Spam führt; wirklich schlüssige Antworten auf diese Fragen gibt aber es nicht. Die Veröffentlichung von eMail-Adressen im Online-Personalverzeichnis der Uni Wien (`http://online.univie.ac.at/pers`) trägt vermutlich kaum – wenn überhaupt – zum Spam-Aufkommen bei. Auch sind diese Adressen im Quelltext der Seite kodiert angegeben, was ein automatisiertes Auslesen erschwert.

rüsten im *Comment 03/1* zu finden.[7] Eine relativ neue Entwicklung sind Blacklists, welche die Domains von URLs enthalten, die in Spam-Mails beworben werden. Solche Blacklists sind außerordentlich erfolgreich, weil sie eine Schwachstelle von Spammern treffen: Diese können sich zwar immer gefinkeltere Umwege ausdenken, um IP-basierten Blacklists zu entgehen, aber die URLs der Webseiten, über die sie ihre zweifelhaften Produkte verkaufen wollen, müssen irgendwo im Klartext stehen und können sich auch nicht allzu schnell ändern.

Es gibt auch ***Whitelists***, das sind „Weiße Listen" von vertrauenswürdigen Adressen. In Österreich wird z.B. eine Whitelist vom Verband der Internet-Provider (ISPA, `www.ispa.at`) gepflegt: Die teilnehmenden Provider verpflichten sich, an ihren Mailservern ausreichende Maßnahmen gegen Spam zu ergreifen, im Gegenzug behandeln sie alle anderen Mailserver auf dieser Whitelist bevorzugt und ignorieren etwaige Einträge in beliebigen Blacklists (auch als seriöser Betreiber eines Mailservers kann man relativ leicht auf einer Schwarzen Liste landen).

Spammer haben es beim Mailversand grundsätzlich sehr eilig. So kommen sie mit dem Umstand, dass ein Mailsystem temporär Probleme haben könnte, nicht sonderlich gut zurecht. Normalerweise legt ein Mailserver bei Zustellungsproblemen die betroffene Nachricht in eine Warteschlange und versucht es in regelmäßigen Intervallen erneut. Spammern ist das aber zu aufwendig. Sie probieren es daher meist nur einmal pro Mail und ignorieren alle Rückmeldungen vom Mailserver des Empfängers. Dieser Umstand wird vom ***Greylisting*** ausgenutzt, einer höchst wirksamen Methode zur Spambekämpfung: Beim Eintreffen einer neuen Nachricht wird diese vorerst mit einem temporären Fehler abgewiesen, aber dabei die Kombination aus Absenderadresse, Empfängeradresse und IP-Adresse notiert. Erst wenn „der Postmann zweimal klingelt", d.h. wenn innerhalb eines gewissen Intervalls ein zweiter Zustellversuch erfolgt, wird daraus gefolgert, dass es der Absender ernst meint, und die Nachricht wird zugestellt. Der große Vorteil von Greylisting ist, dass praktisch keine False Positives auftreten: Schlimmstenfalls kommt es zu gewissen Verzögerungen bei der Zustellung. „Kollateralschäden" gibt es höchstens bei fehlerhaften Programmen zur automatisierten (aber legitimen) Versendung von Mail, die temporäre Fehler bei der Zustellung ebenfalls nicht richtig behandeln.

Inhalt und Form

Zu guter Letzt bleibt noch die Möglichkeit, programmgesteuert das zu tun, was auch ein Mensch tut, der seine Post liest und Spam dabei löscht: anhand verschiedener formaler und inhaltlicher Kriterien zu entscheiden, ob es sich um Spam handelt oder nicht. Für einen „menschlichen Spamfilter" sind hauptsächlich inhaltliche Kriterien ausschlaggebend, die sich aber relativ schwer automatisiert überprüfen lassen. Zwar sind viele Programme in der Lage, nach verdächtigen Phrasen wie *Order Viagra now* zu suchen, im Allgemeinen sind jedoch formale Kriterien Erfolg versprechender: Blacklists, Phantasie-Adressen als Absender, spezielle HTML-Formatierung und viele andere.

Eines der erfolgreichsten Programme dieser Art ist ***SpamAssassin*** (`http://spamassassin.apache.org/`). Dieser unterwirft jede Nachricht einer Reihe von aufwendigen Tests. Für jede „verdächtige" Eigenschaft gibt es Schlechtpunkte (in seltenen Fällen vergibt SpamAssassin auch Gutpunkte). Am Ende werden alle Testergebnisse addiert und das abschließende Urteil in Form von Kopfzeilen (*Header*) vermerkt. SpamAssassin ist sehr flexibel und kann beliebig an individuelle Bedürfnisse angepasst werden. Diese Flexibilität ist sehr wichtig, um auch für die Zukunft gerüstet zu sein, da Spammer ihre Taktiken andauernd ändern.

Neu: Drei Fallen für Spammer

Beim neuen Spamfilter der Universität Wien muss eine Nachricht im Wesentlichen drei Tests bestehen, bevor sie zugestellt wird:

- Der Transport von eMail erfolgt nach wohldefinierten Regeln. Die Basis bildet das *Simple Mail Transfer Protocol* (SMTP), das in mehreren Standard-Dokumenten, so genannten RFCs, definiert ist (siehe `http://de.wikipedia.org/wiki/Request_for_Comments`). Wer das Protokoll nicht einhält, muss damit rechnen, dass seine Nachrichten nicht ankommen. Da sich Spammer an keinerlei Regeln halten, ist es weiter nicht verwunderlich, dass sie auch bei der Einhaltung von RFCs immer wieder Fehler begehen. Deshalb ist es möglich, bis zu einem Viertel der unerwünschten Mails schon anhand solcher Kriterien einfach abzulehnen, ohne sich der Gefahr von False Positives auszusetzen.

- Die zweite Hürde, die eine Nachricht zu überwinden hat, ist das Greylisting. Um eine generelle Verzögerung bei der Zustellung zu vermeiden, kommt eine leicht abgeschwächte Version von Greylisting zum Einsatz: Mails von unverdächtigen IP-Adressen werden sofort zugestellt (dazu gehören insbesondere alle Adressen, die auf der ISPA-Whitelist stehen). Dadurch ist weitestgehend sichergestellt, dass erwünschter Mailverkehr ungehindert passieren kann. Ist der Absender aber auch nur im Geringsten verdächtig, d.h. steht er auf einer beliebigen der zahlreichen Blacklists, so heißt es beim ersten Zustellversuch *„bitte warten"*. Insbesondere werden auch jene Listen berücksichtigt, die Netze mit dynamisch vergebenen IP-Adressen beinhalten (Wählleitungszugänge, ADSL-Anschlüsse usw.). Zwar sind das meist die Adressen von braven BürgerInnen, aber gerade die haben oft virenverseuchte PCs und verschicken, ohne es zu wis-

7) siehe *Comment 03/1*, Seite 37 bzw. unter `www.univie.ac.at/comment/03-1/031_37.html`

8) siehe *Kammerjäger im Netz* in *Comment 06/1*, Seite 31 bzw. unter `www.univie.ac.at/comment/06-1/061_31.html`

sen, massenhaft Spam.[8)] Nach unseren bisherigen Erfahrungen scheitert weit mehr als die Hälfte aller Spam-Nachrichten am Greylisting.

- Anschließend werden alle restlichen Nachrichten von SpamAssassin auf Herz und Nieren geprüft. Dieses Programm markiert in Form von Kopfzeilen, ob es die jeweilige Nachricht für Spam hält oder nicht. Natürlich gibt es dann noch immer einen unvermeidlichen Rest, der auch SpamAssassin durch die Lappen geht – der ist allerdings kaum mehr der Rede wert.

Wie aktiviere ich den Spamfilter?

Den schon eingangs abgeblockten Spam – sei es aufgrund von Regelwidrigkeiten oder durch Greylisting – bekommt man sowieso nie zu Gesicht; hier ist eine Aktivierung nicht erforderlich. SpamAssassin hingegen filtert Spam nicht aus, sondern markiert ihn nur. Das eigentliche Filtern kann auf mehrere Arten erfolgen:

- **Am Mailserver (die empfohlene Methode):** Zur Aktivierung muss die Webseite **`www.univie.ac.at/ZID/spamfilter-webmaske/`** aufgerufen werden. In den Standard-Einstellungen werden alle Nachrichten mit einem Spam-Level von 15 oder mehr automatisch gelöscht – hier sind False Positives praktisch ausgeschlossen. Mails mit einem Spam-Level von 8 oder mehr werden in einen eigenen Ordner verschoben. Auch hier sind False Positives extrem selten, aber nicht ganz unmöglich, weshalb sich von Zeit zu Zeit ein Blick in diesen Ordner empfiehlt (wer seine Mail mittels POP abruft, kann den Spam-Ordner via Webmail überprüfen). Nach einer frei wählbaren Zeitspanne (Standard: 30 Tage) werden die Nachrichten in diesem Ordner automatisch gelöscht.

  Im Unterschied zum bisherigen Spamfilter werden nun auch Nachrichten gefiltert, die indirekt zugestellt werden, z.B. über eine Service-Mailadresse mit einer Weiterleitung. Eine separate Aktivierung des Spamfilters für Service-Mailadressen ist daher normalerweise nicht erforderlich.

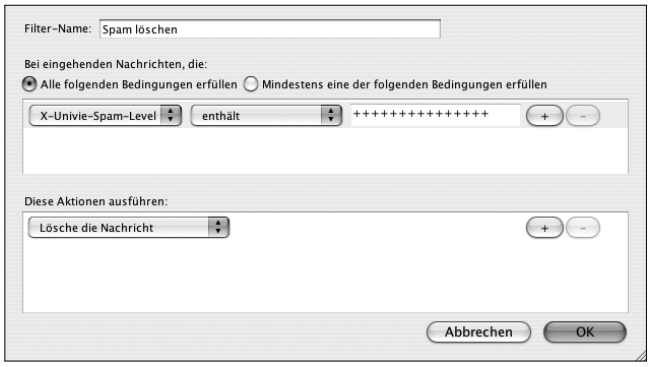


Abb. 1: Thunderbird – Konfiguration einer Regel zum Löschen von Mails, sobald das Spam-Level größer als 15 ist (*Extras – Filter – Neu*)

- **Am Klienten:** Die meisten Mailprogramme unterstützen das Sortieren anhand beliebiger Kopfzeilen. SpamAssassin ist so konfiguriert, dass es zahlreiche Kopfzeilen mit sehr vielen Detailinformationen liefert (siehe Kasten auf Seite 14). Am besten geeignet zur Filterung durch Klienten ist wohl die Zeile **`X-Univie-Spam-Level`**. In Abb. 1 ist dargestellt, wie eine solche Sortier-Regel im Mailprogramm Thunderbird konfiguriert werden kann; das Dialogfenster ist unter ***Extras – Filter – Neu*** zu finden. Falls Sie zusätzlich eigene Filter-Regeln (z.B. nach Absender/Betreff oder anhand von Black-/Whitelists) definieren wollen, so verwenden Sie dazu bitte Ihr Mailprogramm: Diese Funktionen werden vom neuen Spamfilter vorerst nicht unterstützt.

Electronic Mail ohne Spam – bis auf Weiteres ist das wohl ein unerreichbares Ideal. Mit dem neuen Spamfilter kommen wir diesem Ideal aber ein gutes Stück näher.

Wolfgang Breyha & Peter Marksteiner ■

EVALUIERUNG DES ZID-INFORMATIONSANGEBOTS

Der Zentrale Informatikdienst führte im Zeitraum von Ende März bis Ende April 2006 eine Umfrage unter Studierenden zu den Dokumentations- und Informationsmaterialien des ZID (Anleitungen, Folder, Webseiten, Zeitschrift *Comment*) durch. Wir möchten uns an dieser Stelle nochmals ganz herzlich bei all jenen bedanken, die sich die Zeit genommen haben, an unserer Befragung (online bzw. per Fragebogen) teilzunehmen – zu unserer großen Freude hat sich die überwiegende Mehrheit der Angesprochenen spontan zur Teilnahme bereit erklärt.

Bis zu den Sommerferien werden wir nun damit beschäftigt sein, die Daten der Evaluierung auszuwerten und die aus den Ergebnissen gewonnenen Erkenntnisse in die zukünftige Gestaltung unserer Medien einfließen zu lassen. Ihr Feedback dient uns dabei als unschätzbare Orientierungshilfe, um unser Angebot stetig für Sie zu verbessern und zu erweitern.

In diesem Sinne freuen wir uns natürlich auch weiterhin über Ihre Anregungen und Wünsche – ob nun postalisch („Leserbrief"), als eMail-Nachricht an **`redaktion.zid@univie.ac.at`** oder auch als Posting im *Comment*-Board des ZIDforum (**`www.univie.ac.at/ZID/forum/`**). Herzlichen Dank im Voraus!

Michaela Bociurko ■

Social Software mit dunkler Seite

Warum Internet-Telefonie via Skype Debatten über Freiheit und Missbrauch der Netze schürt

Während es in den letzten Jahren ganz selbstverständlich geworden ist, das Internet mit surfen, emailen, chatten, spielen, publizieren, tauschen, ansehen, anhören, kaufen, ersteigern, sich selbst darstellen etc. – und auch gerne alles auf einmal – für Unterhaltungs-, Informations- und Kommunikationszwecke zu nutzen, hat ein weiteres, uns bereits sehr vertrautes Anwendungsgebiet seinen festen Platz im Online-Bereich gefunden: Internet-Telefonie oder auch *Voice over Internet Protocol* (VoIP).

Wer gerade nicht über Festnetz erreichbar ist, den rufen wir ganz selbstverständlich auf dem Handy an, ganz egal, an welchem Ort sich der gewünschte Gesprächspartner soeben befindet. Ob geschäftlich oder privat, die stete telefonische Verfügbarkeit ist aus unserem Kommunikationsrepertoire einfach nicht mehr wegzudenken. Und obwohl uns heutzutage selbst ein Telefongespräch zwischen Gramatneusiedl und einem beliebigen Punkt auf der Chinesischen Mauer kaum mehr spektakulärer erscheint als der Anruf bei Frau Müller um die Ecke – abgesehen von der späteren Rechnung und das auch nur vielleicht –, suchen wir immer wieder nach weiteren, neuen und auch preiswerteren Alternativen, die uns ungebundene und allerorten verfügbare Erreichbarkeit ermöglichen. Die Internet-Telefonie verspricht hier neue Lösungen zu bieten.

Vor allem ein Programm ist dabei ganz besonders in den Fokus der Aufmerksamkeit – nicht nur vieler begeisterter User, sondern vor allem auch entgeisterter Security-Fachleute – gerückt: der VoIP-Client namens Skype.

Was genau ist Skype?

Skype ist eine gratis erhältliche, proprietäre[1] VoIP-Software, die sowohl das kostenlose Telefonieren im Internet, als auch kostenpflichtige Gespräche ins Fest- und Mobilnetz (*SkypeOut*) sowie eine Erreichbarkeit aus herkömmlichen Telefonnetzen (*SkypeIn*) ermöglicht. Darüber hinaus bietet Skype die Möglichkeit, Sofortnachrichten zu versenden – sprich zu chatten –, Dateien zu übertragen sowie Telefonals auch Chat-Konferenzen mit mehreren Usern gleichzeitig abzuhalten. Seit Anfang des Jahres unterstützt die Software auch Videotelefonie. Mit der neuesten Beta-Version[2] kann der Benutzer so genannte Skypecasts – moderierte VoIP-Diskussionsgruppen – einrichten oder an diesen mitwirken und zudem erstmalig auch SMS versenden.

Begonnen hat Skype als reines Peer-to-Peer-Netzwerk[3], in dem sich der Nutzer registriert und dann mittels Skype-Software für andere Online-Teilnehmer erreichbar ist. Mit der Registrierung wird jeder Nutzer direkt in eine Art Telefonbuch (*Buddy-Liste*) eingetragen. So lässt sich jeder User anhand des Benutzernamens ausfindig machen und kontaktieren.

Der Erfolg von Skype wurde vor allem im Laufe des letzten Jahres sichtbar. Weltweit verzeichnet der Dienst über 100 Millionen registrierte User. Noch im Mai 2005 belief sich die durchschnittliche Zahl der Skype-User, die gleichzeitig online waren, weltweit auf knapp über 3 Millionen. Im Juni 2006 ist diese Zahl bereits auf über 6 Millionen User angewachsen.

Über die Homepage von Skype (`www.skype.com`) kann sich jeder das Programm für sein entsprechendes Betriebssystem (Windows, Mac OS X, Linux sowie für Pocket PCs) herunterladen. Die Installation ist spielend einfach: *Download*-Button klicken, Installationsdatei ausführen, einen Usernamen, Passwort und seine eMail-Adresse angeben und schon lässt sich kostenlos drauf los telefonieren.[4] Weitere Einstellungen oder Konfigurationen sind normalerweise nicht notwenig. Selbst Netzwerk- oder Firewall-Einstellungen sollten Skype, im Gegensatz zu den meisten anderen VoIP-Clients, keine Probleme bereiten. Ein ganz entscheidender Grund, warum Skype bei den Usern so beliebt ist – und Netzwerkadministratoren einen kalten Schauer über den Rücken laufen lässt.

Was ist also dran an Skype? Und warum spaltet gerade dieser Client – wo der Markt doch genügend andere, vermeintlich gleichwertige oder gar bessere Programme[5] zur Verfügung stellt – Nutzer und Gegner in zwei scheinbar unvereinbare Lager?

---

1) Hier im Sinne von nicht allgemein anerkannter Standard in der IT-Branche; eine Art „hauseigene“ Entwicklung.

2) Beta-Version bezeichnet eine unfertige Version eines Programms, das jedoch zum Testen an die User freigegeben wurde.

3) Netzwerk ohne zentrale Instanz: In einem Peer-to-Peer-Netz (auch: P2P) sind alle Computer gleichberechtigt und können sowohl Dienste in Anspruch nehmen als auch zur Verfügung stellen.

4) Benutzerleitfäden zu Skype finden sich auf der Website `www.skype.com/intl/de/help/guides/`

5) siehe *VoIP-Clients (Auswahl)* im Kasten auf Seite 32

Grundlegendes über IP-Telefonie

Die Anfänge der Sprachübertragung über das Internet lassen sich bereits zehn Jahre zurückverfolgen, als die Firma VocalTec das erste öffentliche Telefongespräch von Computer zu Computer vorführte. Der IP-Telefonie ging es damals auch nicht anders als vielen innovativen Online-Features: Die Leistungsfähigkeit der Netze und der verfügbaren Hardware waren noch zu gering, als dass Sprachübertragungen in einer zufrieden stellenden Qualität von einem gebräuchlichen Rechner mit Internetanschluss aus möglich gewesen wären. Mittlerweile verschmelzen bei der Internet-Telefonie kaum merkbar die beiden bisher getrennten Bereiche Sprach- und Datenübertragung. Dabei hat sich seit Beginn der elektrischen, damals noch handvermittelten, Sprachübertragung Ende des 19. Jahrhunderts über Einführung digitaler Übertragung von Sprache via ISDN und Etablierung der Mobilkommunikation mit GSM bis hin zur Sprache über IP am eigentlichen Funktionsprinzip der Telefonie nichts geändert.

Bei der IP-Telefonie teilt sich vergleichbar zur klassischen Telefonie das Gespräch in zwei voneinander getrennte Vorgänge auf: der Verbindungsaufbau und die Gesprächsübertragung. Im Unterschied zum herkömmlichen Telefonnetz, in dem für jedes Gespräch eine dedizierte Verbindung freigeschaltet wurde, wird bei VoIP Sprache erst komprimiert und digitalisiert, dann in jeweils nur kleine, zerlegte Pakete, eventuell auch über verschiedene Wege transportiert, um beim Empfänger wieder entpackt, zusammengefügt und ausgegeben zu werden. Innerhalb eines bestehenden Netzwerkes werden so die vorhandenen Datenleitungen für verschiedene Dienste je nach Bedarf genutzt. Grundsätzlich gilt einmal, dass Gespräche über VoIP entweder netzintern, also nur von Computer zu Computer, oder aber netzübergreifend geführt werden können. Dabei werden dann Verbindungen zwischen Computer und Festnetztelefon bzw. Mobiltelefon hergestellt, oder gar Gespräche von Telefon zu Telefon via Internet über ein Voice-Gateway geführt. Diese Vermittlungsrechner werden eingesetzt, um eine Verbindung aus einem Datennetz in ein reines Telefonnetz herzustellen und Anfragen zwischen den verschiedenen Netzen zu bearbeiten und weiterzuleiten.

