WWW.UNIVIE.AC.AT
Alte Adresse, neue Architektur

Ein neuer Webserver?

Seit den Anfängen des Webauftritts der Universität Wien im Jahr 1995 wurde im *Comment* schon mehrmals ein „neuer Webserver" angekündigt.[1)] Diese neuen Webserver waren jedesmal mit einer Erneuerung des Software-Standes und neuen Features verbunden (z.B. die PHP-Unterstützung seit Juni 2005), das Grundkonzept des Servers WWW.UNIVIE.AC.AT wurde aber seit 1995 nicht wesentlich verändert. Im Großen und Ganzen hat sich dieses Konzept auch gut bewährt: Der derzeit verwendete Unix-Server ist sehr leistungsfähig und kann mehrere Millionen Anfragen pro Tag problemlos bewältigen – an Spitzentagen zu Semesterbeginn sind es alles in allem an die 13 Millionen.

Ein Problem dieses „monolithischen" Servers (siehe **Abb. 1**) ist allerdings eine gewisse Anfälligkeit: Der Server beherbergt mehrere Millionen HTML-Dokumente und andere Dateien, zahlreiche CGI-Skripts und PHP-Programme. Jede einzelne Seite kann Ziel einer *Denial of Service*-Attacke werden; Probleme durch ein einziges fehlerhaftes Programm können zu übermäßigem Ressourcenbedarf führen und dadurch den ganzen Server in Mitleidenschaft ziehen. Durch geeignete Maßnahmen kann man solche Probleme zwar eindämmen, aber nicht ganz verhindern. Auch die Software-Wartung ist auf einem so großen und komplexen System schwierig, weil jede Änderung unvorhergesehene Auswirkungen haben kann.

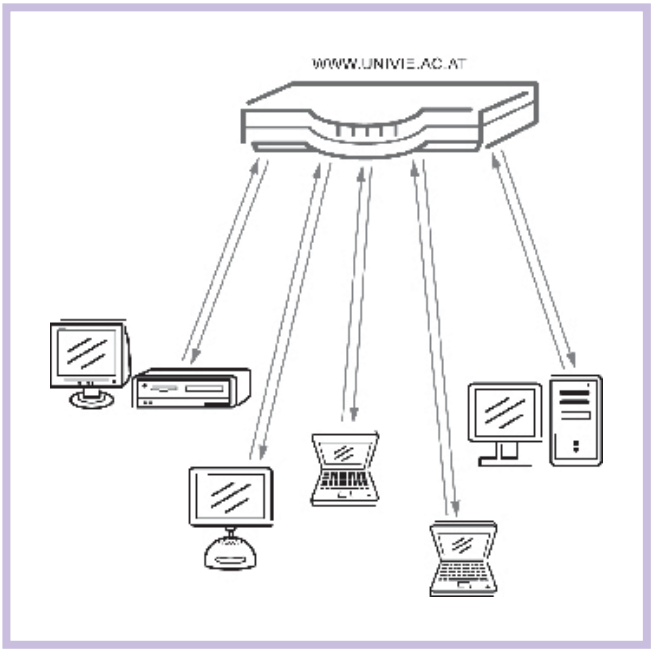

Abb. 1: Das bisherige Konzept des Webservers der Uni Wien: Ein einzelner Server beantwortet alle Anfragen.

Da der aktuelle Server demnächst an die Grenzen seiner Leistungsfähigkeit stoßen wird, ist bald wieder ein „neuer Webserver" erforderlich. Es wäre relativ einfach, die Hardware zu tauschen (es gibt noch wesentlich stärkere Server!), aber um die oben beschriebenen Anfälligkeiten zu beseitigen, hat sich der ZID entschlossen, stattdessen ein radikal neues Konzept von verteilten Servern einzuführen, das im Folgenden näher beschrieben wird.