Eine Verbindung zwischen zwei Rechnern wird über die jeweilige IP-Adresse hergestellt, die sich vor allem bei Privatnutzern ändern kann. Ihnen wird beim Verbindungsaufbau für die Dauer einer Online-Sitzung eine dynamische IP-Adresse zugewiesen. Eine eindeutige Ansprache des Teilnehmers im Netz ist somit nicht so einfach möglich. Um dem entgegenzuwirken, wurde das *Session Initiation Protocol* (SIP) entwickelt, welches erlaubt, sich an einem zentralen SIP-Server zeitlich befristet anzumelden und dort die momentane IP-Adresse zu hinterlassen. SIP bietet zudem die Möglichkeit, über eine eigene, eindeutige Adresse angesprochen zu werden, die entweder in der Form `sip:`*`user@domain`* oder aber als herkömmliche Rufnummer vorliegen kann. Eine Rufnummer ist dann zu bevorzugen, wenn zwischen Computer und Telefonapparat oder zwei Apparaten gesprochen werden soll. Es geht aber auch ganz ohne Nummer. Für die Peer-to-Peer-Telefonie mit zentraler Verwaltung, beispielsweise bei Skype, reicht auch nur ein eindeutiger, frei wählbarer Username. Spezielle Server vermerken, wer online ist, und tragen die Teilnehmer mit Status *verfügbar* in so genannte Buddy-Listen ein. Einziger Haken ist, dass beide Teilnehmer für die Gesprächsführung online sein müssen.

Vor der privaten Nutzung ist Sprachkommunikation über Datennetze zuerst für Unternehmen und Institutionen interessant geworden. Gerade Firmen, die neben einer konventionellen Telefonanlage über ein firmeninternes Netzwerk verfügen, rechnen sich mit der Umstellung auf nur eine gemeinsame Sprach-Daten-Lösung neben geringerem Installations- und Wartungskostenaufwand auch Kostenersparnis bei Gesprächs- und Datenübertragungen aus. Ebenso sind Zwischenschritte denkbar, wenn etwa firmenintern via VoIP gesprochen wird und externe Anschlüsse weiterhin über das herkömmliche Telefonnetz erreicht werden. Private Haushalte versprechen sich beim Telefonieren über das Internet vor allem einen entscheidenden Kostenersparniseffekt, besonders dann, wenn man nur von Computer zu Computer telefoniert. Netzinterne Gespräche, sprich Telefonate im Internet oder LAN, sind nämlich kostenlos. Hierbei fallen in der Regel nur die Kosten für den Internetzugang selbst an, unabhängig davon, ob der angesprochene Rechner direkt nebenan oder um den halben Erdball entfernt steht. Mit zusätzlichen Gesprächsgebühren muss allerdings rechnen, wer netzübergreifend telefoniert. Hier lassen sich die Telefongesellschaften die Vermittlung von Gesprächen über ihre Netze grundsätzlich bezahlen. Inwieweit die Preise hierfür unter oder gar über den normalen Telefongebühren liegen, ist von Anbieter zu Anbieter verschieden.

Durch die Verbreitung von Breitband-Internetanschlüssen wird die IP-Telefonie vermutlich immer stärker ins Blickfeld der privaten Nutzer rücken. Wer zudem ohnehin ständig online ist, kann mit netzinterner Telefonie durchaus Geld sparen. Ein weiterer positiver Aspekt neben der Kostenersparnis liegt in der Mobilität. Mit dem eigenen Laptop können von jedem beliebigen Einwahlpunkt kostenlose bzw. kostengünstige Gespräche über das Internet geführt werden. Mit gratis erhältlichen VoIP-Clients (siehe Kasten auf Seite 32) ist es zudem für jeden Interessierten ein Leichtes, Telefonie über das Internet auszuprobieren und zu entscheiden, ob und inwieweit man dieses Medium nutzen möchte.

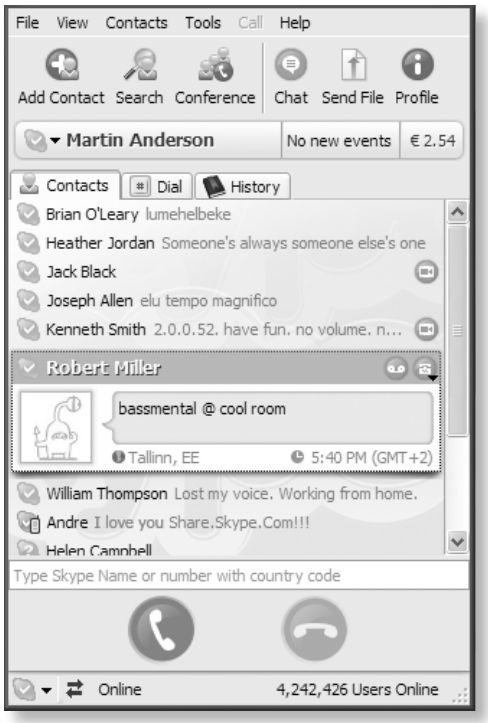
Skype aus Sicht einer Userin

Als sich Skype in meinen kommunikationstechnischen Wahrnehmungshorizont schob, dauerte es keine drei Tage und ich war süchtig. Ein guter Freund – mit Wohnsitz jenseits dieser Landesgrenzen – legte mir damals nach Wochen des reduzierten Sprachaustauschs aufgrund horrender Handyrechnungen weniger bittend als vielmehr verpflichtend das Programm Skype ans mitteilsame Herz.

Schon ein erster Blick auf die Website (`www.skype.com/intl/de/index.html`) stimmte mich vergnügt: Zum einen stach mir direkt das Motto „kostenlos telefonieren" ins Auge. Seit neuestem gibt's das sogar mit Videotelefonie, um einander amüsiert zuzuwinken. Wenn das eigene Büro dann schon von Haus aus mit einem Highspeed-Internetzugang ausgestattet ist, benötigt man nur mehr ein Headset – und wer spielerisch veranlagt ist, eine Webcam – und dem gebührenfreien Telefonieren steht nichts mehr im Weg. Zum anderen animierten besonders die herzigen Flash-Filmchen für Einsteiger sowie die ausgesprochen überzeugend und flott geschriebenen Texte der Website zum Weiter- und letztendlich *Download*-Button-klicken.

Click 'n' Call

Später fand ich noch heraus, dass sich mit Skype auch normale Telefonanschlüsse erreichen lassen, nur dass für diese Anrufe gezahlt werden muss. Um „nach draußen" zu telefonieren, muss man sich zuerst einmal ein entsprechendes Konto über die Skype-Website einrichten und dieses mit einem Gesprächsguthaben auffüllen, das sich dann ähnlich einer Prepaid-Karte für das Handy ganz einfach abtelefonieren lässt. Bezahlt wird, wie im Internet meistens üblich, mit Kreditkarte, wobei man sofort, nachdem die Dateneingabe erfolgt ist, den ersten Anruf tätigen kann. Der Skype-Client verfügt dazu über entsprechende Ziffern-Wähltasten, mit denen ganz normal eine Rufnummer eingegeben werden kann, so wie man es auch vom herkömmlichen Telefon her kennt. Danach den grünen Hörer anklicken und die Verbindung wird aufgebaut.



Der Skype-Client mit Kontaktliste, Guthabeninfo, Wähltasten und Symbolleiste. Unten rechts die aktuelle Anzahl der Online-User.

Die Tarife für SkypeOut-Gespräche sind dabei äußerst einfach gestaltet: Grundsätzlich ist es einmal egal, von woher man einen Anruf tätigt. Interessant ist nur, wohin auf der Welt das Gespräch tatsächlich geht. Dabei hat Skype für bestimmte Zielorte weltweit eine einheitliche Globalgebühr eingerichtet, die zum Beispiel für ein Telefonat von Wien nach Neuseeland, Kanada, Hongkong, nach China aufs Handy oder auch nur innerhalb Österreichs pro Minute den gleichen Betrag in Rechnung stellt, und der, verglichen mit Telekom, Handy oder selbst Billigdrittanbietern wie Telediscount[6], deutlich preiswerter ist. Verschiedene Tageszeiten oder Wochentage haben dabei keinen Einfluss auf den Minutenpreis. Dieser bleibt rund um die Uhr immer gleich. Berechnet werden nur die reinen Gesprächsgebühren, weitere Kosten für Anmeldung, Aktivierung etc. fallen nicht an.

Alle machen mit

Es verging keine Woche, da waren Freunde, Bekannte, Verwandte und Kollegen – eben all jene Leute, die meines Wissens ohnehin ständig online sind – mit dem Link zur Skype-Homepage und ein paar animierenden Zeilen versorgt. Wer nicht gleich anbiss, den hat der gruppendynamische Sozialdruck letztendlich überzeugt. Denn nur so funktioniert Skype: als proprietäres, zu allen anderen VoIP-Clients inkompatibles Protokoll sind kostenlose Gespräche nur zu anderen Skype-Usern möglich. So macht Skype erst dann richtig Sinn (und Spaß), je mehr Mitglieder die Gemeinschaft verzeichnet. Und wie man diese für sich gewinnt, hat Skype mit technischer Raffinesse und gekonntem Marketing bereits bestens unter Beweis gestellt.

Kommunizieren ohne Limit

Was mit einer Spielerei begann, hat sich mittlerweile bei einer befreundeten Kollegin zugunsten ihrer wissenschaftlichen Arbeit verfestigt. Wie die meisten der fest angestellten MitarbeiterInnen der Uni Wien verfügt auch sie über einen eigenen PC-Arbeitsplatz mit frei nutzbarem Internetzugang. Beim Telefon sieht das jedoch schon anders aus. Hier werden grenzüberschreitende Gespräche in der Regel reglementiert. Meistens muss hierfür sogar eine gesonderte Berechtigung beim Institut beantragt werden. Gerade für WissenschaftlerInnen, deren Arbeit von internationalem Austausch geprägt ist und die oft selber aus dem Ausland kommen, keine sehr günstigen Voraussetzungen.

Zum anderen ist es des Öfteren der Fall, dass eMail-Accounts auf ein bestimmtes, manchmal nur sehr geringes Datenvolumen beschränkt sind. Und nicht jeder kennt sich mit FTP oder dergleichen aus. Was also tun, wenn man die umfangreichen Konferenzpapiere dem Kollegen nach Berlin schicken will? Auch hier entpuppte sich Skype als ungeahnt hilfreiches Werkzeug, das für den unkomplizier-

6) `www.telediscount.at`

ten Austausch von Dateiformaten jeder Art benutzt werden kann. Das Skype-Transfervolumen unterliegt dabei keinerlei Beschränkungen, was vor allem dann sehr nützlich ist, wenn der eigene bzw. der eMail-Dienst des Kommunikationspartners Kapazitäts- oder Übertragungsbeschränkungen aufweist und auch sonst keine adäquate Transfermöglichkeit besteht.

Und selbst das ist noch nicht genug: Wer gerne mit mehreren Freunden oder KollegInnen gleichzeitig chatten oder telefonieren möchte, weil man an einer gemeinsamen Arbeit tüftelt oder einfach nur das letzte Wochenende ausgiebig erörtern mag, lädt einfach mehrere Skype-Kontakte zu einer Gruppenunterhaltung oder Konferenzschaltung ein, und schon lässt sich mit bis zu vier weiteren Personen telefonieren oder mit so vielen Leuten chatten wie man will.

Alles super – Alles schlecht

Internet-Telefonie scheint somit für vieles die Lösung zu sein: Sie kostet einen selbst sowie die Institute keinen Cent, bedient sich der bereits vorhandenen Infrastruktur und funktioniert quasi von allein. Nichts an Skype ist kompliziert. Wer sich weder von der Einfachheit noch vom nicht ausbleibenden Fun-Faktor überzeugen lässt, ist spätestens von der Sprachqualität und den wirklich günstigen Gesprächspreisen ins Festnetz begeistert.

Es sei denn, man arbeitet als Security Coordinator in der Netzwerkabteilung des ZID. So erntet man von diesem – im Gegensatz zur Kollegin, die immer wieder betont, wie dankbar und begeistert sie ist – als (technisch interessierte und durchaus datensicherheitsbedachte) Autorin eines *Skype-ist-Klasse*-Artikels jede Menge Missfallen, einen mehrstündigen Vortrag über Sicherheit im Netz und den Anflug eines schlechten Gewissens, weil man nun vielleicht für naiv gehalten wird. Und so bröckelt die *Macht-Spaß-und-kostet-nix*-Fassade von Skype ein wenig dahin.

Wo liegt nun das Problem mit Skype?

Das Problem mit Skype, so habe ich mir sagen lassen, ist, dass keiner eigentlich weiß, was es wirklich tut. Erst unlängst veröffentlichten zwei Mitarbeiter der EADS[7], Philippe Biondi und Fabrice Desclaux, in ihrem Vortrag *Silver Needle in the Skype* (`www.secdev.org/conf/skype_BHEU06.handout.pdf`) umfassendere Analyseergebnisse zur Arbeitsweise von Skype, deren Aufdeckung von den Skype-Machern aller Wahrscheinlichkeit nach nicht sehr gerne gesehen wird. Biondi und Desclaux konnten zwar Teile des sehr gut verschlüsselten Codes[8] freilegen, nur ob sich, wie von Sicherheitsspezialisten vermutet, eine Backdoor im System befindet oder VoIP-Daten umgeleitet oder gar belauscht werden, bleibt weiterhin fraglich.

Jetzt stellt sich einem natürlich die Frage, welchen Nutzen jemand davon haben könnte, den Inhalt meines Skype-Telefonats über die nette Zugbekanntschaft eines Freundes – mal abgesehen von dessen fester Freundin – in Erfahrung zu bringen. Und auch meine versandten Daten sind nicht besonders sensibel, es sei denn, jemand interessiert sich brennend für diverse Partybilder vom letzten Wochenende. Vermutlich nicht. Und so ist es dem „einfachen" User erst einmal egal, wie und was und überhaupt. Hauptsache es funktioniert. Und das tut es, bestens sogar.

Dabei schürt neben der strikten Geheimhaltung des Programmcodes noch eine weitere Eigenheit des Skype-Clients die Debatte um das Für und Wider: Die Rede ist hier vom Begriff Supernode. Was es damit und der vermuteten Backdoor auf sich hat, ist im folgenden Exkurs *The Dark Side of the Skype-Hype* genauer zu erfahren:

✧ ✧ ✧

The Dark Side of the Skype-Hype

Alexander Talos, IT-Security Coordinator des ZID

Die Entwickler von Skype haben bereits mit KaZaA [1] bewiesen, dass sie begnadete Programmierer sind. Beide Peer-To-Peer-Programme folgen einem einleuchtenden Erfolgsrezept: Sie machen Spaß, kosten nichts, bieten endlich die kommunikativen Goodies, die die Menschheit vor der Vereinsamung erretten sollen – und funktionieren, ohne dass die hauptamtliche Spaßbremse, der Firewall-Administrator, es verhindern könnte.

Hier zeigt sich ein klassisches Dilemma: Sobald die User die ihnen – im Namen der Sicherheit – auferlegten Beschränkungen als schikanös oder ungebührlich hinderlich empfinden, werden sie sie zu umgehen versuchen – mit allzu oft fatalen Folgen. So ist völlig klar, dass restriktive Handhabung von telefonischen Privat- und Auslandsgesprächen in Kombination mit lächerlichen Mailquota und drakonischer Firewall-Konfiguration zu einer katastrophalen Lösung wie Skype führen mussten.

Skype ist ein geniales Underground-Produkt und gleichzeitig ein Musterbeispiel dafür, wie man vieles falsch machen kann:

- Der Erfolg des Internet und all seiner Dienste fußt auf ausreichend diskutierten, standardisierten und veröffentlichten Protokollen. Was Skype über die Leitungen schickt, ist hingegen ein Geheimnis. [2]

- Vor Einführung eines Service sollte man sich Gedanken machen, welche Folgen das für das Netz hat und wie

7) *European Aeronautic Defence and Space Company*; `www.eads.net`

8) Die Studie gibt Aufschlüsse über den Netzwerkverkehr, die Art der Datenverschlüsselung, die Berechnung des Schlüssels sowie die Authentifizierung von Skype (siehe dazu auch `www.heise.de/newsticker/meldung/71094/`)

man die Voraussetzungen für einen reibungslosen, sicheren und kontrollierbaren Betrieb schafft. Skype verwendet im Gegensatz zu fast allen offiziellen Internet-Protokollen keine fixen Port-Nummern [3] und entzieht sich somit jedem Management.

- Der verantwortungsvolle Betrieb eines Dienstes erfordert Werkzeuge zu seiner Wartung und Kontrolle. Die Erfinder von Skype haben immensen Aufwand betrieben, genau dies zu verhindern.

Ein selbst gebasteltes Protokoll

Alle großen Netze haben eines gemeinsam: verbindliche Vereinbarungen, wie alles funktionieren soll. Beim Fernsehen etwa gibt es die Standards PAL, SECAM, NTSC, und jeder Fernseher, der sich daran hält, kann teilnehmen. Ebenso gibt es Standards für Festnetz- und Mobiltelefonie, genau wie für den Straßen-, Schiffs- und Luftverkehr. Anders ginge es nicht, das versteht jedes Kind. Besonders beim Internet gibt es eine solide Tradition, wie Dienste spezifiziert werden. Die drei Säulen sind:

- Aufbau auf bewährten, erprobten Protokollen – Webseiten werden z.B. über das *Transmission Control Protocol* (TCP) transportiert, das in vielen Anwendungen erfolgreich eingesetzt wird.

- Diskussion des Entwurfs durch Experten aus verschiedenen Fachrichtungen, wobei zum Beispiel die Folgen für die Netzwerkinfrastruktur und Sicherheitsüberlegungen von Anfang an einfließen.

- Veröffentlichung, Implementation durch mehrere Hersteller und bei Bedarf Evaluation sowie Erweiterung bzw. Verbesserung. [4]

Im Gegensatz dazu wurde Skype im stillen Kämmerchen ausgetüftelt und unter Verschluss gehalten. Es ist nicht ersichtlich, dass vorhandene Methoden verwendet werden. Dabei existieren längst echtzeitfähige Streaming-Protokolle, die von Routern entsprechend priorisiert und von Skype hätten verwendet werden können.

Über die Sicherheit von Skype oder darüber, was passiert, wenn tatsächlich großflächig mit Skype telefoniert wird, kann derzeit kaum eine seriöse Aussage getroffen werden. Dass die übliche Begutachtung fehlt, legt aber den Verdacht nahe, dass sich einige fundamentale Schnitzer eingeschlichen haben.

Da das von Skype verwendete Protokoll geheim ist [5], können auch keine Verbesserungsvorschläge einfließen, wie das sonst üblich ist. Besonders schmerzlich ist, dass selbst Technikern wenig Verständnis dessen möglich ist, was vor sich geht. Im Fall von Störungen können – außer von Skype selbst – keine zielgerichteten Maßnahmen ergriffen werden. Schon gar nicht können die für das Netz Verantwortlichen diese Probleme vorhersehen oder abwenden.

Nebenstellen der Uni Wien via VoIP erreichbar

Seit kurzem können alle Nebenstellen des Telefonsystems der Uni Wien auch über VoIP (*Voice over IP* = Internettelefonie) erreicht werden.

Wenn Sie ein ENUM-fähiges (ENUM = *Electronic Number Mapping*; siehe Artikel auf Seite 36) SIP-Phone verwenden, so geben Sie die gewünschte Uni-Rufnummer mit Vorwahl ein (z.B. `+431427714060`).

Sonst lautet der URI `sip:`*`nebenstelle`*`@univie.ac.at` (z.B. `sip:14060@univie.ac.at`). Ein ENUM-taugliches SIP-Phone für Windows XP ist unter `www.enum.at/index.php?id=softphone` kostenlos verfügbar.

Für einen erfolgreichen Betrieb ...

... ist es offensichtlich notwendig, den Client auf dem Computer zu installieren. Dass das mit eineinhalb Mausklicks in Null-Komma-Nix vonstatten geht, ist schön, aber nicht hinreichend.

Da stellt sich schon einmal die Frage nach dem Telefonbuch, der Buddy-Liste. Wer soll verhindern, dass irgendjemand die Katze seiner Nachbarin als Professorin der Rechtswissenschaften bei Skype einträgt und beliebigen Unfug treibt?

Legt man die Aufregung, die die vergleichsweise leicht zu durchschauenden Phishing-Attacken (Näheres siehe Artikel auf Seite 37) auslösen, auf die Skype-Buddy-Liste um, wird sofort klar, dass der Beruf des Internetbetrügers einige Zukunft hat (Fernstudien dazu bietet das Humbug-Fernlehrinstitut unter `www.humbug.at` an).

Die Verankerung in einem professionellen Umfeld, etwa so wie die Verknüpfung des Telefonsystems der Universität Wien mit der Personaldatenbank und Services wie CTI, ist bei einem geschlossenen und undokumentierten System wie Skype nicht möglich.

Und wie sieht es mit Notrufen aus? Eine im wahrsten Sinne des Wortes vitale Infrastruktur – bei Skype aber ausdrücklich ausgeschlossen. Das ist ausgesprochen hilfarm.

Telefonie ist für eine Universität eine ausgesprochen wichtige Infrastruktur, und es wurden zum Beispiel vom ZID jede Menge Vorkehrungen getroffen, um die Zuverlässigkeit der Telefonanlage zu gewährleisten. Ein wichtiger Punkt dabei sind Wartungsverträge mit garantierten Reaktionszeiten. Wie sieht das bei Skype aus?

> *Furthermore, You acknowledge and agree that Skype, in its sole discretion, may modify or discontinue or suspend Your ability to use any version of the Skype Software,*

Startbedingungen – Wie der Computer zum Telefon wird

Hardware

Wer VoIP ausprobieren möchte, benötigt zuerst einmal einen Computer mit einer Verbindung zum Internet. Die Grundanforderungen sollten bereits mit einem Rechner um die 400 Megaherz und einem 56 Kbps-Modem (V.90 Standard) erfüllt sein, wobei selbstverständlich die Devise gilt: Je leistungsfähiger die Hardware ist, umso qualitativ besser wird das Ergebnis bei der Sprachübertragung sein. Ferner muss der Rechner mit einer Soundkarte ausgestattet sein, die im Vollduplex-Modus arbeiten kann, um gleichzeitiges Hören und Sprechen zu ermöglichen. Zur Spracheingabe bzw. -ausgabe empfiehlt sich, statt separatem bzw. eingebautem Mikrofon und Lautsprechern, ein Headset, also eine Mikrofon-Kopfhörer-Kombination. Hier ist zu beachten, dass ein Computer-Headset im Gegensatz zum Telefon-Headset über zwei separate Anschlüsse (für das Mikrofon und für den Lautsprecher) verfügt, sofern es sich nicht um ein USB-Headset handelt, das ebenfalls verwendet werden kann und sogar ohne Soundkarte funktioniert. Wer lieber einen Hörer in die Hand nehmen will, kann sich auch ein USB-Telefon, Netzwerktelefon oder einen VoIP-Adapter, um ein „normales" Telefon zu nutzen, zulegen. Ein brauchbares Stereo-Headset bekommt man schon ab ca. 15 Euro, für ein USB-Headset muss man ebenfalls ab 15 Euro rechnen. Im Skype-Webshop wird zudem ein preiswertes USB-Telefon bereits um 22 Euro angeboten.

Internetzugang

Vor allem die Anforderungen an die Internetverbindung sind nicht zu unterschätzen, da die Sprache der Teilnehmer während des Gespräches permanent digitalisiert, komprimiert, dekomprimiert und in Form kleiner Datenpakete über das Datennetz, zumeist unter Beteiligung mehrerer Rechner, hin und her transportiert werden muss. In Abhängigkeit von der Datenleistung der Verbindung kann es zu transportbedingten, nicht vollständig eliminierbaren Verzögerungen der Übertragung kommen, die sich in zerhackter oder verzerrter Sprache, in Gesprächsechos oder gar im kompletten Verlust der Daten, sprich einem Gesprächsaussetzer oder gar Gesprächsabriss, äußern.

Studierenden und MitarbeiterInnen der Universität Wien stehen für den Internetzugang von zu Hause verschiedene vergünstigte Angebote zur Verfügung, darunter auch Breitbandzugänge über uniADSL, chello oder xDSL. Ferner können Unet- oder Mailbox-User, die über ein eigenes Notebook mit WLAN-Karte verfügen, sich in Bereichen des WLAN-Service des ZID (siehe auch Seite 53*)* mit dem Datennetz der Uni Wien verbinden und dann beispielsweise aus den Höfen des Alten AKH Gespräche via Internet-Telefonie in die ganze Welt führen. Auf den Webseiten des ZID finden Sie alle Infos zu Konfiguration, Einwahl und Standorten des WLAN-Service unter dem Link `www.univie.ac.at/ZID/wlan/`.

Software

Sofern die benötigte Hardware und ein Internetanschluss vorhanden sind, kann man sich nach einem entsprechenden Programm zur Internet-Telefonie umsehen. Mittlerweile gibt es die verschiedensten Produkte mehrerer Anbieter, von denen Skype neben GMX NetPhone, Freenet iPhone und Yahoo! Voice Messenger wohl am bekanntesten und weitesten verbreitet ist. Welches Produkt das Richtige ist, muss im Endeffekt jeder für sich selbst entscheiden und hängt ganz vom individuellen Geschmack, von den entsprechenden Anwenderkenntnissen sowie den gewünschten Funktionen ab, wobei einige grundlegende Kriterien zu beachten sind: Unmittelbare Computer-zu-Computer-Kommunikation kann nur dann stattfinden, wenn beide Telefonpartner zum Zeitpunkt des Anrufes online sind. Zudem sollten die Teilnehmer über eine gleichwertige Rechnerausstattung verfügen und müssen in jedem Fall kompatible, wenn nicht gar identische Programme auf dem Rechner installiert haben.

VoIP-Clients (Auswahl)

Freenet iPhone:
`www.freenet.de/freenetiphone/`

Gizmo:
`http://gizmoproject.com/intl/de/`

GMX NetPhone:
`http://faq.gmx.de/dienste/netphone/`

SIP Discount:
`www.sipdiscount.com`

sipgate X-Lite:
`www.sipgate.at`

Skype:
`www.skype.com/intl/de/index.html`

SparVoIP:
`www.sparvoip.de`

VoIPBuster:
`www.voipbuster.com/de/index.html`

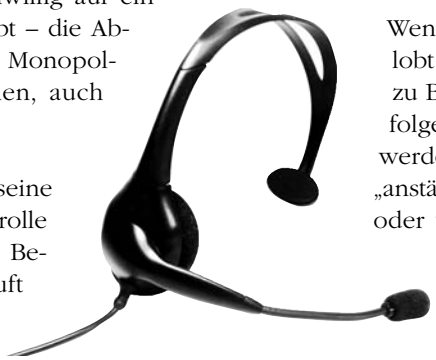
web.de FreePhone:
`www.freephone.web.de`

WengoPhone:
`www.openwengo.com`

Yahoo! Voice Messenger:
`http://de.messenger.yahoo.com/`

and/or disable any Skype Software You may already have accessed or installed without any notice to You, [...] [6]

Eine Selbstverständlichkeit bei jeder Produktion ist die zweite Bezugsquelle. Kein Betrieb setzt freiwillig auf ein Produkt, für das es nur einen Lieferanten gibt – die Abhängigkeit ist unkalkulierbar. Skype ist ein Monopolprodukt. Damit lässt sich kein Staat machen, auch keine Uni.



Jedes seriöse Unternehmen muss sich auf seine Werkzeuge verlassen können, also die Kontrolle darüber behalten, was es tut und was nicht. Bereits bei der Installation von Skype verkauft man jedoch die Seele seines Computers an den Teufel:

4.1 Utilization of Your computer. You hereby acknowledge that the Skype Software may utilize the processor and bandwidth of the computer (or other applicable device) You are utilizing, for the limited purpose of facilitating the communication between Skype Software users. [7]

Von dieser Möglichkeit wird fleißig Gebrauch gemacht:

Die Firma Skype erbringt nämlich die Funktion eines Wählamts – nicht mit eigenen Servern, sondern sie verwendet dafür die Rechenleistung und den Internetanschluss der Skype-User. Wann immer der User mit Skype online ist, kann es passieren – ohne dass der User etwas davon wüsste oder dagegen unternehmen könnte –, dass sein Rechner plötzlich zu einem so genannten *Supernode* wird und anderer Leute Telefonate abwickelt. Das hat drei potentiell verheerende Folgen:

- Es werden, auch ohne dass telefoniert wird, unkontrollierbare Datenmengen transportiert. Pech für die, die ein Download-Limit haben, und besonders schmerzhaft, wenn bei dessen Überschreitung das Datenvolumen verrechnet wird.

- Was es bedeutet, ein Telefonie-Provider zu sein, erfährt der überraschte User möglicherweise erst dann, wenn die Polizei bei Verfolgung eines Drohanrufs oder dergleichen mit dem Einsatzkommando an die Wohnungstür klopft.

- Bildungsnetze wie die Uni Wien bzw. das ACOnet haben dadurch, dass keine Dienste für Dritte an Dritte erbracht werden, in vielfacher Hinsicht eine Sonderstellung, die durch öffentliche Server wie Supernodes gefährdet würde. In Providerverträgen ist, wenn auch aus anderen Gründen, der Serverbetrieb meist ebenfalls verboten.

Ganz allgemein weiß man nicht so genau, was Skype auf dem Computer tut. Die Erinnerung an die Spyware-Funktionen von KaZaA (das, wie gesagt, aus gleicher Hand stammt) lässt Böses ahnen. Konkrete Anhaltspunkte für diesen Verdacht gibt es zwar zur Zeit keine, aber wir können nicht abschätzen, ob oder wann sich das ändern könnte.

Außer Kontrolle...

Wenn Skypes Firewall-Freundlichkeit gelobt wird, stehen dem Netzwerker die Haare zu Berge. In Wahrheit bedeutet das nämlich folgendes: Um auf keinen Fall behindert zu werden, verwendet Skype keine – wie die „anständigen" Services – fixen Portnummern oder wenigstens dedizierte Server. Folglich ist das Sperren, Priorisieren, aber auch nur Messen oder Erkennen von Skype-Datenverkehr – etwa um ihn im Rahmen von *Intrusion Detection Systems* [8] als harmlos einzustufen – mit herkömmlichen Werkzeugen unmöglich. Den Entwicklern war offenbar in der Tradition der Spaßguerilla die unkontrollierbare Hacker-Aura wichtiger als die Einhaltung guter Netzwerk-Sitten.

Angenommen, Skype würde ein ähnlicher Schnitzer passieren wie Microsoft mit seinem MS-SQL-Server. Zur Erinnerung: Der Wurm SQL-Slammer infizierte am 25. Januar 2003 in so kurzer Zeit so viele Rechner, dass es weltweit zu schweren Ausfällen und Beeinträchtigungen im Internet kam. Die Epidemie konnte jedoch eingedämmt werden, da MS-SQL einen fixen Port verwendet, der dann im Netzwerk gesperrt wurde. Sollte Vergleichbares bei Skype passieren, gibt es jedoch kein Mittel, gezielt diesem Problem zu begegnen. Im Wesentlichen bliebe nur, quasi das Internet abzuschalten und auf bessere Zeiten zu warten. [9]

Dadurch, dass Skype Sicherheitslücken aufweist, unterscheidet es sich nicht von anderer Software. In Kombination mit der völligen Unkontrollierbarkeit ergibt sich aber eine neue Gefährdung: Da man nicht weiß, was normal ist, kann niemand feststellen, wenn mit Skype irgendetwas nicht stimmt. Es kann passieren – und nichts rechtfertigt die Annahme, dass das nicht geschehen wird –, dass ein Heer von kompromittierten Skype-Rechnern entsteht, ohne dass irgendjemand etwas davon merkt. Was man mit einem solch immensen Botnet (siehe Artikel *Kammerjäger im Netz* in *Comment 06/1*, Seite 31 bzw. unter `www.univie.ac.at/comment/06-1/061_31.html`) anstellen könnte, will man sich nicht vorstellen.

Software, deren Funktion in keiner Weise nachvollziehbar ist, hat auch auf die Firewall, die Angriffe von außen abwehren soll, Auswirkungen: Die Firewall wird Makulatur. Vom Trojanischen Pferd her kennen wir es alle: Ist der Feind erst einmal innerhalb der Stadtmauern, helfen diese nicht mehr.

Die Filetransfer-Möglichkeiten von Skype verdienen ebenfalls besondere Beachtung. Während die Mailserver des ZID die weitergeleiteten eMails nach Viren durchsuchen

und so einen großen Teil der Schädlinge vom Uni-Netz fernhalten, ist, wegen der Geheimniskrämerei von Skype, eine derartige Maßnahme dort unmöglich. Erfahrungsberichte von Netzen, in denen andere Peer-to-Peer-Programme gefiltert wurden, deuten darauf hin, dass bis zu zwei Drittel der Viren auf diesem Weg übertragen wurden.

Warnung des Gesundheitsministers

Es gibt also durchaus gute Gründe – und viele davon gelten ebenso für die meisten anderen P2P-Programme – auf die Benutzung von Skype zu verzichten: Aus der Sicherheitsperspektive ist die Benutzung des Skype-Clients zumindest sehr bedenklich, und für ein nicht gerade lebensnotwendiges Produkt ein Risiko einzugehen, zahlt sich wohl kaum aus. Der CERN [10] – immerhin die Wiege des World Wide Web – ist sogar so weit gegangen, die Verwendung von Skype zu verbieten. [11]

Auf keinen Fall sollte man auf die Idee kommen, mit Skype ließe sich die herkömmliche Telefonie auch nur teilweise ersetzen und damit gar auch noch Geld sparen.

Der ZID der Universität Wien kann keine Empfehlung für die Verwendung von Skype abgeben, will aber die bisherige Übung, die Freiheit von Forschung und Lehre durch möglichst liberale Handhabung des Datennetzes zu unterstützen, fortsetzen. Deswegen gibt es vorerst kein direktes Verbot. In jedem Fall ist es sinnvoll, Skype und alle anderen Peer-to-Peer-Programme aufmerksam und kritisch im Auge zu behalten. Wie allerdings der Laie diese Verantwortung wahrnehmen soll, wenn sogar die Experten nicht recht wissen, was bei Skype abläuft, ist unklar und wir raten daher zur Enthaltsamkeit.

Anmerkungen:

[1] KaZaA ist eine Internet-Tauschbörse basierend auf dem Peer-to-Peer-System, die durch integrierte Spyware (Software, die persönliche Daten des Benutzers ohne dessen Wissen oder gar Zustimmung an den Hersteller der Software oder an Dritte sendet) in Verruf gekommen ist.

[2] Eine fundierte Analyse dessen, was sich dennoch beobachten lässt, stellt Simson L. Garfinkel in seinem Paper *VoIP and Skype Security* dar: `www.tacticaltech.org/files/tacticaltech/Skype_Security.pdf`

[3] Mit einer Ausnahme: Für den Login-Vorgang verwendet Skype den Port, der eigentlich für Webseiten reserviert ist, und entzieht sich somit auch hier jeder Kontrolle.

[4] *The Internet Standards Process – Revision 3*: `http://ftp.univie.ac.at/netinfo/rfc/rfc2026.txt`

[5] Unter `www.secdev.org/conf/skype_BHEU06.handout.pdf` findet sich zwar eine Analyse einer bestimmten Skype-Version; da Skype seine Software und ihr Verhalten aber jederzeit ändern kann, stellt diese Analyse lediglich eine Momentaufnahme dar.

[6] EULA 2.5: `www.skype.com/company/legal/eula/`

[7] EULA 4.1, 4.2: `www.skype.com/company/legal/eula/`

[8] *Intrusion Detection Systems* sind Software- oder Hardware-Werkzeuge, mit denen unauthorisierte Zugriffe auf Computersysteme oder Netzwerke aufgespürt werden können.

[9] Das ist übrigens kein an den Haaren herbeigezogenes Szenario: Am 25. Oktober 2005 wurde eine Lücke in Skype gefunden, die genau wie damals beim MS-SQL-Server die Ausführung beliebigen Codes durch ein einziges UDP-Paket erlaubt. Glücklicherweise war der Entdecker verantwortungsbewusst und hat den Fehler bei Skype gemeldet, statt einen Wurm zu schreiben.

[10] CERN: Europäische Organisation für Kernforschung, an der Tim Berners-Lee im Jahr 1990 die Idee des WWW (*World Wide Web*) auf den Weg brachte.

[11] siehe `http://security.web.cern.ch/security/skype/`

✧ ✧ ✧

Zum Weiterlesen und -klicken:

Wer sich eingehender über das Thema IP-Telefonie informieren möchte, der sei auf den Artikel *Infrastructure ENUM – Die Inter-Net(z)-Verbindung für Telefonprovider* auf Seite 36 verwiesen.

Weiteres erfahren Sie im Artikel *ENUM: Eine Nummer Und Mehr – Telefonie und Internet verbünden sich* in *Comment* 05/1, Seite 27 bzw. unter `www.univie.ac.at/comment/05-1/051_27.html`.

Ebenso sei hier auf die Notiz *Nebenstellen der Uni Wien über VoIP erreichbar* auf Seite 31 verwiesen.

Ausführliches Funktionsprinzip von IP-Telefonie:
`http://de.wikipedia.org/wiki/IP-Telefonie`

FAQ zu VoIP – Antworten auf die häufigsten Fragen:
`www.heise.de/ct/05/18/174/default.shtml`

Skype aus Sicht einer Userin – *Revised*

Pro und Contra für Skype sollten nun erst einmal auf der Hand liegen. Vor allem die Argumente gegen diesen Client erscheinen einleuchtend, denn wer hätte ehrlich gewusst, was ein Supernode ist oder warum die Verwendung einer fixen Portnummer sicherheitsrelevante Bedeutung hat? Ob Skype dagegen nun wirklich Böses im Schilde führt oder ob die Verschlüsselung rein wettbewerbsrelevante Hintergründe hat, um die eigene Marktposition zu verteidigen, bleibt vorerst unbeantwortet.

So stellt sich nun die Frage, was davon abhält, einfach auf eine andere, vergleichbare, noch weniger bekannte VoIP-Software umzusteigen? Warum gerade Skype so bekannt und überaus erfolgreich ist, bleibt nur mehr zu erahnen. Mit Sicherheit, weil sie mit die ersten waren, die ein ausgefeiltes Marketing betrieben haben, weil es eben so prima einfach und unkompliziert funktioniert und es deswegen viele verwenden.

Weiterhin skypen?

Dabei beweist gerade letzterer Punkt enormes Gewicht. So zeigt ein pflichtbewusster Selbstversuch, den mit Skype vergleichbaren VoIP-Client WengoPhone downzuloaden, bereits beim ersten Klick auf die Website (`www.openwengo.com`) die Marketing-Fauxpas der WengoPhone-Macher: Die Seite gibt es nämlich nur auf Englisch und Französisch – neuerdings auch Mandarin, wem das hilft (dazu Skype im Vergleich: die Website gibt es in 24 Sprachen).

Hat man diese Hürde genommen, klappt es mit Download und Installation dann genauso gut wie mit Skype. OpenWengo schenkt dazu jedem neu registrierten User 80 Eurocent für netzübergreifende Telefonate oder – was Skype bisher nicht kann[9] – um SMS zu versenden. Klingt und funktioniert soweit gut! Neues Problem jetzt: Außer mir kenne ich keinen Menschen, der WengoPhone benutzt. Kostenlose Gespräche sind somit erst mal keine drin (und jemand völlig Fremden anzurufen, habe ich jetzt auch keine große Lust ...). Bliebe wieder nur die eMail an Freunde, Verwandte etc. Aber auch das ist schwierig, jetzt, wo man mal Skype hat.