Das neue Server-Konzept

Es gibt verschiedene Ansätze, ein verteiltes Konzept zu realisieren. Eine Möglichkeit wäre ein Cluster von Servern, die alle unter demselben Hostnamen zu erreichen sind und über ein verteiltes Filesystem alle auf dieselben Daten zugreifen. Ein Vorteil eines solchen Clusters ist die perfekte Lastverteilung (*Load Balancing*) – jede Anfrage kann von jedem beliebigen Server im Cluster beantwortet werden. Wir haben uns jedoch für eine andere Lösung entschieden: Nachdem der Webserver der Universität Wien ein historisch gewachsenes, komplexes System ist, kann eine so weit reichende Umstellung kaum auf einmal durchgeführt werden, sondern muss vielmehr schrittweise und ohne nennenswerte Unterbrechung des laufenden Betriebs erfolgen. Auch sollen möglichst wenige Änderungen von Benutzerseite erforderlich sein – d.h. was bisher funktioniert hat, soll auch weiterhin funktionieren.

Die Hauptbestandteile der neuen verteilten Server-Architektur sind ein *Frontend* und mehrere *Backends*:

- Der **Frontend-Server** ist von außen unter der Adresse WWW.UNIVIE.AC.AT zu erreichen und nimmt alle Anfragen der Klienten (Browser) entgegen. Auch alle virtuellen Hosts (z.B. WWW.UB.UNIVIE.AC.AT) sind auf dem Frontend-Server angesiedelt. Das Frontend beantwortet die Anfragen jedoch nicht selbst, sondern reicht sie unverändert[2)] an den zuständigen Backend-Server weiter, erhält von diesem die Antwort und schickt sie an die Klienten zurück: Das Frontend ist ein so genannter *transparenter Proxy*. Das ist eine wenig anspruchsvolle Aufgabe, die von einem einzigen Server mühelos bewältigt werden kann; als Frontend dient daher bis auf weiteres der bisherige WWW-Server.

- Den Großteil der Arbeit verrichten die **Backend-Server**: Dort befinden sich alle HTML-Dokumente und anderen Daten[3)], dort werden auch alle PHP- und sonstigen Skripts ausgeführt. In der Anfangsphase gibt es nur einen Backend-Server; sobald er ausgelastet ist, können problemlos weitere Server angefügt werden. Dadurch ist

diese Architektur praktisch beliebig skalierbar. Die Backend-Server sind von außen nicht sichtbar und durch eine Firewall vor jeglichem direkten Zugriff geschützt. Auf welchem Backend sich eine Applikation oder ein Dokument befindet, ist vollkommen unerheblich, weil der Hostname des Backend-Servers nirgends aufscheint. Deshalb ist es auch relativ leicht möglich, Applikationen von einem Backend auf ein anderes zu übersiedeln.

Neben dem Frontend und den Backends zählen noch einige andere Server (Datenbank-, Zugangs- und Logserver) zur Server-Farm, die in ihrer Gesamtheit den „neuen Webserver" bildet (siehe **Abb. 2**). Manche dieser Server sind als virtuelle Maschinen unter VMWare implementiert.[4)]