Zudem ist Skype mittlerweile an vielen prägnanten – scheinbar vertrauenswürdigen – Ecken des WWW anzutreffen. So wurde Skype erst kürzlich an das Online-Auktionshaus Ebay (`www.ebay.at`) verkauft, das zukünftig Internet-Telefonie in seine Auktionen einbauen will. Nutzerstarke Kontaktbörsen wie z.B. die Business-Plattform OpenBC (`www.openbc.com`) oder die österreichische Singlebörse Websingles (`www.websingles.at`) haben die Referenz des Skype-Usernamens bereits in ihre Profilvorlage fest integriert. Das trägt nicht nur dazu bei, die Skype-Gemeinschaft ungemein zu erweitern, sondern setzt damit auch gegenüber diesem Client einen Vertrauensvorschuss in Gang, der heutzutage vielerorts im Netz vorausgesetzt wird.

Wachsamkeit statt Hausverbot

Nichtsdestotrotz ist das Bewusstsein für Sicherheit im Netz und von elektronischen Daten bei den meisten von uns sehr wohl vorhanden. Wir wissen, dass wir nicht jeder eMail sorglos trauen dürfen, da sie Viren oder gefälschte Links enthalten kann (mehr dazu ist im Artikel *Phishing: Bitte nicht anbeißen!* auf Seite 37 zu finden), dass man sich mit unbedachten Klicks auf Webseiten böswillige Dialer einfangen kann. Wir haben schon mal von Spyware und Cookies gehört, die versuchen, Daten und Surfverhalten auszuspionieren. Man ist vorsichtig geworden. Man überlegt durchaus, sich ein Programm wie Skype einfach herunterzuladen, und hätte sicher größere Bedenken, wenn es nicht aus „vertrauenswürdigen" Quellen käme. Und in letzter Instanz fühlen wir uns noch immer von unserer Firewall geschützt, über deren Achillesferse man aus diesem Artikel gelernt haben sollte.

Größeres Augenmerk ist wohl auch auf die Supernode-Eigenheit von Skype zu richten, insbesondere dann, wenn man über einen trafficlimitierten Internetanschluss verfügt, beispielsweise *chello StudentConnect*. Wer sich Gedanken über sein Datenvolumen macht, kann sich mit einem kleinen Zusatzprogramm[10] ganz einfach die übertragenen Datenmengen anzeigen lassen.

Koexistenz

Was Ausfallsicherheit, Wartungsverträge, Notrufe etc. angeht: Bisher deuten noch alle Zeichen darauf hin, dass VoIP-Clients nach Vorbild Skype als reines Zusatzangebot zur herkömmlichen Telefonie in klar umrissenen Bereichen genutzt werden. Dass Skype tatsächlich in näherer Zukunft Festnetztelefon oder gar Handy ersetzt, ist nicht abzusehen. So bleibt auch die klassische Telefonie der Uni Wien in ihren Grundfesten von kostenloser Internet-Telefonie erst einmal völlig unberührt. Hier sind die Entwicklungen rund um ENUM (siehe Artikel *Infrastructure ENUM – Die Inter-Net(z)-Verbindung für Telefonprovider* auf Seite 36) weitaus interessanter.

So spricht durchaus eine ganze Reihe an Faktoren dafür, Skype trotz aller Bedenken weiterhin – wenn auch differenzierter und gegenüber seinen Unzulänglichkeiten sensibler – zu verwenden. Zurück bleibt vielmehr ein kritisches Hinterfragen und Beobachten, ob und was Skype in Zukunft von sich hören lässt.

Katharina Lüthke ■

9) In der aktuellen Beta-Version ist diese Funktion bereits vorhanden, womit zu erwarten ist, dass demnächst auch mit Skype SMS versandt werden können.

10) z.B. Net Meter 3.0 (`www.mp3cdsoftware.com/net-meter-download-19912.htm`) oder Online Eye 2.11 (`http://download.freenet.de/archiv_o/online_eye_4275.html`) für Windows; für Mac-User gibt es Net Monitor (`http://homepage.mac.com/rominar/net.html`)

INFRASTRUCTURE ENUM

Die Inter-Net(z)-Verbindung für Telefonprovider

Als im Dezember 2004 die weltweit erste ENUM-Registrierungsstelle[1] in Österreich in Betrieb genommen wurde, hatte auch der ZID der Universität Wien Grund zum Feiern: Die Software-Entwicklung und die Implementierung dieses Service wurde von derselben Arbeitsgruppe am Zentralen Informatikdienst durchgeführt, die auch die technischen Bereiche des Registry-Service der nic.at seit Jahren erfolgreich betreut (siehe Kasten *Who is who?*).

Ende April 2006 fiel der Startschuss für den zweiten Teil der ENUM-Story: Die RTR GmbH beauftragte enum.at mit dem Betrieb einer neuen ENUM-Variante, wobei für die technische Realisierung dieses so genannten „Infrastructure ENUM" wiederum der Zentrale Informatikdienst der Uni Wien verantwortlich zeichnet. Der Testbetrieb hat bereits im Mai 2006 begonnen.

Who is who?

enum.at

Die *enum.at GmbH* (`www.enum.at`), eine Schwesterorganisation von nic.at, verwaltet die österreichische ENUM-Zone `3.4.e164.arpa` sowie das neue Infrastructure ENUM.

nic.at

Die *nic.at Internet Verwaltungs- und Betriebsgesellschaft m.b.H.* (`www.nic.at`) ist für die Registrierung und Verwaltung aller Domains unter `.at`, `.co.at` und `.or.at` zuständig – also für die gesamte österreichische Topleveldomain mit Ausnahme des Bildungsbereichs (`.ac.at`), der vom österreichischen Wissenschaftsnetz ACOnet (`www.aco.net`) verwaltet wird.

RTR GmbH

Die *Rundfunk und Telekom Regulierungs-GmbH* (`www.rtr.at`) fungiert als österreichische Regulierungsbehörde für Rundfunk und Telekommunikation.

ZID

Die Entwicklung der Registry-Software sowie der technische Betrieb des Registry-Service für die `.at`-Topleveldomain, für das User-ENUM und für das Infrastructure ENUM wird von der Arbeitsgruppe *Internet-Domainverwaltung* des Zentralen Informatikdienstes der Universität Wien (`www.univie.ac.at/ZID/`) durchgeführt.

Was ist ENUM?

ENUM steht für *Electronic NUmber Mapping* – ein Standard, der regelt, auf welche Weise Informationen zu Telefonnummern im DNS (*Domain Name System*, eine globale Datenbank zur Umwandlung von Hostnamen in IP-Adressen) gespeichert werden können. Die Hauptanwendung dafür liegt im Zusammenschluss von klassischem Telefonnetz (PSTN, *Public Switched Telephone Network*) und VoIP (*Voice over IP*, Telefonieren über das Internet). Während im PSTN Telefonnummern zur Adressierung von TeilnehmerInnen verwendet werden, sind es bei VoIP üblicherweise Adressen der Form `sip:`*`user@domain`*. ENUM vermittelt zwischen diesen Welten, indem es eine Übersetzung von Telefonnummern auf VoIP-Adressen ermöglicht.

User-ENUM

Das Zielpublikum für die ENUM-Variante, die im Dezember 2004 in Österreich in Betrieb genommen wurde („User-ENUM"), sind die EndkundInnen: Der jeweilige Nummerninhaber hat das Verfügungsrecht über die ENUM-Domain zu seiner Telefonnummer. Das ist primär dann interessant, wenn der Nutzer selbst eine VoIP-Infrastruktur – etwa eine moderne Nebenstellenanlage – betreibt. In diesem Fall ermöglicht ENUM die automatische Kopplung solcher Nebenstellenanlagen über das Internet, sodass für Gespräche zwischen ENUM-NutzerInnen keine Dienste von Telefonnetz-Betreibern mehr benötigt werden.

Infrastructure ENUM

Die Kopplung von VoIP-Systemen ist aber nicht nur auf der Ebene von privaten VoIP-Geräten oder Firmen-Nebenstellenanlagen ein Thema, sondern auch zwischen Netzbetreibern: Auch dort ersetzen VoIP-basierte Lösungen zunehmend die klassische Vermittlungstechnik. Ob die KundInnen per VoIP oder über andere Technologien angebunden sind, spielt dabei kaum eine Rolle.

Wenn – wie es jetzt bereits geschieht – die Kernnetze auf VoIP umgestellt werden (bzw. neue Betreiber erst gar keine alten Systeme einsetzen), ist es natürlich sinnvoll, die Querverbindungen zwischen den Providern ebenfalls auf VoIP umzustellen. Auch hier braucht man ENUM, um eine Telefonnummer auf eine VoIP-Adresse umzusetzen.

---

1) Ausführliche Informationen über ENUM finden Sie im Artikel *ENUM: Eine Nummer Und Mehr – Telefonie und Internet verbünden sich* in *Comment 05/1*, Seite 27 bzw. unter `www.univie.ac.at/comment/05-1/051_27.html`.

Dieses „Infrastructure ENUM“ (kurz I-ENUM) unterscheidet sich vom User-ENUM in einigen wesentlichen Punkten:

- Der Netzbetreiber trägt seine Rufnummern ein. Die Zustimmung des Nummerninhabers ist dazu nicht nötig; dieser kann auch nicht die im I-ENUM abgelegten Informationen bestimmen.
- Eine Überprüfung (Validierung) der Nutzungsberechtigung ist nicht erforderlich.
- Die VoIP-Adressen sind nicht mehr notwendigerweise offen erreichbar, sondern die Netzbetreiber können definieren, von welchen anderen Betreibern sie Gespräche per VoIP annehmen wollen.
- Beim User-ENUM werden die Adressinformationen zu den Rufnummern bei der jeweiligen Registrierungsstelle gehalten (die übergeordnete Registry macht nur entsprechende Verweise), beim Infrastructure ENUM werden sie hingegen direkt in der zentralen Registry-Datenbank verwaltet.

Eine direkte Verbindung per VoIP hat für die Netzbetreiber viele Vorteile – nicht zuletzt auch finanzielle: Da die Zusammenschaltung von zwei Betreibern keine dedizierte physikalische Verbindung mehr benötigt, sondern das Internet als Transportmedium nutzt, lassen sich Transitnetze vermeiden und somit die Kostenstrukturen im Telefonnetz revolutionieren.

Otmar Lendl (enum.at) & Gerhard Winkler ■

PHISHING: BITTE NICHT ANBEISSEN!

Als versucht wurde, mittels Massenmails und gefälschter Webseiten die Zugangscodes der KundInnen einiger österreichischer Banken zu stehlen, wurde *Password Fishing*, kurz *Phishing*[1)], plötzlich auch hierzulande als Bedrohung wahrgenommen. Dabei kämpft der gesamte eCommerce von Anfang an mit zwei Problemen.

Das erste: Die KundInnen misstrauen dem elektronischen Hokuspokus und shoppen und „banken“ nur zögerlich online. Das ist schade für die Firmen (schließlich ließen sich doch auf diese Weise Kosten sparen), und so begegneten sie dieser Herausforderung fachgerecht und nicht ohne Erfolg mit der Werbekeule.

Das andere Problem liegt tiefer und Fachleute wissen es schon längst: Das Misstrauen der technikfeindlichen eSkeptiker ist nicht ganz unberechtigt. Zwar haben – wie der Artikel *WWW + SSL = HTTPS* auf Seite 46 zeigt – die TechnikerInnen einiges unternommen, um elektronische Transaktionen sicher abwickeln zu können, doch der Faktor Mensch bleibt ein mitunter recht schwaches Glied in der Kette.

Die Rache der Benutzerfreundlichkeit

In ein Geschäft gehen, eine Wurstsemmel verlangen und ein paar Münzen hinlegen – das durchschaut jedes Kind, und allen Beteiligten ist wenigstens im Prinzip klar, worauf sie aufpassen müssen, um nicht über den Tisch gezogen zu werden. Dennoch finden BetrügerInnen immer wieder ein Opfer.

In der virtuellen Welt haben die intuitive Bedienbarkeit und die enorm gestiegene Benutzerfreundlichkeit zweierlei Erfolge gebracht: Jeder kann etwas mit dem Computer anfangen, und niemand weiß mehr, was er eigentlich tut. Wer hat schon eine Ahnung, was passiert, wenn wir auf der Telebanking-Webseite irgendwohin klicken? Wer kann sagen, worauf wir aufpassen müssen, um nicht übers Ohr gehauen zu werden? Nur ein verschworener Klüngel von Bitologen und Byte-Experten ist, wenn überhaupt, in der Lage, von sich aus die lauernden Gefahren zu überschauen und zu vermeiden.

Ergebnis: Nicht weil die Technik versagt, ist Internet-Betrug so einfach, sondern weil sie ihre AnwenderInnen beherrscht anstatt umgekehrt.

Das Kind nicht mit dem Bade ausschütten

Einerseits nicht der Paranoia zu verfallen und die ganze Computerei zum Teufel zu jagen, andererseits dennoch ein sozial verträgliches Maß an Sicherheit für die BenutzerInnen herzustellen, ist eine große Herausforderung, der wir alle uns jetzt stellen müssen.

Serverbetreiber und Softwarehersteller müssen, das versteht sich von selbst, ihre Systeme dem Stand der Technik entsprechend konzipieren und dafür sorgen, dass allfällige

1) Die Benennung erfolgte in Anlehnung an das in den frühen 90er-Jahren in Hacker-Kreisen übliche *Phreaking*, das von *Phone Freak* abgeleitet wurde.

Fehler unverzüglich behoben werden. Das ist der vergleichsweise einfache Teil.

Wesentlich komplizierter ist es, Rahmenbedingungen zu schaffen, die Sicherheit ermöglichen:

- Da neue Features neue Käufer anlocken und Geldverdienen das Ziel jeder Firma ist, werden gerne neue Funktionen erfunden. Dort allerdings, wo die Beherrschbarkeit und Sicherheit des Produkts gefährdet sind, müssen dem Featurismus Grenzen gesetzt werden. Ein Beispiel, das uns bereits viele Tränen gekostet hat: Die Möglichkeit, kinderleicht mit einem Mausklick aus einer eMail heraus neue Software zu installieren und auszuführen, hat sich als extrem ärgerliches und teures Feature erwiesen. Der Großteil aller Würmer, Viren und Trojaner – die heute zunehmend kriminellen Zwecken dienen[2)] und sich auch für Phishzüge vorzüglich eignen – kam so in die PCs, und dass das passieren musste, war abzusehen.

  Brauchbare Ansätze für einen diesbezüglichen Paradigmenwechsel sind leider rar. Auch Microsofts kommendes Betriebssystem Windows Vista, in dem Security als Feature vermarktet wird, dürfte sich in dieser Hinsicht eher als Marketing-Luftblase erweisen (siehe dazu den Artikel *Veni, vidi – und testete Vista!* auf Seite 18).

- Nur sehr zögerlich spricht sich in die Chefetagen durch, dass Sicherheit ein unternehmenskritischer Prozess ist, der bei Entscheidungen unbedingt berücksichtigt werden muss. Eine gesunde Balance zwischen der Technokratie paranoider Hacker[3)] und der Erfolgsorientiertheit bilanzfixierter Schlipsträger[4)] zu finden, erfordert einige Dialogbereitschaft zwischen diesen beiden Gruppen, die einander leider eher als natürliche Fressfeinde erleben dürften.

- Die BenutzerInnen müssen selbstverständlich über den richtigen und sicheren Umgang mit den Systemen, die sie verwenden sollen, Bescheid wissen. Dazu gehört ein ausreichendes Verständnis von deren inneren Abläufen – zumindest so weit, dass man einigermaßen beurteilen kann, was man gerade im Begriff ist zu tun.

In Bezug auf Phishing gibt es eine gute Nachricht: Eigentlich sind es gar nicht so viele Dinge, auf die man achten muss, um einigermaßen sicher durch – und eben nicht in – das Netz zu gehen.

Die Bedrohung

Bevor wir auf Angriffe und Gegenmaßnahmen eingehen, sei das Bedrohungsszenario skizziert, das als Phishing bezeichnet wird.

Als Ersatz für das persönliche Erscheinen im Geschäft, das eine Identität bildet, weist man sich beim digitalen Shopping in den meisten Fällen durch Nennung eines Namens (UserID, Kontoname, Nickname) und eines Geheimnisses (Passwort, PIN, Geheimzahl) aus.[5)] Wird die Kombination von Name und Geheimnis Dritten bekannt, können diese im Namen des Berechtigten alle Verfügungen treffen, die das System ermöglicht. Bei einem Bankkonto sind die Konsequenzen offensichtlich.

Es gibt eine ganze Reihe von Wegen, wie das vertrauliche Passwort in die falschen Hände geraten kann. Die meisten davon fallen in eine der beiden folgenden Kategorien:

- Der Geheimnisträger gibt es freiwillig preis[6)] oder

- der Bösewicht belauscht den Geheimnisträger, während dieser sich mit dem Passwort ausweist.

Eine Variation dieses Themas, wenn z.B. Einmalpasswörter, TANs oder zeitabhängige Passwörter verwendet werden:

- Der Bösewicht klinkt sich in die Kommunikation zwischen Geheimnisträger und System ein und verändert deren Inhalt.

Die scheinbar einfache (Techniker-)Antwort auf diese Probleme – *„Verwenden Sie doch HTTPS!“*[7)] – hat allerdings einen Haken: HTTPS hilft nicht, wenn der Benutzer nicht den Server seiner Bank, sondern den des Bösewichts kontaktiert. Ihn dazu zu überreden, genau darum geht es beim Phishing.

Panik killt gesunden Menschenverstand

Technik wird häufig als kinderfressendes Monster erlebt, vor dem man sich lieber fürchtet, als gelassen darüber nach-

2) siehe Artikel *Kammerjäger im Netz* in *Comment 06/1*, Seite 31 bzw. www.univie.ac.at/comment/06-1/061_31.html

3) Seebach, Peter: *The Hacker FAQ* (www.plethora.net/~seebs/faqs/hacker.html)

4) Seebach, Peter: *The Manager FAQ* (www.plethora.net/~seebs/faqs/manager.html)

5) Chipkarten stellen bei der Mehrzahl der Anwendungsszenarios lediglich eine teilweise Verbesserung mit enttäuschendem Sicherheitsgewinn dar.

6) Dies ist ein Vorteil der Passwörter: Man kann erforderlichenfalls ein Recht befristet hergeben und gleich darauf durch Änderung des Passworts wieder zurücknehmen. Bei biometrischen Verfahren geht beides nicht.

7) siehe Artikel *WWW + SSL = HTTPS* auf Seite 46

8) Glücklicherweise handelt es sich hier noch um eine Simulation: Das Passwort-Formular versendet das eingegebene Passwort nicht, und der abgerufene Server befindet sich im Wohnzimmer des Autors. Obwohl die verlinkte Seite von einer Uni-Webseite optisch kaum zu unterscheiden ist, hat dieser „Phishing-Server“ – wie beim echten Phishing – netzwerktechnisch und administrativ nichts mit der Universität Wien zu tun.

zudenken. Angenommen, jemand würde folgende Nachricht massenweise an Uni-Mailadressen verschicken:

```
From: Sicherheit <password@univie.ac.at>
To: Uni-Angehoerige <password@univie.ac.at>
Subject: Diebstahl Ihres Passwortes

Sehr geehrte Damen und Herren,

Österreich ist derzeit von einer großangelegten
elektronischen Betrugswelle betroffen. Es mehren
sich die Berichte, dass in zahlreichen öffent-
lichen Einrichtungen die geheimen Nutzerkennungen
gestohlen worden sind. Damit können jetzt Unbe-
kannte Ihre eMail lesen, auf Ihre Dateien zu-
greifen, Ihre Homepage ändern, ein Diensthandy
bestellen, mittels CTI Ihr Telefon kontrollieren
und so weiter.

Wir ersuchen Sie dringend, Ihre Nutzerdaten auf
folgender Webseite zu prüfen:

http://security.univie.atat.at/validation.htm

Damit können wir sichergehen, dass Ihr Zugang
nicht missbraucht wurde. Wenn Sie nicht innerhalb
der nächsten Tage Ihren Zugang bestätigen, müssen
wir diesen leider deaktivieren.

Mit freundlichen Grüßen,
Ihre IT-Sicherheitsabteilung
```

Selbst wenn die Mehrheit unserer BenutzerInnen sich nicht ins Bockshorn jagen lässt: In der ersten Aufregung über die Gefahr eines massiven Eingriffs in die Privatsphäre würden wohl allzu viele sofort auf den angegebenen Link klicken. Dieser führt aber nicht zu einer Seite der Uni Wien (auch wenn die angezeigte Seite so aussieht), sondern zu einem Phishing-Server.[8)] Auf diese Weise könnten angesichts unserer nicht geringen Benutzerzahlen sicher einige tausend Mailbox- und Unet-Passwörter „gewonnen“ werden.

Was ist passiert? Der Geheimnisträger hat sich reinlegen lassen und selbst sein Geheimnis verraten. Dagegen sind keine technischen Maßnahmen möglich. Hilfreich, aber leider nur spärlich vorhanden, sind Schulungen und eindeutige Handlungsanleitungen.

Gute Ratschläge, kostenlos

Aus dem geschilderten Szenario lassen sich einige allgemeine Empfehlungen ableiten:

- Achten Sie bei sensiblen Transaktionen darauf, dass der URL der angezeigten Seite mit `https://` beginnt und dass das **Schloss-Symbol rechts unten im Browserfenster geschlossen**  ist (im Browser Firefox wird bei verschlüsselten Seiten zusätzlich die Adresszeile gelb hinterlegt). Lassen Sie sich nicht von Bildchen innerhalb einer Seite, die behaupten, diese sei sicher, in die Irre führen: Jeder HTML-Anfänger kann ein Logo in eine Webseite einblenden.

- Rufen Sie sensible Seiten soweit wie möglich über die **Bookmark-Funktion** Ihres Browsers auf (für den Urlaub können Sie diese auch als Webseite exportieren und auf Ihrer Homepage an geeigneter Stelle speichern). Dann kann Ihnen niemand plötzlich einen gefälschten URL unterjubeln.

- Prägen Sie sich wenigstens bei Ihrer Bank den **Domainnamen** ein und behalten Sie im Auge, wie deren URLs aussehen. Wenn diese nicht mehr wie gewohnt – z.B. mit `https://telebanking.meine-bank.at/` – beginnen (zu beachten sind `https`, der richtige Domainname und dass der Schrägstrich unmittelbar dahinter liegt), sondern stattdessen beispielsweise

  - `https://192.168.23.44/xxx`
    (also eine IP-Adresse),

  - `https://telebanking.meine-bank.at@eine.andere.domain/xxx`
    (also ein @-Zeichen vor dem Schrägstrich),

  - `https://telebanking.meine-bank.as/xxx`
    (also ein anderes Land) oder

  - `https://telebanking.maine-bank.at/xxx`
    (also eine geringfügig abweichende Schreibweise)

  erscheint, sind Sie höchstwahrscheinlich auf einer Phishing-Seite gelandet. Leider sind mehr Methoden der URL-Verschleierung bekannt, als hier aufgezählt werden können, aber häufig geben sich Phisher in dieser Hinsicht keine besondere Mühe.

- Wenn Sie den Verdacht haben, fehlgeleitet worden zu sein, kontrollieren Sie das **Zertifikat** (siehe Seite 50): Stimmen Name und Adresse? Ist der Aussteller vertrauenswürdig, ist die Zertifikatskette vollständig? Eine gute Idee ist es, das bereits frühzeitig an bekannten Seiten (z.B. `https://www.univie.ac.at/`) auszuprobieren.

- Vorsicht bei Links, die Sie **per eMail** erhalten haben! Diesem wichtigen Punkt widmet sich der folgende Abschnitt.

Gefahrenquelle eMail

Über die Probleme, die eMail als Virenträger und Belästigungsmedium mit sich bringt, wird seit Jahren in allen einschlägigen Medien ausführlichst berichtet. Die zahlreichen Täuschungsmöglichkeiten werden durch das fragwürdige Feature „formatierter“ HTML-Mails um eine Facette bereichert, die zum Missbrauch förmlich einlädt:

Wenn Sie in einer eMail einen Link auf `https://telebanking.meine-bank.at/xxx` sehen, bedeutet das noch lange nicht, dass Sie ein Klick darauf auch tatsächlich zur angegebenen Seite führt. Was bei Webseiten normal ist, nämlich dass sich der auf der Seite angezeigte Link-Text

ZID, fisch mit!

Unfreiwillige Mithilfe beim Phishing

Wer phishen geht, möchte dabei natürlich nicht erwischt werden. Daher verwenden Phisher nicht ihren eigenen Server, sondern missbrauchen fremde Rechner, zu denen sie irgendwie Zugang erhalten haben. Ist ein solcher gekaperter Rechner im Bereich des österreichischen Wissenschaftsnetzes ACOnet angebunden, sorgt das ACOnet-CERT (siehe Artikel *Kammerjäger im Netz* in *Comment 06/1*, Seite 31 bzw. unter `www.univie.ac.at/comment/06-1/061_31.html`) dafür, dass dieser Zustand schnellstmöglich behoben wird. In den meisten Fällen ist der Tathergang relativ unspektakulär: Mit Hilfe eines Virus (genauer: Trojaners) oder eines schwachen Passworts, das mittels automatisiertem Ausprobieren „erraten" wurde, bemächtigt sich der Phisher eines Rechners und missbraucht ihn – vom Anwender unbemerkt – als Webserver für Phishing-Seiten. Einmal jedoch war unser eigener Webserver WWW.UNIVIE.AC.AT auf ungewöhnliche Art und Weise daran beteiligt, Zugangsdaten einer südamerikanischen Bank zu erhaschen:

Was geschah?

Die Webseiten eines Instituts der Uni Wien enthielten eine Übung, in deren Rahmen ein Webformular auszufüllen war. Dabei wurde ein verbreitetes, vorgefertigtes CGI-Skript dazu verwendet, die in diesem Formular eingegebenen Daten automatisch per eMail an den Übungsleiter zu übermitteln. Dummerweise ist dieses Skript so gestaltet, dass es sämtliche Anweisungen – vor allem die eMail-Adresse, an welche die Daten zu senden sind – aus den ihm übergebenen Formulardaten nimmt. Unserem Phisher kam dieses Übungsskript gerade recht: Da es willig und ungeprüft beliebige Daten an beliebige Adressen sendet, spielte es ihm auf nur schwer nachzuvollziehende Weise die erschlichenen Bankcodes zu. Um es zusammenzufassen: Ein von einem Institut auf dessen Webseiten installiertes Skript zur Auswertung von Webformularen wurde von einem Phisher für seine Zwecke mitverwendet, und dazu musste dieser nicht einmal in den Uni-Webserver einbrechen.

Die Reaktion

Als die betroffene Bank das ACOnet-CERT kontaktierte, waren die Phishing-Webseiten, die auf den Uni-Webserver verwiesen hatten, bereits aus dem Netz genommen worden. Von Seiten des Instituts wurde das Skript zügig entfernt. Die Logfiles des Webservers verzeichnen auch den sogenannten *Referer*, das ist die Seite, von welcher der Besucher auf den Server verwiesen wurde. Daraus ergab sich, dass das missbrauchte Skript an diesem Tag nur von Phishing-Opfern aufgerufen worden war. Um der Bank die Chance zu geben, die Kunden, die auf den Phishzug hereingefallen waren, zu identifizieren und zu warnen, wurden ihr etwa 250 betroffene IP-Adressen übermittelt.

Spurensuche

Leider war nicht mehr feststellbar, wohin die Formulardaten gesendet wurden: Da die Phishing-Webseiten bereits entfernt worden waren, konnten wir den Vorgang nicht mehr „live" beobachten. Das Skript selbst führt keine Protokolle und verwendete für den Versand keine uns bekannten Mailserver, deren Logfiles uns Hinweise hätten geben können.

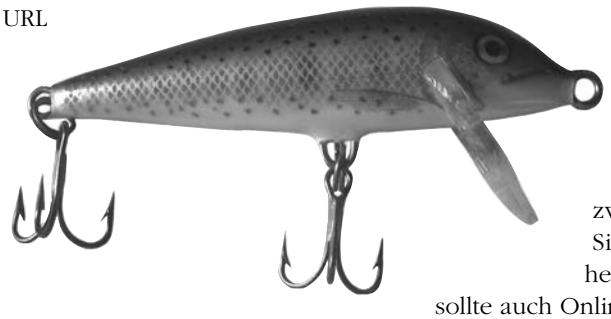
Eine weitere Frage beschäftigte uns: Wie kam ein offenbar im spanischen Sprachraum agierender Phisher darauf, dass es tief vergraben in den Webseiten eines österreichischen Universitätsinstituts ein Skript namens `uebung.cgi` gibt, das sich gut gebrauchen lässt? Ein Blick auf den Referer, der beim ersten Zugriff auf dieses Skript im fraglichen Zeitraum aufgezeichnet worden war, beantwortete diese Frage (Daten leicht verändert):

```
10.14.60.123 - - [16/Mar/2006:02:45:48 +0100] "GET /Institut/Lehre/uebung.cgi HTTP/1.1"
200 47 "http://www.google.es/search?hl=es&q=inurl%3A.cgi+intitle%3ANo+input+data&meta="
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)"
```

Des Rätsels Lösung: Der Robot von Google gibt beim Indizieren des fraglichen Skripts natürlich keine Formulardaten ein. Das führt zur Fehlermeldung *No input data*, und diese wird von Google gespeichert. Genau danach – das ist im Referer zu lesen, da bei Google die Frage immer Teil des URLs ist – hat der Phisher gesucht und auf diese Weise zu uns gefunden. Die gezeigte Abfrage wurde also vom Phisher selbst getätigt; folglich hätte `10.14.60.123` seine IP-Adresse sein müssen. Leider führte auch diese Spur nicht zum Täter: Es handelte sich um einen trojanisierten PC, der als Proxy missbraucht wurde. Naturgemäß war nicht mehr festzustellen, von woher der Phisher auf diesen PC zugegriffen hatte.

Eine Konsequenz konnten wir aus dem Ereignis ziehen: Wir befragen jetzt selbst regelmäßig Google, um solche verwundbaren Skripts in unserem Netz aufzuspüren und deren Betreiber rechtzeitig warnen zu können.

und der tatsächlich verlinkte URL unterscheiden, kann in eMails gewinnbringend verwendet werden: Gezeigt wird der richtige URL der Bank, verwiesen wird hingegen auf die Phishing-Seite.



Die notwendigen Vorsichtsmaßnahmen sind also eigentlich ganz einfach:

- **Links, die Sie per Mail erhalten haben, sollten Sie möglichst überhaupt nicht anklicken.** Besonders wenn es sich um ein Service handelt, für das Sie ein Passwort oder dergleichen besitzen, ist es besser, dessen Homepage aus den Bookmarks heraus aufzurufen und zu versuchen, mittels „Durchklicken" zur angegebenen Seite zu gelangen.

- Je dringlicher die Nachricht ist und je größer die geschilderte Katastrophe: **Überprüfen Sie, z.B. durch Anruf bei der Hotline, ob die Story echt ist.** Die Telefonnummer dürfen Sie natürlich nicht der eMail entnehmen – es könnte ja auch die gesamte Hotline ein Fake sein.

- Wenn Sie meinen, dass Sie dem Absender vertrauen können, und einen Link daher doch anklicken wollen, sollten Sie folgende Punkte beherzigen:

  - **Geben Sie keine Passwörter oder sonstigen vertraulichen Daten auf per eMail-Link erreichten Seiten ein.**

  - **Kontrollieren Sie auf jeden Fall das TLS/SSL-Zertifikat**, wie auf Seite 50 beschrieben.

  - **Prüfen Sie, sofern vorhanden und möglich, die digitale Unterschrift.** (Es ist sehr bedauerlich, dass sich diese Technik in eMail bisher nicht durchgesetzt hat, daher wird das leider nur selten gelingen.)

  - **Bedenken Sie, dass Sie der Absender unwissentlich auf eine Phishing-Seite verweisen könnte**, der er selbst soeben auf den Leim gegangen ist.

Es gibt viel zu tun

Geschäfte im Internet lassen sich auch für NichtexpertInnen sicher – also mit vertretbarem Restrisiko – gestalten. Wenn die Betreiber von Telebanking-Seiten, Online-Shops usw. mitarbeiten und ihrerseits eine klare Anti-Phishing-Strategie festlegen, dann könnten die obigen Ratschläge noch um einiges kürzer ausfallen.

Banken und andere Betreiber heikler Services müssen einen Mittelweg zwischen Benutzerfreundlichkeit und Sicherheit finden. So wie das Sicherheitsballett in Flugzeugen Vorschrift ist, sollte auch Online-KundInnen eine Anleitung gegeben werden, die z.B. folgenden Inhalt haben könnte:

Das Team der Firma WirSindToll freut sich, Sie als Kunde in unserem Online-Shop begrüßen zu können. Wir setzen stets die allerneuesten Sicherheits-Technologien ein. Damit diese zum Tragen kommen, beachten Sie bitte vier einfache Tipps:

- Rufen Sie unseren Online-Shop stets nur aus den Bookmarks Ihres Browsers auf, nicht durch Links in eMails oder fremden Webseiten.

- Wenn Sie bei uns einkaufen, achten Sie darauf, dass der URL im Browserfenster immer mit https://shop.wirsindtoll.at/ beginnt.

- Achten Sie darauf, dass das Schloss rechts unten im Browserfenster geschlossen ist.

- Niemals senden wir Ihnen eMail, die einen anzuklickenden Link enthält und zur Aufforderung führt, ein Passwort einzugeben. Wenn Sie eine solche eMail-Nachricht erhalten, löschen Sie diese ganz einfach.

Vergleichen Sie diesen Text mit den Unterlagen Ihres Telebanking-Zugangs. Vermutlich werden Sie enttäuscht feststellen, dass dort nur zu lesen ist, dass wegen toller Verschüsselung alles ganz sicher ist und Sie sich keine Sorgen machen müssen. Diese Banken haben ihre Hausaufgaben leider nicht gemacht – wohl, um die Kunden nicht zu verunsichern. Hier hätte die Chefetage besser ihren TechnikerInnen zugehört, denn ein falsches Gefühl der Sicherheit zu erzeugen, ist natürlich der Kardinalfehler schlechthin.

Phishing ist ein Phänomen mit furchterregendem Entwicklungspotential. Zum einen gilt es daher, durch technische Mittel, Aufklärung und zweckmäßige Sicherheitsgebräuche auf Betreiberseite dagegen vorzugehen.[9] Zum anderen zeigt sich wieder, dass mit Viren, Würmern oder Trojanern infizierte PCs ein unkalkulierbares – aber jedenfalls gewaltiges – Sicherheitsrisiko darstellen und dass Softwarehersteller, Netzbetreiber und AnwenderInnen gemeinsam alle erdenklichen Anstrengungen unternehmen müssen, um die zahllosen verseuchten Rechner aus dem Verkehr zu ziehen.

Alexander Talos ■

9) Auch die Uni Wien ist in dieser Hinsicht noch kein leuchtendes Vorbild, aber wir arbeiten daran. Dass es bei uns noch niemand ernsthaft probiert hat, hat wohl zwei Gründe: Noch ist die Phishing-Branche in Europa nicht so richtig in Fahrt gekommen, und wir sind für Phisher nicht so interessant wie eine Bank.

SSL-Zertifikate: Ein „Reisepass“ für Webseiten

Heute werden mehr und mehr Geschäfte via Internet abgewickelt – vom Reißnagel bis zur Weltreise kann man dort mittlerweile alles kaufen, verkaufen, tauschen oder versteigern. Dabei ist es von essentieller Bedeutung, dass diese Transaktionen sicher durchgeführt werden können. Und nicht nur, wenn es ums Geld geht, ist Sicherheit wichtig: Vertrauliche Daten werden ebenfalls zunehmend im bzw. über das Internet transportiert, und private eMails, Dokumente und Ähnliches sollen natürlich auch vertraulich bleiben und nicht von jedermann abgehört werden können.

Was sind SSL-Zertifikate?

Im WWW hat sich als Standard für sichere Datenverbindungen das Protokoll HTTPS auf Basis von TLS/SSL etabliert (siehe Artikel *WWW + SSL = HTTPS* auf Seite 46 und *Was ist TLS/SSL?* auf Seite 43). Ein wesentlicher Teil dieses Konzepts sind die so genannten SSL-Zertifikate, die nähere Angaben über die Server enthalten, mit denen man Verbindung aufgenommen hat.

Ein Zertifikat soll vor allem sicherstellen, dass der Eigentümer einer Webseite auch wirklich der ist, der er zu sein vorgibt. Jedes Zertifikat ist signiert; wie viel das Zertifikat wert ist, hängt natürlich davon ab, wer es signiert. Im Prinzip ist es auch möglich, ein Zertifikat selbst zu signieren. Ein solches Zertifikat ist als Nachweis der Identität allerdings ungeeignet, deshalb präsentieren Webbrowser und andere Klientenprogramme den BenutzerInnen jedesmal ein Pop-up-Fenster mit einer Warnung, wenn ein solcherart zertifizierter Server aufgerufen wird.

Aus diesem Grund lassen seriöse Anbieter von sicheren Webseiten ihre Zertifikate von „Vertrauenswürdigen Dritten“ erstellen, deren Signatur in den Webbrowsern verankert ist. Derartige CAs (*Certificate Authorities*) gibt es fast wie Sand am Meer, allerdings unterscheiden sie sich zum Teil sehr in der Qualität des Service, der Verifikation des Zertifikatsbestellers und damit der „Vertrauenswürdigkeit“ des Zertifikats. Nicht zuletzt unterscheiden sich die CAs auch beim Preis: Ein Zertifikat kann durchaus mit mehreren hundert Euro zu Buche schlagen.

Auch für eine Universität, die zwar nicht im eCommerce tätig ist, sehr wohl aber eine Unzahl von Services bietet, die ebenfalls mit Verschlüsselung angeboten werden (müssen), kann das schnell sehr teuer und sehr aufwendig werden.

SCS – Der Anfang

Da sich viele Universitäten in dieser misslichen Lage befinden, lag es nahe, sich gemeinsam um günstigere Zertifikate für die Bildungseinrichtungen zu bemühen. Unter der Schirmherschaft von TERENA (dem Dachverband der europäischen Wissenschaftsnetze, `www.terena.nl`) schlossen sich daher im Jahr 2004 acht Wissenschaftsnetze[1)] zusammen, um ein Service für „Pop-Up Free SSL Certificates“ für die europäischen Universitäten aufzubauen – das Projekt **SCS (*Server Certificate Service*)** war geboren.

Die Idee war, eine Certificate Autority zu finden, die imstande ist, mit der großen Zahl an potentiell benötigten Zertifikaten umzugehen und diese auf Basis der Gesamtmenge möglichst kostengünstig anzubieten. Die administrative Tätigkeit des Verifizierens der Anträge sollte dabei jedoch in der Hand der einzelnen Wissenschaftsnetze bleiben. Da das SCS-Projekt für die kommerziellen Zertifizierungsstellen Neuland war, musste für dieses Projekt einiges an Vorarbeiten geleistet werden. TERENA entschloss sich deshalb im Sommer 2005, eine Ausschreibung für dieses Service zu starten. Etliche Firmen haben auch Angebote eingebracht, sodass im Herbst mit allen interessierten Unternehmen konkrete Gespräche geführt werden konnten.

Im Dezember 2005 wurde schließlich die Firma Globalsign (`www.globalsign.com`) als „Bevorzugter Anbieter“ ausgewählt, und am 9. Jänner 2006 konnte der Vertrag zwischen TERENA und Globalsign unterzeichnet werden (siehe `www.terena.nl/activities/tf-emc2/scs.html`). Im Februar und März 2006 galt es dann, die technischen Rahmenbedingungen zu schaffen, um die neuen Zertifikate den einzelnen KundInnen möglichst unkompliziert zur Verfügung stellen zu können.