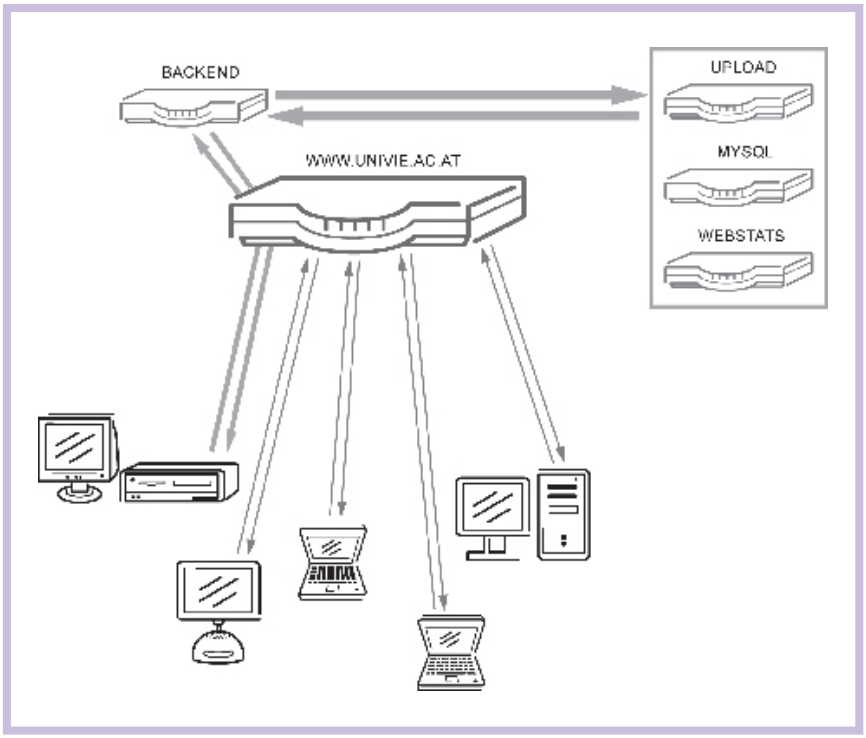

Abb. 2: Der Webserver in der derzeitigen Übergangsphase zu einem verteilten System: Ein Teil der Webseiten ist bereits auf den Backend-Servern angesiedelt; für diese fungiert der Frontend-Server als Proxy. Der Rest befindet sich noch auf dem Frontend-Server.

Software-Ausstattung der Backend-Server

Das neue Konzept mit mehreren Backend-Servern bietet auch den Vorteil, dass auf verschiedenen Servern unterschiedliche Software (Betriebssystem, Webserver, Applikationsserver usw.) installiert werden kann, sodass Applikationen mit beliebigen Anforderungen unterstützt werden könnten. Für einige Anwendungen wird es spezielle Backends geben, die meisten der Backend-Server werden jedoch eine identische Standard-Ausstattung erhalten: eine LAMP-Architektur (*Linux–Apache–MySQL–PHP*), die im Open Source-Bereich häufigste Software-Ausstattung von Webservern.

- **Betriebssystem**: Als Betriebssystem dient Redhat Enterprise Linux Server Release 5 (`www.redhat.com`).

- **Webserver**: Hierfür wird die neueste Version 2.2.4 von Apache eingesetzt (`http://httpd.apache.org/`). Einige lokale Modifikationen der Software sorgen dafür, dass die Backends nichts davon merken, dass sie nicht direkt mit dem Klienten sprechen, sondern mit dem Frontend. Das ermöglicht u.a. eine Zugriffskontrolle auf Basis der IP-Adressen der Klienten, obwohl alle Anfragen eigentlich von der IP-Adresse des Frontends kommen.

- **PHP**: Bisher stand auf dem Webserver der Universität die Version 4.2.2 von PHP (`http://at.php.net/`) zur Verfügung. Mit Ende des Jahres läuft aber der Support für die Version 4 aus. Daher wird empfohlen, PHP-Applikationen möglichst bald auf einen Backend-Server zu übersiedeln (siehe Abschnitt *Migration*), wo die neueste PHP-Version 5.2.4 installiert ist.

- **Perl**: CGI-Skripts in Perl oder anderen Sprachen werden weiterhin unterstützt; Perl (`www.perl.org`) steht in der Version 5.8.8 zur Verfügung.