SCS – Status quo

Auch das österreichische Wissenschaftsnetz ACOnet hat im Laufe des März die nötigen Vorbereitungen getroffen, um das *Server Certificate Service* allen ACOnet-Teilnehmern zugänglich zu machen (Näheres siehe `www.aco.net`). Auf Basis dieses Service ist es nun für die ServerbetreiberInnen an Österreichs Bildungseinrichtungen erstmals möglich, SSL-Zertifikate ohne Lizenzkosten ausstellen zu lassen. Innerhalb der Universität Wien können wir das Service an Institute und Dienststellen weitergeben; dadurch profitieren auch jene Server von diesen Zertifikaten, die von den Instituten selbst betrieben werden.

Mittels SCS lässt sich im Prinzip jedes Service zertifizieren, das TLS/SSL nutzt; allerdings muss der Domain-Name, unter

1) ACOnet (Österreich), CARNet (Kroatien), CESNET (Tschechien), RENATER(CRU) (Frankreich), RedIRIS (Spanien), SURFnet (Niederlande), SWITCH (Schweiz) und UNI-C (Dänemark)

dem der Server läuft, auf die Universität Wien registriert sein. Jeder Serverbetreiber kann die benötigten Zertifikate selbst beantragen. Nach einer Bestätigung des Antrags durch den von der Universität authorisierten Ansprechpartner – den so genannten *Proxy* – wird das Zertifikat von der im ACOnet angesiedelten *Registration Authority* (RA) freigegeben und dann sofort vom Globalsign-System ausgestellt.

Eine genaue Beschreibung der Voraussetzungen und des Anmeldevorgangs finden Sie im Artikel *Der Weg zum SSL-Zertifikat für Uni-Server* auf Seite 44.

Fazit

Nachdem die Frage der Zertifizierungskosten dank SCS keine ausschlaggebende mehr ist, entfällt der wichtigste Grund, SSL nicht zu verwenden. TLS/SSL – bzw. ganz allgemein der Einsatz verschlüsselter Übertragungsprotokolle – ist heute im Interesse der Security schon fast ein Muss, und dieses Service bietet die Gelegenheit, im universitären Bereich eine möglichst flächendeckende Verschlüsselung einzuführen.

Ulrich Kiermayr ■

Was ist TLS/SSL?

Bei TLS (*Transport Layer Security*) oder SSL (*Secure Sockets Layer*) handelt es sich um ein Verschlüsselungsprotokoll zur Datenübertragung im Internet bzw. um eine verschlüsselte Netzverbindung zwischen Server und Client, über die auch unverschlüsselte Anwendungsprotokolle (z.B. HTTP, POP3, IMAP, SMTP, NNTP, SIP, ...) sicher transportiert werden können.

TLS/SSL sorgt also dafür, dass die Daten verschlüsselt über das Netz geschickt werden und somit vor unerwünschten Zugriffen und Manipulationen geschützt sind. Es sichert jedoch nur den Übertragungsweg zwischen Server und Client; auf alles, was davor oder danach mit den Daten geschieht, hat TLS/SSL keinen Einfluss.

Warum zwei Namen?

SSL Version 1.0 wurde 1994 von der Firma Netscape entwickelt. Als SSL 3.0 schließlich 1999 vom Standardisierungs-Gremium IETF (*Internet Engineering Task Force*) im RFC 2246[1)] als *Proposed Standard* festgelegt wurde, benannte man es auf TLS um. Die Unterschiede zwischen SSL 3.0 und TLS sind minimal; umgangssprachlich wird daher meistens weiterhin der Begriff SSL verwendet.

Wie funktioniert SSL?

Bei SSL kommen verschiedene kryptographische Methoden[2)] zum Einsatz:

- **Symmetrische Verschlüsselung**: Hierbei wird für die Ver- und Entschlüsselung der Daten derselbe Schlüssel (*Key*) verwendet.
- **Asymmetrische Verschlüsselung**: Asymmetrische Verfahren benutzen zwei verschiedene Schlüssel zum Ver- und Entschlüsseln – einen öffentlichen (*Public Key*) und einen geheimen (*Private Key*).
- **Hash-Funktion**: Damit wird ein „digitaler Fingerabdruck" mit einer konstanten Länge (128 bis 512 Bit, abhängig vom verwendeten Algorithmus) erstellt, anhand dessen kontrolliert werden kann, ob die übermittelten Daten am Weg zum Empfänger verändert wurden.

Das SSL-Protokoll selbst besteht aus zwei übereinanderliegenden Schichten:

- Auf der unteren Schicht befindet sich das ***SSL Record Protocol***. Dieses prüft, ob die übertragenen Daten vollständig und unverändert ihren jeweiligen Empfänger erreichen und verschlüsselt, sofern dies gewünscht wird, die Daten mit einem symmetrischen Verfahren. Der dabei verwendete Schlüssel wird über das *SSL Handshake Protocol* vereinbart.
- Die obere Schicht enthält unter anderem das ***SSL Handshake Protocol***.[3)] Dieses baut auf dem *SSL Record Protocol* auf und wird einerseits zum Aushandeln der verwendeten kryptographischen Algorithmen und Schlüssel benötigt, andererseits zur Identifikation und Authentifizierung der Kommunikationspartner mit Hilfe asymmetrischer Verschlüsselungsverfahren (in der Regel authentifiziert sich zumindest der Server gegenüber dem Client).

Susanne Kriszta ■

1) siehe `www.ietf.org/rfc/rfc2246.txt` (mittlerweile abgelöst durch RFC 4346, `www.ietf.org/rfc/rfc4346.txt`)

2) Detailliertere Informationen zu den einzelnen Methoden finden Sie z.B. im Artikel *Grundbegriffe der Kryptographie* in *Comment 00/3*, Seite 20 bzw. unter `www.univie.ac.at/comment/00-3/003_20.html`.

3) Neben dem *SSL Handshake Protocol* umfasst die obere Schicht auch noch das *SSL Application Data Protocol*, das *SSL Alert Protocol* und das *SSL Change Cipherspec. Protocol*, die ebenfalls ihr Scherflein zu einer sicheren Datenübertragung beisteuern, hier jedoch nicht näher beschrieben werden.

Der Weg zum SSL-Zertifikat für Uni-Server

Das Zertifizierungs-Service des ZID (Näheres dazu siehe Seite 42) bietet allen Instituten und Dienststellen der Universität Wien die Möglichkeit, ihre diversen Server mit SSL-Zertifikaten auszustatten.

Voraussetzungen

- Die Weitergabe der Zertifikate an Dritte sowie ihre Verwendung für kommerzielle Zwecke (z.B. für Webshops) ist nicht erlaubt.

- Die Zertifikate werden nur für Domains ausgestellt, deren Inhaber die Universität Wien ist. Bei Domains, die auf Universitäts-MitarbeiterInnen bzw. Studierende persönlich registriert sind, kann dieses Service nicht genutzt werden.

- Zertifikate für Domains, die nicht auf `univie.ac.at` enden, sind möglich, benötigen allerdings eine längere Bearbeitungszeit und sind daher rechtzeitig zu beantragen.

Das Service ist für die EndbenutzerInnen kostenlos, erfordert jedoch am Zentralen Informatikdienst einen gewissen administrativen Aufwand. Wir sind zwar bemüht, die Zertifikate so schnell wie möglich (d.h. in der Regel innerhalb weniger Tage) auszustellen, bitten aber um Verständnis dafür, dass wir keine Antwortzeiten garantieren können.

Schritt für Schritt zum Zertifikat

Zunächst muss der Administrator des Servers – der *Technical Contact* – einen *Private Key* und einen *Certificate Signing Request* (CSR) generieren. Das dazu benötigte Programm (z.B. openssl bei Apache-Webservern) ist in der Serversoftware enthalten. Nähere Informationen zu diesem Schritt finden Sie in Ihrer Serverdokumentation und auf der Webseite `https://www.univie.ac.at/ZID/ssl-antrag/` unter dem Link *Help with creating your CSR*.

Die Webseite **`https://www.univie.ac.at/ZID/ssl-antrag/`** müssen Sie auch aufrufen, um das Zertifikat zu beantragen:

Step 1:

Wählen Sie unter dem Punkt *Options* die gewünschte Laufzeit (maximal 3 Jahre) und den Typ des Zertifikats (das Standardprodukt ist *SureServerEDU TLS*) sowie Ihren Webserver-Typ. Anschließend kopieren Sie den zuvor generierten CSR in das Eingabefeld darunter und klicken auf *Go to step 2* (siehe Abb. 1).

Abb. 1: SCS-Zertifikat beantragen – Step 1

Step 2:

Hier sind die Daten des Antragstellers auszufüllen (siehe Abb. 2 auf Seite 45). Der *Technical Contact* ist der Administrator des jeweiligen Servers. Unter dem Punkt *Email* ist auch die Angabe einer Gruppen-Mailadresse möglich und sinnvoll – an diese Adresse werden nämlich das Zertifikat und die Warnungen über den Ablauf geschickt.

Die Funktion der *Admin Contact Person* (auch *Proxy* genannt) hat für die Universität Wien ein Mitarbeiter des Zentralen Informatikdienstes inne. Es ist Bestandteil der Vertragsvereinbarungen mit der Firma GlobalSign, dass der Request ausschließlich von der Person bearbeitet werden darf, die an dieser Stelle im Formular genannt wird. Der Name und die Kontaktdaten des jeweils aktuellen „Proxy vom Dienst" sind im rechten Bereich des Webformulars eingeblendet (siehe Abb. 2); bitte übertragen Sie dort angegebenen Daten in Ihren Antrag.

Step 3:

Abschließend erhalten Sie nochmals eine Zusammenfassung Ihrer Angaben (siehe Abb. 3 auf Seite 45). Sofern alles korrekt ausgefüllt ist, klicken Sie

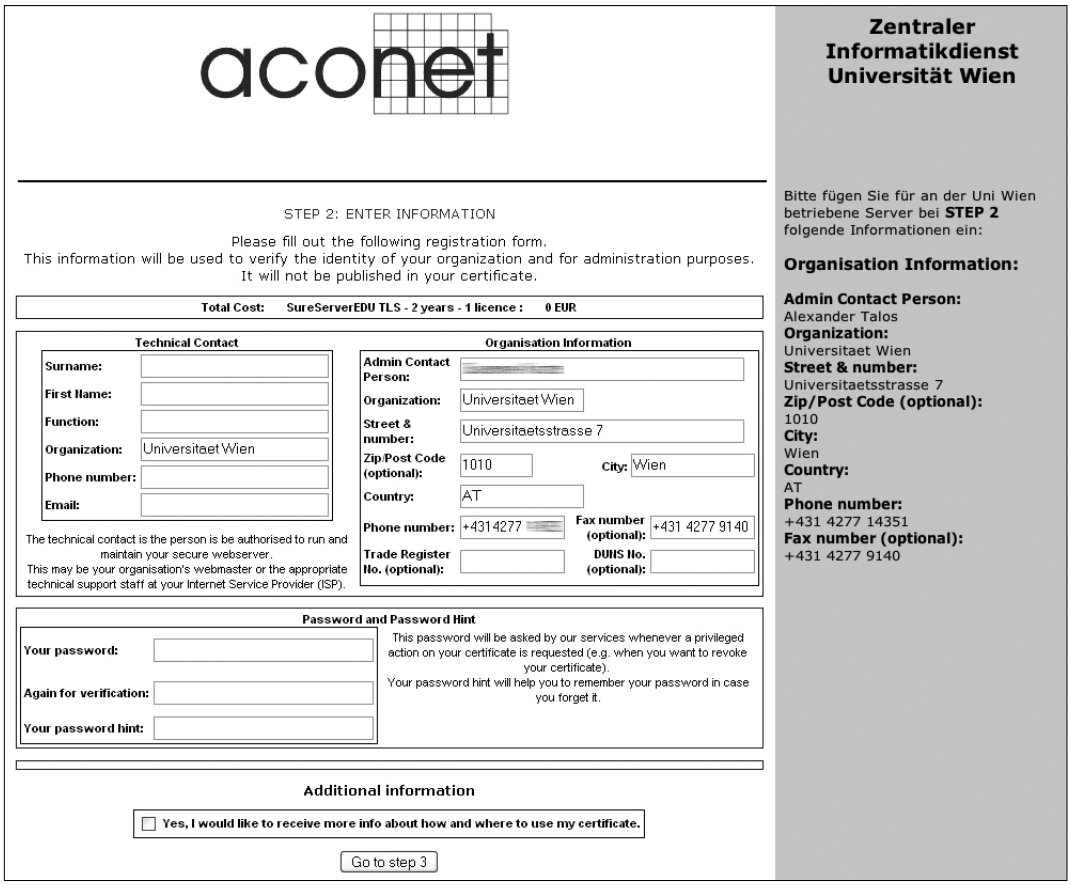


Abb. 2: SCS-Zertifikat beantragen – Step 2

Abb. 3: SCS-Zertifikat beantragen – Step 3

auf *Request this certificate!*, um Ihren Antrag abzuschicken.

Was passiert dann?

Der *Proxy* kontaktiert nun den *Technical Contact* per eMail, um zu überprüfen, ob dieser auch tatsächlich das jeweilige Zertifikat beantragt hat. Innerhalb von 14 Tagen muss eine Bestätigung via Mail erfolgen, sonst wird der Request automatisch aus dem System gelöscht (bei Unklarheiten benötigen wir zusätzlich eine Bestätigung des Institutsvorstands). Sofern keine Komplikationen auftreten, erhält der *Technical Contact* wenige Tage nach Eintreffen der Bestätigung eine eMail-Nachricht mit dem signierten Zertifikat, einem Link für dessen zukünftigen Download sowie einem Link, unter dem es widerrufen werden kann (siehe unten).

Das Zertifikat erlischt automatisch nach Ablauf der gewünschten Zeitspanne. Eine Verlängerung ist nicht möglich, sondern das Zertifikat muss – wie oben beschrieben – neu beantragt werden. Wenn der *Private Key* kompromittiert wurde (z.B. durch Einbruch in den Server), muss das Zertifikat vom *Technical Contact* unter dem per Mail übermittelten Link widerrufen werden. Dazu ist das bei der Anmeldung gewählte Passwort erforderlich. Sollte der *Technical Contact* dieses vergessen haben, kann er den Widerruf – nach Vorlage eines Lichtbildausweises – auch durch den Proxy durchführen lassen (dessen aktuelle Kontaktdaten sind unter dem URL `https://www.univie.ac.at/ZID/ssl-antrag/` zu finden).

Weitere Infos

GlobalSign bietet ein Support-Portal mit jeder Menge Dokumentation zum Thema Zertifikate an, das unter **`http://support.globalsign.net/`** zu finden ist. Bitte wenden Sie sich mit Fragen, Anregungen bzw. mit Meldungen über Probleme mit dem System nicht an GlobalSign, sondern per Mail an **`security.zid@univie.ac.at`**.

Susanne Kriszta ■

WWW + SSL = HTTPS

Der steinige Weg zum sicheren Surfen

Bei all dem Tamtam, das in dieser Ausgabe des *Comment* um TLS bzw. SSL gemacht wird[1], drängt sich eine Frage auf: *Was, ganz konkret, habe ich davon?* – Verständlich, denn bei TLS/SSL ist es durchaus eine Tugend, gleich einem Butler völlig unbemerkt zu dienen. Das vergleichsweise auffälligste Anwendungsgebiet soll hier näher beschrieben werden: der Aufruf von Webseiten mit dem Protokoll HTTPS.

Was ist HTTPS?

TLS/SSL (*Transport Layer Security / Secure Sockets Layer*) fungiert als „digitale Eskorte" für die beim Websurfen übertragenen Bits und Bytes. Es wird als Sicherheitsschicht zwischen dem für den Webseiten-Transport zuständigen HTTP (*Hypertext Transport Protocol*) und dem Transportprotokoll TCP (*Transmission Control Protocol*) eingefügt.

HTTP (WWW-Inhalt)
TCP (Transport)
IP (Internet-Fundament)

normales Websurfen

HTTP (WWW-Inhalt)
SSL (Crypto)
TCP (Transport)
IP (Internet-Fundament)

mit TLS/SSL gesichertes Surfen

Da sozusagen das **HTTP** mit **S**ecurity angereichert wird, nennt man das Duo dann **HTTPS** (*Secure HTTP*). Das können Sie bereits am URL in Ihrem Browser erkennen, z.B. wenn Sie das Webmail-Service der Universität Wien aufrufen (`http`**`s:`**`//webmail.univie.ac.at/`).

Was das für die Sicherheit bedeutet, sieht man am besten an den konkreten Bedrohungen, die damit abgewehrt werden – oder eben nicht. Dabei werden gewöhnlich drei Kategorien betrachtet:

- **Vertraulichkeit**,
- **Integrität** (die Daten müssen unverändert sein und von der richtigen Quelle stammen) und
- **Verfügbarkeit** (Daten, die man nicht bekommt, nützen einem nichts).

Durch Verschlüsselung kann die Vertraulichkeit geschützt werden, aber das setzt, wie dieser Artikel zeigen wird, die ohnehin geforderte Sicherung der Integrität voraus. In diesem Bereich hat TLS/SSL einiges zu bieten. Zur Verfügbarkeit, das sei gleich vorweggenommen, kann TLS/SSL nichts beitragen. Eher im Gegenteil: Das System wird durch seinen Einsatz komplexer und damit etwas verwundbarer.

Lauschen – geht das denn?

Die Verbindung zwischen Browser und Webserver ist nichts anderes als eine Folge von Datenpaketen, jedes mit einer Zieladresse – je nach Richtung ist das die des Servers oder die des Browsers – beschriftet, die von den einzelnen Internet-Knoten etappenweise näher zum Ziel transportiert werden, bis sie dort angekommen sind. Damit sie belauscht oder manipuliert werden können, müssen diese Datenpakete beim Langohr vorbeikommen.

Betrachten wir zunächst einen einfachen Rechner (in dieser Hinsicht sind der Webserver und der PC weitestgehend gleich). Dieser „sieht" natürlich sämtliche Pakete von Verbindungen, an denen er selbst teilnimmt.

- Lokale Netze (LANs, z.B. Institutsnetze oder das lokale Netz daheim) werden heutzutage durch so genannte Switches verbunden, die aus Effizienzgründen Daten stets nur zum bestimmungsgemäßen Empfänger-PC oder dem Router, dem Tor zur Außenwelt, weitersenden. Damit sind jedoch keinerlei Sicherheitsgarantien verbunden, und es sind verschiedene Methoden bekannt, einen Switch dazu zu überreden, seine Datenpakete anderswohin umzuleiten.[2] In einem lokalen Netz kann mit etwas Glück auch ein Rechner einen anderen dazu verleiten, ihm seine Pakete zu schicken.[3] Wer einen Rechner belauschen möchte, der nicht im selben LAN angeschlossen ist, kann sich z.B. durch Verwendung verwaister Netzwerksteckdosen, Anzapfen von Leitungen etc. Zugang dazu verschaffen.

- Aus der Ferne kann ein Angreifer sozusagen einen Agenten in das abzuhörende lokale Netzwerk entsen-

---

1) siehe *SSL-Zertifikate: Ein „Reisepass" für Webseiten* (Seite 42), *Was ist TLS/SSL?* (Seite 43), *Der Weg zum SSL-Zertifikat für Uni-Server* (Seite 44) und *Das Postamt zieht um: Ein neues Mailsystem für die Uni Wien* (Seite 11)

2) *CAM Table Flooding*, Näheres siehe `www.packetwatch.net/documents/papers/layer2sniffing.pdf`

3) *ARP Cache Poisoning*, siehe ebenfalls `www.packetwatch.net/documents/papers/layer2sniffing.pdf`

4) z.B. *DNS Cache Poisoning* (erklärt im Wikipedia-Artikel `http://de.wikipedia.org/wiki/DNS-Spoofing`), gefälschte Einträge in der `hosts`-Datei (siehe `www.heise.de/security/news/meldung/52935`)

5) siehe EU-Richtlinie 2006/24/EG: *Vorratsspeicherung von Daten* (`www.bmvit.gv.at/telekommunikation/recht/europa/richtlinien/rl2006-24.html`)

6) Nähere Informationen dazu finden Sie z.B. im Artikel *Grundbegriffe der Kryptographie* in *Comment 00/3*, Seite 20 bzw. unter `www.univie.ac.at/comment/00-3/003_20.html`.

7) Die mit einer bestimmten Schlüssellänge erzielte Sicherheit kann von Verfahren zu Verfahren variieren: 3DES mit 160 Bit gilt als weniger sicher als AES mit 128 Bit.

den: Entweder er infiltriert damit einen Rechner, der sich in diesem Netz befindet – dafür steht eine reiche Auswahl von Viren, Trojanern und fertigen Scripts zur Verfügung – oder er zielt unmittelbar auf den abzuhörenden Rechner. Wenn lediglich Zugriff auf dessen Konversation mit einem bestimmten anderen Rechner erlangt werden soll, gibt es auch die Möglichkeit, die Namensauflösung zu manipulieren.[4] Gelingt dies, dann sendet das Opfer seine Daten unwissentlich direkt zum Lauscher.

Wer zentrale Knoten des Internet betreibt, verfügt über Geräte, die viele (wenn auch nicht alle) Daten verarbeiten, die international oder weitläufig national transportiert werden. Während die Internet Service Provider selbst keinerlei Interesse an diesen Daten haben, sind die Begehrlichkeiten mehr oder weniger rechtsstaatlicher Instanzen im Zunehmen.[5]

Im Internet ist es also für Unbefugte zwar unterschiedlich schwierig, aber keinesfalls unmöglich, auf fremden Datenverkehr zuzugreifen.

Schutz der Vertraulichkeit

Die Vorstellung, dass beim Online-Shoppen mehr oder weniger jeder die Kreditkartennummer und das Gültigkeitsdatum mithören und dann damit einkaufen gehen kann, lässt einem kalte Schauer über den Rücken laufen. Der folgerichtige Schluss ist der Ruf nach Verschlüsselung, getreu dem Motto: *Gefahr erkannt, Gefahr gebannt.*

Das Verschlüsseln von Daten hat jedoch mit zahlreichen Problemen zu kämpfen. Eines der prominentesten davon ist folgendes: Wie vereinbaren die Gesprächspartner den Schlüssel?

Daran haben sich die Kryptologen jahrtausendelang die Zähne ausgebissen, bis Computer jene komplizierten mathematischen Verfahren alltagstauglich gemacht haben, auf denen die *Public Key*-Kryptosysteme (auch asymmetrische Verschlüsselung genannt) beruhen.[6] Der Gag daran ist, dass ein Schlüssel hier aus zwei Teilen besteht, einem öffentlichen und einem privaten Schlüssel, und was der eine Teil verschlüsselt hat, kann nur der andere entschlüsseln.

Bei HTTPS geben beide Gesprächspartner zu Beginn der Verbindung ihren öffentlichen Schlüssel bekannt. Der jeweils andere kann damit Nachrichten verschlüsseln, die nur der berechtigte Empfänger entschlüsseln kann, weil er allein den zweiten Teil, den privaten Schlüssel, besitzt. Das Verfahren ist genial: Es ermöglicht abhörsichere Kommunikation, ohne dass im Vorhinein ein gemeinsames Geheimnis mühsam vereinbart werden müsste.

Einen Schönheitsfehler hat die Sache: Diese asymmetrischen Verfahren sind viel zu rechenaufwendig, um im großen Stil (etwa auf einem Webserver zur Verschlüsselung der gesamten Kommunikation) eingesetzt zu werden. Daher wird – mit dieser Methode geschützt – zu Beginn der Verbindung ein so genannter *Session Key* ausgehandelt, ein Schlüssel für symmetrische Verschlüsselung, der (bzw. die) anschließend für die Dauer der Verbindung verwendet wird. Da symmetrische Verschlüsselung deutlich schneller und ebenfalls sehr sicher ist, sofern der Schlüssel geheim vereinbart wurde, hat man dadurch das Beste aus allen Welten unter einen Hut gebracht.

Verschlüsselung ist gut, man muss aber auch darauf achten, dass der Schlüssel zufällig gewählt und nicht vorhersagbar ist (das stellt TLS/SSL sicher), dass er ausreichend lang ist, um nicht durch Ausprobieren geknackt zu werden, und dass das gewählte Verfahren ausreichend sicher ist. Bei den zur Zeit üblicherweise eingesetzten Systemen kann man sich an die Faustregel[7] halten: Wenn die Schlüssellänge mindestens 128 Bit beträgt, ist alles gut. Das überprüft man mit Hilfe des geschlossenen Schloss-Symbols rechts unten im Browserfenster, das bei jeder verschlüsselten Seite angezeigt wird: Nach einem Doppelklick auf dieses Schloss erscheint das Fenster *Seiteninformation*, und auf der Registerkarte *Sicherheit* ist der verwendete Algorithmus angeführt (siehe Abb. 1).

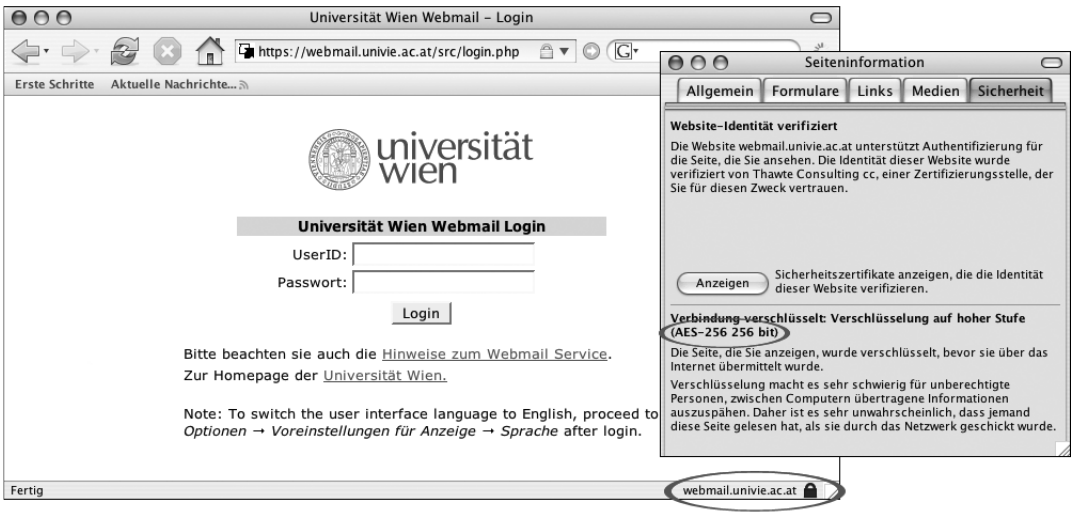


Abb. 1: Durch Doppelklick auf das Schloss-Symbol rechts unten im Browserfenster erscheint die Registerkarte *Sicherheit* der *Seiteninformation*, auf der der verwendete Schlüssel angezeigt wird.

An dieser Stelle ist ein Hinweis angebracht: Alle „Klickanweisungen“ und Abbildungen in diesem Artikel beziehen sich, sofern nicht anders angegeben, auf den Open Source-Browser Firefox, dessen deutsche Version unter dem URL `www.mozilla-europe.org/de/products/firefox/` kostenlos erhältlich ist. Es handelt sich dabei um eine „abgespeckte“, auf die Browser-Funktionalitäten reduzierte Version der Mozilla Application Suite, die mittlerweile in vollem Umfang – d.h. inklusive Browser, Mail- und Chatprogramm, Newsreader, HTML-Editor – unter dem Namen SeaMonkey weiterentwickelt wird und von der Webseite `http://mozilla.kairo.at/` bezogen werden kann. SeaMonkey ist also sozusagen ein viergängiges Menü, Firefox die Hauptspeise daraus – mit etwas weniger Beilagen (sprich Einstellungsoptionen), aber für den durchschnittlichen Hunger durchaus ausreichend.

SeaMonkey-AnwenderInnen haben z.B. die Möglichkeit (das ist eine der Beilagen), alle „schwachen“ Schlüssel in der Browserkonfiguration zu verbieten: Unter *Preferences – Privacy & Security – SSL* findet sich dort die Schaltfläche *Edit Ciphers*. Dahinter kann (und sollte) man für *SSL2*, *SSL3/TLS* und *Extra SSL3/TLS* jeweils alle Schlüssel deaktivieren, die weniger als 128 Bit verwenden (siehe Abb. 2). In Firefox geht das leider nicht, oder zumindest nicht so einfach.

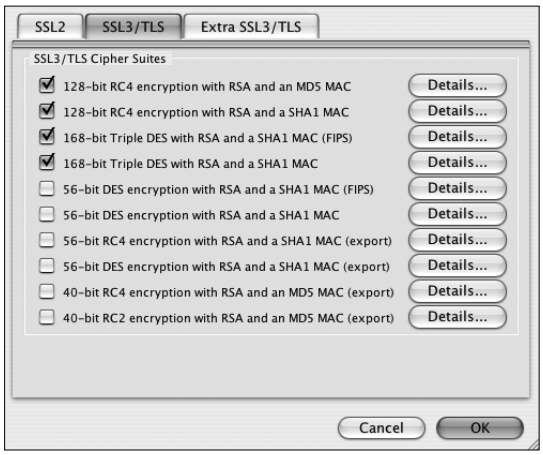


Abb. 2: Auswählen von „starken“ Schlüsseln in SeaMonkey *(Preferences – Privacy & Security – SSL – Edit Ciphers)*

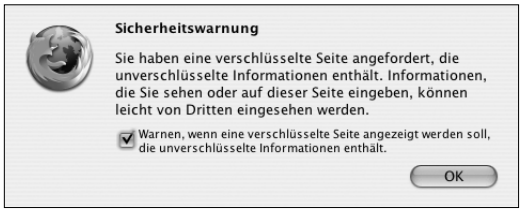


Abb. 3: Warnmeldung bei Seiten, die sowohl verschlüsselte als auch unverschlüsselte Informationen enthalten

Also wenn wir mit ganz vielen Bits verschlüsseln, dann ist alles sicher?

Leider nein, aber danke fürs Mitspielen – um es mit den Worten von Mr. Keating im *Club der toten Dichter* zu sagen. Ebensowenig wie sich der Wert eines Gedichts einfach durch Berechnung von Perfektion in der X-Achse und Ausdruck in der Y-Achse bewerten lässt, kann man Sicherheit allein an der Schlüssellänge ermessen. Es gibt noch viel mehr zu bedenken.

Eine Gefahr, die trotz Verschlüsselung noch nicht gebannt ist, besteht darin, dass eine Webseite in der Regel aus mehreren Teilen besteht (z.B. Bilder, Frames, Stylesheets, Flash-Animationen, Hintergrundmusik), die separat transportiert werden. Was nützt es, wenn ein Teil davon gesichert übertragen wird, aber vielleicht genau dort, wo es ums Eingemachte geht, die Verschlüsselung leider nicht angewendet wird? Klar, dann hat der Seitenverantwortliche einen Fehler gemacht, und bei einer professionell gestalteten Site sollte das nicht passieren – aber das hilft uns nicht weiter. Immerhin zeigen Webbrowser eine Warnung an (siehe Abb. 3), wenn HTTPS und unverschlüsseltes HTTP gemischt werden. Die Browserhersteller neigen hier jedoch zum Unterden-Teppich-Kehren: Browser jüngeren Datums warnen nicht, wenn Stylesheets und Bilder unverschlüsselt übertragen werden, wohl aber bei Hintergrundmusik und Frames.

Das Kontrollkästchen unterhalb dieser und ähnlicher Warnungen hat leider einen fatalen Designfehler: Es muss beim ersten Auftauchen angeklickt werden, damit die Warnung bei gegebenem Anlass auch in Zukunft erscheint. Bitte achten Sie also darauf, dieses Kästchen zu aktivieren, sobald Sie es zu Gesicht bekommen! Auch hier haben SeaMonkey-AnwenderInnen einen Vorteil: Sie können diese Warnungen nachträglich unter *Preferences – Privacy & Security – SSL* aktivieren (siehe Abb. 4).

Gerade die Warnung bei Webseiten mit „Protokollmixtur“ bringt die AnwenderInnen in eine unangenehme Situation: Zwar ist offenbar irgendetwas nicht koscher, aber es erfordert ein fundiertes Verständnis von HTML, um beurteilen zu können, ob ein ernsthaftes Problem vorliegt. Wir können nur empfehlen, in solchen Fällen vorsichtig zu sein und keine sensiblen Daten zu übertragen, ohne vorher jemanden um Rat zu fragen – etwa den Seitenbetreiber selbst, der sich des Problems möglicherweise gar nicht bewusst ist. Die Warnung einfach zu ignorieren, ist eher keine gute Idee.

Was auf diese Weise leider nicht festgestellt werden kann, ist, ob Teile der Seite von einem anderen Server stammen. Das kann absolut erwünscht sein – etwa bei großen Sites, die statische Bilder auf anderen Servern ablegen als die Seiten-Bestandteile, die von Datenbanken generiert werden. Es kann aber auch sein, dass fremde Inhalte ihren Weg auf die Seite gefunden haben, was gar nicht geplant war. Der Browser hat leider keine Chance, das zu beurteilen, und kann also auch nicht davor warnen. Wovor Ihr Browser jedoch warnt: Wenn ein gesicherter Bereich verlassen wird (siehe Abb. 5). Besonders kritisch ist das dann, wenn Sie beispielsweise auf einer sicheren Seite ein Formular finden, dort Ihre Kreditkartendaten eingeben, diese aber beim Klick auf *Absenden* oder *Bestellen* unverschlüsselt übertragen werden (siehe Abb. 6).

Abb. 4: Aktivieren von Warnmeldungen in SeaMonkey *(Preferences – Privacy & Security – SSL)*

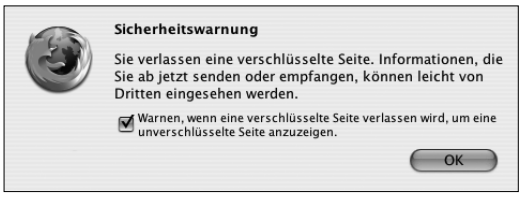


Abb. 5: Warnmeldung bei Verlassen einer verschlüsselten Seite

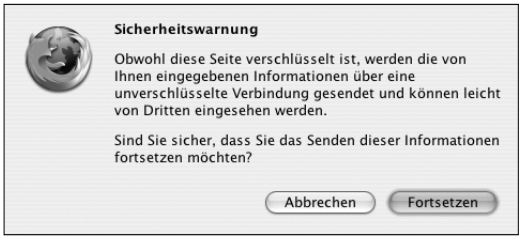


Abb. 6: Warnmeldung bei Versenden von Formulardaten über eine unverschlüsselte Verbindung

Schutz der Integrität

In der chinesischen Schrift gibt es verschiedene Sätze von Zahlzeichen: einfache Zeichen für den alltäglichen Gebrauch und eine Langform aus komplizierteren Graphemen, die wegen ihrer Fälschungssicherheit bei Verträgen verwendet werden (siehe dazu `http://de.wikipedia.org/wiki/Chinesische_Zahlen`). Ein Webbrowser kommuniziert mit dem Webserver nicht mittels Pinsel und Tusche, sondern mittels elektronischer Signale, die völlig ohne Farbkleckse oder Kratzspuren zu fälschen sind. Dennoch kann und muss die weise Voraussicht der ehrwürdigen Chinesen ins Zeitalter des Internet übertragen werden.

Plumpe Fälschung

Ein gängiger Irrglaube ist, dass durch die Verschlüsselung auch die Manipulation verhindert wird. Zwar wird die freie Gestaltung beim Fälschen durch die Verschlüsselung deutlich erschwert, aber je nach den konkreten Umständen gibt es doch die Möglichkeit, etwas Sinnvolles einzufügen. Es mag einem Saboteur aber auch genügen, die Nachricht einfach nur zu verstümmeln.

Technisch kann zwar die Manipulation nicht verhindert werden, aber es ist möglich, sie zu erkennen. Dazu werden die übertragenen Datenpakete ganz einfach digital unterschrieben. Das funktioniert so: Der Absender bildet eine kryptographische Prüfsumme aus der Nachricht und dem Session Key und sendet das Ergebnis mit, das vom Empfänger nachgerechnet wird. Da außer Sender und Empfänger niemand den Session Key kennt, kann niemand die zur einer gefälschten Nachricht passende Prüfsumme berechnen. Wenn Prüfsumme und Nachricht nicht übereinstimmen, wird die Verbindung sofort beendet.

Bis repetita non placent[8)]

Trotz all dieser Sicherungen sind die Cyberbetrüger noch nicht mit ihrem Latein am Ende. Mit so genannten *Replay Attacks* kann man, indem man die gesamte Verbindung oder einen Teil davon wie mit einem Kassettenrekorder aufnimmt und später wieder abspielt, zumindest jede Menge Schaden anrichten. Aber auch eine tausendfach wiederholte Überweisung ist denkbar, oder dass irgendjemand nur den Loginvorgang aus der Konserve abspielt und die Account-Daten dann für seine Zwecke missbraucht. Bei menschlicher Konversation würden solche Wiederholungen schnell auffallen; ein Computer führt jedoch bereitwillig *ad nauseam*[9)] denselben Dialog immer wieder, ohne sich zu wundern.

Das Protokoll HTTPS wehrt sich gegen Replay-Attacken, indem jeder Nachrichtenblock innerhalb einer Verbindung eine fortlaufende Nummer erhält. Da sowohl der Session Key als auch die Blocknummern in die Berechnung der integritätsschützenden Prüfsumme einbezogen werden, wird jeder Versuch des Daten-Recyclings sofort erkannt und führt zur Beendigung der Verbindung.

Da aß der Wolf etwas Kreide und machte seine Stimme ganz fein...

Zum Schutz der Integrität gehört es auch, die Authentizität einer Nachricht oder eines Kommunikationspartners sicherzustellen. Wenn der Wolf Teig auf seine Pfoten streichen lässt und Kreide frisst, will er damit eines erreichen: Dass die Geißlein ihn für ihre Mutter halten und ihm vertrauen.

Ein Internet-Wolf würde damit anfangen, z.B. die Telebanking-Startseite auf seinem eigenen Server nachzubauen. Mittels Kopieren und Einfügen ist das eine weitgehend tri-

8) *„Wiederholungen gefallen nicht“* – Julius Cäsar zu Tullius Firlefanzus, als er einen erneuten Angriff auf Gergovia ablehnt (*Asterix XI/46*; `www.comedix.de/lexikon/db/bisrepet.htm`)

9) *„bis zur Übelkeit“*

viale Angelegenheit. Eine andere Methode, die noch subtilere Manipulationen ermöglicht, besteht darin, ähnlich dem bekannten *Stille-Post*-Spiel alle Anfragen an den zu imitierenden Server weiter- und dessen Antworten zurückzureichen. Auf seinem Klon-Server hat der Bösewicht dabei die volle Kontrolle über das Geschehen: Er kann Daten (z.B. Passwörter) mitschneiden, Kontonummern austauschen – der Phantasie sind da keine Grenzen gesetzt.

Um einen Browser zu diesem falschen Server zu locken, kann man sich der eingangs beschriebenen Umleitungsverfahren bedienen. Wie wirkt nun der TLS/SSL-Schutz, soweit er bisher beschrieben wurde, angesichts dieser Fälschung?

Verschlüsselung und Integritätsschutz beruhen auf asymmetrischen Schlüsseln, die Server und Client jeweils selbst bekanntgeben. Das kann der gefälschte Server genauso gut wie das Original. Die Tarnung ist also fast perfekt – eine verschlüsselte Verbindung wird aufgebaut und transportiert die Geheimnisse des Users abhör- und manipulationssicher direkt in die Arme des Abhörers bzw. Fälschers.