- **Datenbank**: Auf den Backends ist lediglich ein MySQL-Klient installiert. Die Datenbanken befinden sich auf eigenen Datenbank-Servern, auf denen die Version 5.0 der MySQL-Datenbank (`www.mysql.de`) installiert ist. Auch hier kommen verteilte Server zum Einsatz: Für jeden MySQL-User wird ein virtueller Hostname (*CNAME*) eingerichtet, der beim Öffnen der Datenbankverbindung anzugeben ist; für den User `ihw` lautet dieser beispielsweise IHW.MYSQL.UNIVIE.AC.AT. Dieser *CNAME* ist ein Aliasname für den Datenbank-Server, auf dem die jeweilige Datenbank installiert ist. Dadurch ist es möglich, Datenbanken von einem Server auf einen anderen zu

---

1) siehe Artikel *Ein neuer Webserver für die Uni Wien* in *Comment 01/3*, Seite 16 bzw. unter `http://comment.univie.ac.at/01-3/16/` und Artikel *Gerda geht in Pension* in *Comment 05/2*, Seite 36 bzw. unter `http://comment.univie.ac.at/05-2/36/`

2) Eine Ausnahme bilden nur verschlüsselte Anfragen (HTTPS), die am Frontend entschlüsselt und unverschlüsselt an die Backends weitergereicht werden: Nachdem die unverschlüsselte Übertragung nur in einem geschützten Netz geschieht, stellt sie kein zusätzliches Sicherheitsrisiko dar.

3) Physisch liegen die Daten auf den Speichersystemen des *Storage Area Network* des ZID (siehe Artikel *SAN: Das Storage-Projekt macht Fortschritte* in *Comment 07/1*, Seite 16 bzw. unter `http://comment.univie.ac.at/07-1/16/`), wobei nur die Backend-Server auf die entsprechenden Speicherbereiche (LUNs) zugreifen können.

4) siehe Artikel *Aus eins mach zehn: Der Zauber der Virtualisierung* in *Comment 07/2,* Seite 7 bzw. unter `http://comment.univie.ac.at/07-2/7/`

verschieben (z.B. zwecks gleichmäßigerer Verteilung der Last), ohne dass irgendwelche Änderungen an Applikationen erforderlich werden.

Von minimalen Anpassungen abgesehen ist die Konfiguration des Webservers auf den Backends identisch mit der bisherigen Konfiguration, sodass alle Funktionen wie Authentifizierung mittels u:net- und Mailbox-Passwörtern weiterhin unverändert eingesetzt werden können. Eine kleinere Änderung gibt es bei der „Rechtschreibprüfung" durch das Apache-Modul *mod_speling*: Dieses ist nun so konfiguriert, dass es nur Abweichungen bei der Groß-/Kleinschreibung von URLs stillschweigend ausbessert, aber keinerlei andere Korrekturen (z.B. vertauschte Buchstaben) vornimmt.