Jede Hoffnung auf Sicherheit wäre damit endgültig dahin, hätten nicht findige Kryptologen auch für dieses Problem eine (allerdings relativ aufwendige) Lösung gefunden. Diese besteht darin, dass der Webserver erst seine Identität nachweisen muss.[10] Hätten die Geißlein Ausweise mit Fingerabdrücken gekannt, wären sie nicht gefressen worden; man braucht also einen solchen Mechanismus auch für HTTPS.

Das Zertifikat – der „Reisepass" für Webserver

Der elektronische Ausweis für den Server, das so genannte TLS/SSL-Zertifikat, ist eine normierte Datenstruktur, die unter anderem folgende Angaben enthält: Rechnername, Organisation, Gültigkeitszeitraum, öffentlicher Schlüssel des Rechners, Bezeichnung der Stelle, die das Zertifikat ausgestellt hat (*Certificate Authority*, kurz CA), sowie deren Signatur. Zur Kontrolle eines Zertifikats entschlüsselt der Browser die Unterschrift der Zertifizierungsstelle mit deren öffentlichem Schlüssel, berechnet selbst die Prüfsumme aus den Angaben im Zertifikat und vergleicht die Ergebnisse. Stimmen sie überein, kann man sich auf die Identität des Servers verlassen – vorausgesetzt, man vertraut dem Zertifikatsaussteller.

Sie können den genauen Zertifikatsinhalt abrufen, indem Sie – wie bei Abb. 1 beschrieben – einen Doppelklick auf das Schloss-Symbol rechts unten im Browserfenster machen und anschließend auf der Registerkarte *Sicherheit* auf die Schaltfläche *Anzeigen* klicken (siehe Abb. 7).

Abb. 7: Anzeigen des Zertifikats einer HTTPS-geschützten Webseite (Aufruf mittels Doppelklick auf das Schloss-Symbol und anschließendem Klick auf die Schaltfläche *Anzeigen* auf der Registerkarte *Sicherheit* der *Seiteninformation*)

Ein Henne-und-Ei-Problem bleibt aber noch zu lösen: Wie kommt Ihr Browser zum öffentlichen Schlüssel der Zertifizierungsinstanz? Es gibt zweieinhalb Möglichkeiten:

- Große Zertifizierungsfirmen wie Thawte oder Globalsign haben Verträge mit Browser- bzw. Betriebssystem-Herstellern abgeschlossen, damit diese deren Zertifikate fix in ihre Software einbauen. Die Voraussetzungen für die Ausstellung eines Zertifikats sind ausgesprochen streng, und es ist zu hoffen, dass die Softwarehersteller deren Einhaltung auch kontrollieren, da Fehler zu nennenswerten Schadenersatzforderungen führen können. Ihren Zertifizierungsdienst lassen sich solche Firmen auch gut bezahlen: Es ist mit Kosten von € 250,– pro Jahr und Rechnername zu rechnen. Daher wurde das auf Seite 42 vorgestellte Projekt SCS (*Server Certificate Service*) ins Leben gerufen, durch das im Universitätsbereich Zertifikate ohne weitere Kosten für den Endverbraucher bezogen werden können.

- Sie importieren das Zertifikat selbst, weil Sie dem Aussteller trauen. Dieser Schritt sollte aber wohl überlegt werden und wird hier nicht weiter beschrieben.

- Die zweieinhalbte Variante ist ein mehrstufiges Verfahren: Das Server-Zertifikat ist mit einem Schlüssel unterschrieben, welcher durch ein zweites Zertifikat bestätigt wird, das seinerseits von einem dem Browser bekannten Zertifikat unterschrieben wurde. Diese Variante ist insofern erwähnenswert, als beim SCS-Projekt genau so verfahren wird.

Um nachzuverfolgen, woraus sich die Identität einer gerade angezeigten Seite ergibt, klicken Sie – wie bei Abb. 1 und Abb. 7 beschrieben – auf das Schloss-Symbol im Browser-

10) Bei TLS/SSL handelt es sich hierbei um ein konfigurierbares Feature, ebenso optional wie die Ausweispflicht für den Client. Bei HTTPS ist das Serverzertifikat allerdings Pflicht.

11) Um der Wahrheit die Ehre zu geben, müssen wir einräumen, dass immer ein Restrisiko bleibt – das aber so gering ist, dass es in deutscher Sprache nicht mehr formulierbar ist.

fenster und anschließend auf der Registerkarte *Sicherheit* der *Seiteninformation* auf die Schaltfläche *Anzeigen*. Diesmal müssen Sie zusätzlich die Registerkarte *Details* auswählen. Abb. 8 zeigt den hierarchischen Aufbau dieser Registerkarte: Wenn Sie im ersten Bereich (*Zertifikatshierarchie*) einen Punkt anklicken, erscheinen die dazu verfügbaren Informationen im Bereich *Zertifikats-Layout* darunter. Wählen Sie hier einen Eintrag aus, so werden die Details dazu im Bereich *Feld-Wert* angezeigt.

Wenn Sie mit HTTPS auf eine Seite gelangen, deren Identität nicht durch eine lückenlose Kette zu einem dieser Zertifikate führt, zeigt der Browser eine Warnung an (siehe Abb. 9).

Das vom Server präsentierte Zertifikat können Sie mit Hilfe dieses Dialogfensters auch wider besseres Wissen akzeptieren. Das sollten Sie jedoch nur unter gewissen Randbedingungen machen, nämlich wenn

- der dargestellte Fingerprint mit dem des gewünschten Servers (den Sie natürlich über einen sicheren – also zumindest anderen – Weg erhalten haben als den, der Sie auf diese Seite geführt hat) verglichen wurde oder

- Sie auf dieser Seite keine sensiblen Daten, insbesondere keine Passwörter, eingeben (wozu dann aber die Verschlüsselung?). Sofern Ihr Browser die Möglichkeit bietet, sollten Sie den Schlüssel nur für diese Sitzung annehmen.

Welche Zertifizierungsinstanzen und welche individuellen Serverzertifikate Ihr Browser akzeptiert, sehen Sie in Firefox unter *Einstellungen – Erweitert – Sicherheit – Zertifikate anzeigen*. Die Zertifikate so genannter „Vertrauenswürdiger Dritter" sind auf der Registerkarte *Zertifizierungsstellen* aufgelistet und werden durch einen Klick auf *Ansicht* angezeigt (siehe Abb. 10 auf Seite 52).

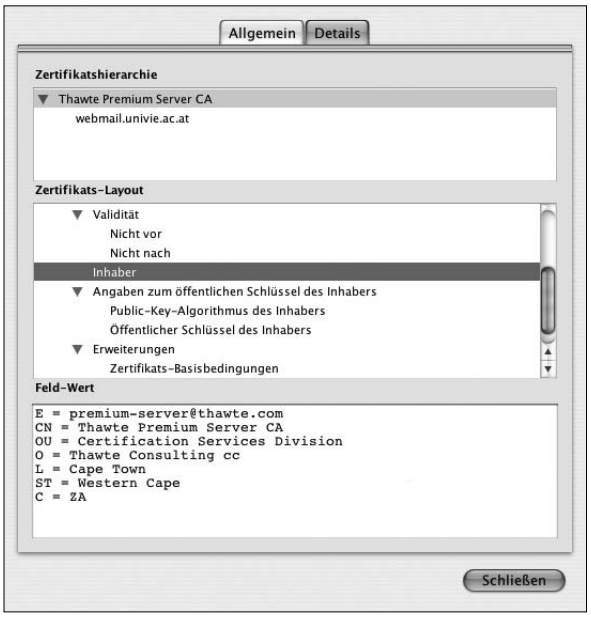


Abb. 8: Anzeigen der Zertifikat-Details einer HTTPS-geschützten Webseite (Aufruf mittels Doppelklick auf das Schloss-Symbol und anschließendem Klick auf die Schaltfläche *Anzeigen* auf der Registerkarte *Sicherheit* der *Seiteninformation*)

Ein ähnlicher Fall wie bei lückenhaften Zertifizierungsketten liegt vor, wenn das Zertifikat abgelaufen ist. Das sollte durch den Seitenbetreiber zügig behoben werden; geschieht dies nicht, wirkt der Server ohnehin nicht vertrauenswürdig. Gänzlich die Finger lassen sollten Sie von einem Server, der anders heißt als sein Zertifikat angibt (siehe Abb. 11): Wenn ein Server sich als jemand ausgibt, der er nicht ist, ist ganz sicher etwas faul. Eine solche Situation ist durchaus einen Anruf bei der Hotline des Betreibers wert, dem sein Problem vielleicht gar nicht bewusst ist. Zwar ist es durchaus üblich, dass ein Server berechtigterweise mehrere Namen hat (beispielsweise bei virtuellen Servern), aber auch diese Situation müssen AdministratorInnen von Services, die den Schutz von TLS/SSL benötigen, zu meistern in der Lage sein.

Mit all diesen Vorkehrungen aber ist HTTPS endlich wirklich sicher.[11)] Der Datenverkehr kann weder belauscht noch manipuliert werden, und es ist sichergestellt, dass sich kein falscher Server einschmuggelt.

Grenzen von TLS/SSL

Es klingt zu gut, um wahr zu sein: TLS/SSL hat sich in über einem Jahrzehnt in höchstem Maße bewährt. Schwächen in manchen Details wurden ausgebessert, haben aber nicht zu spektakulären Einbrüchen geführt. Manche Schlüssel, speziell die von den US-Exportbestimmungen erlaubten Schlüssel mit weniger als 128 Bit, sind unbefriedigend und sollten nicht verwendet werden. Das Konzept selbst aber ist reif und erfolgreich.

Dank TLS/SSL ist das Internet also völlig sicher? Leider immer noch nicht: Nicht das Surfen ist sicher, sondern nur die HTTPS-Verbindung zwischen den Endpunkten einer bestimmten Verbindung – und das ist etwas entscheidend anderes als das gesamte Internet. Dort gibt es noch ein paar weitere Risikofaktoren.

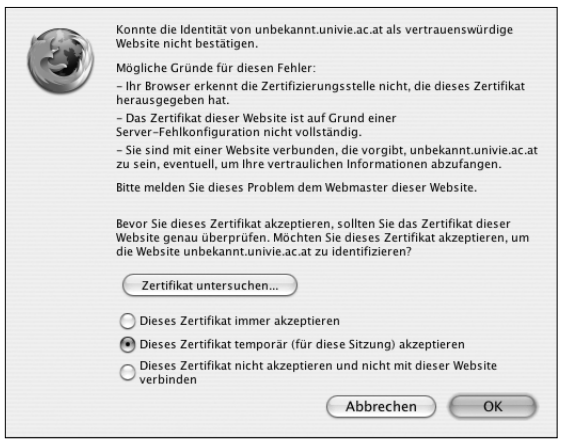


Abb. 9: Warnmeldung bei zweifelhaftem Zertifikat

Abb. 10: Anzeigen der vom Browser anerkannten Zertifizierungsinstanzen (Aufruf mittels *Einstellungen – Erweitert – Sicherheit – Zertifikate anzeigen – Zertifizierungsstellen*)

Der Server

Was nutzt es, wenn die Daten bombensicher transportiert werden, aber der Server nicht dichthält? Leider nichts. Und gerade hier existiert eine ganze Reihe von Problemzonen:

- Menschliches Versagen – eine der größten Bedrohungen der EDV – gibt es auch bei Server-AdministratorInnen.

- Es ist möglich (und auch bereits passiert), dass Fehler in der Server-Software den Schutz zumindest schwächen.

- Der Server könnte gehackt werden. Bei einem gut gewarteten Server ist die Wahrscheinlichkeit dafür zwar gering, aber völlig ausschließen kann das niemand.

- Nachdem in einen Server eingebrochen wurde, kann auch sein privater Schlüssel gestohlen worden sein. Damit ist auch der Zertifikatsschutz hinfällig. Deshalb muss im Fall eines Einbruchs unbedingt das Zertifikat widerrufen und ein neues bestellt werden. Leider prüfen real existierende Browser die so genannten *Certificate Revocation Lists* (CRLs), in denen die widerrufenen Zertifikate aufgelistet werden, derzeit nicht.

- Der Serverbetreiber könnte in Konkurs gehen oder eine seiner Wartungsfirmen könnte den Datenschutz nicht ganz ernst nehmen. Wer aus Konkursmassen oder bei eBay gebrauchte Festplatten kauft, bekommt oft unglaubliche Mengen an Kreditkartendaten oder sonstigen vertraulichen Informationen gratis dazu.[12)]

12) Garfinkel, Simson L.: *Zero-Klick Security* (`www.simson.net/ref/2006/medialab-march6.pdf`)

13) Die vielgerühmten Chipkarten, Iris-Scans, Fingerabdrucksensoren und dergleichen haben ebenfalls mit gravierenden Problemen und Beschränkungen zu kämpfen, sodass in jedem Einzelfall geprüft werden muss, ob sich ihr Einsatz für die geplante Anwendung lohnt.

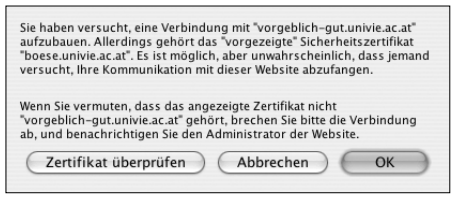


Abb. 11: Warnmeldung, wenn Servername und Zertifikatsbesitzer nicht übereinstimmen
(Bitte lassen Sie sich von dem Wörtchen *„unwahrscheinlich"* nicht in die Irre führen – diese Warnungen sollten unbedingt ernst genommen werden!)

- Webmail, Onlineforen und ähnliche Systeme werden immer wieder durch das so genannte *Cross Site Scripting* missbraucht. Hierbei wird ausgenützt, dass die Inhalte solcher Systeme teilweise vom Benutzer eingefügt werden können, obwohl die Website insgesamt – TLS/SSL-geschützt – unter der Flagge des Betreibers segelt. Bei eBay werden immer wieder Fälle bekannt, wo Benutzer-Passwörter auf diese Weise ausgespäht wurden.

Die Anwenderseite

Der Erfolg des TLS-Schutzes kann ebenso zunichte gemacht werden, wenn beim Webbrowser etwas schief läuft:

- Das beim Server über menschliches Versagen und Softwarefehler Gesagte gilt natürlich auch für den Client.

- Wenn der Benutzer dazu überredet wird, ohne das S in HTTPS sensible Daten zu übertragen, ist TLS/SSL machtlos – da es ja nicht zum Einsatz kommt. Ob es sich hierbei um Fahrlässigkeit oder mangelnde Schulung handelt, ist ein ergiebiges Thema für Schuldzuweisungen.

- Die TLS/SSL-Warnungen werden häufig nicht aktiviert.

- Den Zugang zu Daten oder Diensten mittels UserID und Passwort zu regulieren, ist eine relativ verständliche und bewährte Methode.[13)] Sie wird jedoch in der Praxis dadurch unpraktikabel, dass es so viele Anwendungsgebiete dafür gibt: Einerseits sollte für jeden Dienst ein eigenes Passwort gewählt werden, andererseits wären das zu viele, um sie im Kopf zu behalten. Ein Mindestmaß an Trennung ist dennoch anzuraten: Beispielsweise sollte das Unet- bzw. Mailbox-Passwort nirgendwo sonst verwendet werden.

- Fatal ist es natürlich, wenn der Benutzer ausdrücklich einen anderen Webserver aufruft, als er aufzurufen glaubt. Um das zu erreichen, genügt es oft, eine eMail mit einem plausiblen Vorwand, einen darin enthaltenen Link anzuklicken, zu versenden. Wenn der dort angegebene – vom Angreifer gewählte – Rechnername eine auch nur entfernte Ähnlichkeit mit dem Original hat, werden allzu viele BenutzerInnen darauf reinfallen. (Dem Thema Phishing, das sich im Wesentlichen genau darum dreht, widmet sich der Artikel *Phishing: Bitte nicht anbeißen!* auf Seite 37.)

- Der Rechner könnte kompromittiert oder durch einen Trojaner missbraucht werden. In diesem Fall kann man davon ausgehen, dass jede Tastatureingabe (und damit jedes Passwort) abgehört wird, bevor sie noch im Webbrowser ankommt oder gar von TLS/SSL geschützt werden könnte.

- Dasselbe gilt für im Browser gespeicherte Passwörter und alles, was in Formular-Ausfüllhilfen hinterlegt ist.

Nebenwirkungen

Die Nebenwirkungen von TLS/SSL sind erfreulich gering. Der zusätzliche Rechenaufwand hält sich, zumal bei den heutzutage sehr schnellen Rechnern, in Grenzen. Einen möglicherweise negativen Effekt kann die gesamte Verschlüsselung aber haben: In Netzwerken, wo der HTTP-Verkehr durch einen Proxy geleitet wird, der auch eine Virenscanner-Funktion enthält, wird eben diese umgangen. Es ist einleuchtend, dass der Virenscanner dort nicht scannen kann, wo er nicht hineinsehen kann. Daher kann er in diesem Fall auch keine Viren aus dem Verkehr ziehen.

Fazit

Durch TLS/SSL bzw. HTTPS können Datenverbindungen für Webservices überaus wirkungsvoll gegen Abhören und Fälschen gesichert werden. Das ist ein wichtiger Puzzlestein, zu dem aber noch sichere Server, sichere Clients und die richtige Handhabung durch den Anwender kommen müssen, damit das Bild eines sicheren Webservice komplett wird.

Alexander Talos ■

Neuerungen beim WLAN-Service

Um seine verschiedenen Funknetze (WLANs, *Wireless Local Area Networks*) zu vereinheitlichen und die Servicequalität zu verbessern, hat der ZID im Mai 2006 ein neues WLAN-Management-System in Betrieb genommen. Durch diese Umstellung ergeben sich einige wesentliche Änderungen:

- **Es gibt kein Zeitlimit für die WLAN-Nutzung mehr.** Sie bleiben online, bis Sie sich händisch ausloggen, Ihr Notebook in den Ruhezustand versetzen oder es aus der Reichweite der Accesspoints entfernen. Auch ein **Ortswechsel ohne neuerliches Login** ist jetzt möglich, solange Sie sich nicht aus dem Sendebereich der Accesspoints des ZID bewegen.

- **Die Unterscheidung zwischen Hörsaalnetz und Datentankstellen entfällt** – in den Hörsälen kann nun auch mit Unet-UserID drahtlos gearbeitet werden.

- **Die „Datentankstelle Juridicum" existiert in dieser Form nicht mehr**, sondern wurde in „normale" Datentankstellen umgewandelt. Der Zugang zur Rechtsdatenbank (RDB) ist weiterhin möglich.

Die genannten Änderungen gelten nicht für die verkabelten Datentankstellen – hier bleibt (vorläufig) alles beim Alten.

In diesem Zusammenhang möchten wir nochmals darauf hinweisen, dass an der Universität Wien seit einiger Zeit auch ein verschlüsseltes Funknetz angeboten wird, die **Datentankstelle802.1X**. Sofern Sie ein Notebook unter Windows XP oder Mac OS X 10.4 verwenden, können (und sollten) Sie dieses verschlüsselte WLAN nutzen. Die Konfiguration ist etwas aufwendiger, dafür müssen die Login-Daten aber nur bei der Konfiguration und nicht mehr bei jedem Verbindungsaufbau eingegeben werden. Entsprechende Konfigurationsanleitungen sind unter `www.univie.ac.at/ZID/anleitungen-wlan/` verfügbar; nähere Infos zur Datentankstelle802.1X finden Sie in *Comment 06/1* auf Seite 54 (`www.univie.ac.at/comment/06-1/061_54.html`). Mit UserIDs der Medizinischen Universität Wien kann dieses Service derzeit nicht genutzt werden.

Auch die **eduroam**-Nutzung ist an der Uni Wien möglich. Dabei handelt es sich um ein internationales Projekt, das es erlaubt, mit den Zugangsdaten des Heimatnetzes die WLAN-Infrastruktur zahlreicher europäischer Bildungseinrichtungen zu verwenden (Details siehe *Comment 06/1*, Seite 53 bzw. unter dem URL `www.univie.ac.at/comment/06-1/061_53.html`).

Elisabeth Zoppoth ■

Arbeiten mittels WLAN in den Höfen des Universitätscampus Altes AKH
(Foto: Peter Wienerroither / © Zentraler Informatikdienst der Universität Wien)