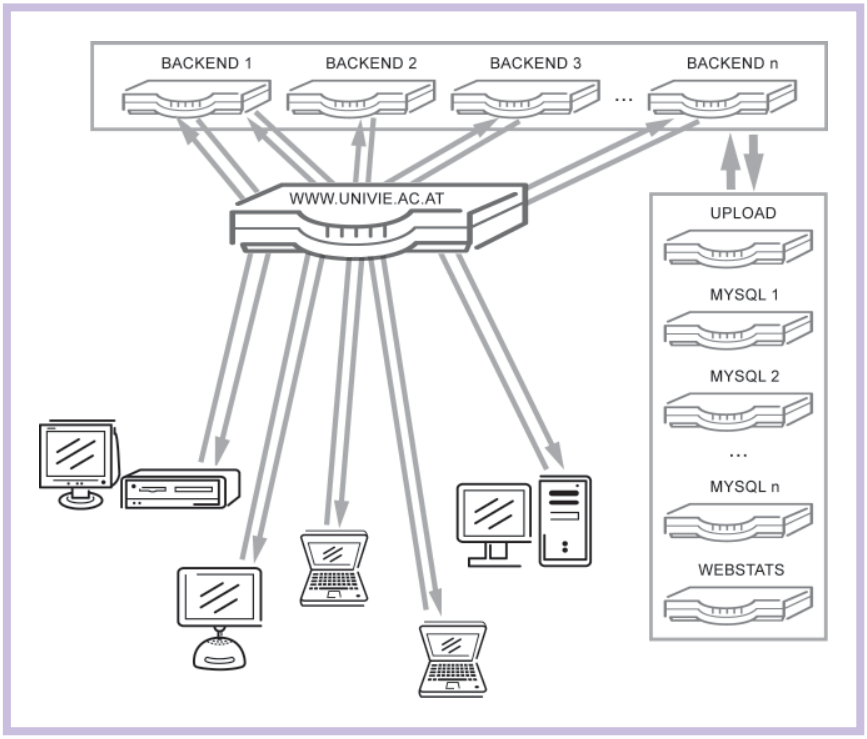

Abb. 3: Endausbau des verteilten Systems: Alle Daten und Anwendungen befinden sich auf den Backends, das Frontend dient nur als Proxy.

Sicherheit und Berechtigungen

Im Abschnitt *Sicherer Multiuser-Betrieb mit PHP und CGI – eine Herausforderung* des eingangs erwähnten *Comment*-Artikels *Gerda geht in Pension* wurde genau beschrieben, welche Schwierigkeiten damit verbunden sind, gleichzeitig PHP- und CGI-Unterstützung anzubieten, den BenutzerInnen möglichst viele Freiheiten zu erlauben und dennoch einen sicheren und stabilen Betrieb aufrecht zu erhalten. Das Hauptproblem ist, dass PHP-Skripts vom Webserver selbst ausgeführt werden und daher mit den (sehr weit reichenden) Rechten des Webservers laufen. Damit die Skripts verschiedener BenutzerInnen einander nicht in die Quere kommen oder gar auf fremde Daten zugreifen können, sind Einschränkungen der Privilegien von PHP-Skripts mittels der PHP-Konfiguration unerlässlich.

Auf den neuen Backends wurde eine andere Lösung implementiert: PHP-Skripts werden nicht vom Apache-Webserver ausgeführt, sondern als externe Prozesse über das CGI-Interface. Das hat folgende Vorteile:

- PHP- und CGI-Skripts laufen ausschließlich mit den Rechten und Privilegien des Eigentümers (*Owner*) des Skripts. Auch Dateien, die von PHP-Skripts angelegt wurden, gehören nunmehr dem Eigentümer des Skripts und nicht mehr dem User `wwwphp`.

- PHP- und CGI-Skripts können in beliebigen Verzeichnissen ausgeführt werden. Das gesonderte Beantragen der PHP-Unterstützung (*nur im Unterverzeichnis php* bzw. *überall*) entfällt.

- Die PHP-Einstellungen *Safe Mode* und *open_basedir* sind damit nicht mehr nötig. Das erleichtert die Installation etlicher Programme, die mit diesen Einstellungen nur schwer zum Laufen gebracht werden können.

Der Nachteil des Ausführens von PHP-Skripts über das CGI-Interface ist eine schlechtere Performance, weil dafür ein eigener Prozess gestartet werden muss. Aus diesem Grund wird die FastCGI-Schnittstelle verwendet, die im Apache-Modul *mod_fcgid* (`http://fastcgi.coremail.cn/`) implementiert ist: Es werden externe Prozesse gestartet, die zahlreiche Skripts abarbeiten können.[5] Zusätzlich sorgt der eAccelerator (`http://eaccelerator.net/`) für eine optimale Performance von PHP-Skripts.

Ein neuer Zugangsserver

Bisher erfolgte die Wartung von Webseiten durch direkten Zugriff bzw. Datenübertragung auf WWW.UNIVIE.AC.AT. Einen solchen Zugriff auf die Backends wird es nicht geben; stattdessen steht dafür ein eigener Zugangsserver namens UPLOAD.UNIVIE.AC.AT zur Verfügung. Die Verzeichnisstruktur ist dieselbe wie auf den Backends.

Anders als bisher sind nun jedoch Dateien im Home-Verzeichnis (z.B. `/u/home/ihw`) für den Webserver nicht mehr sichtbar, daher müssen HTML-Dokumente im Unterverzeichnis `html` abgelegt werden (z.B. in `/u/home/ihw/html`). Will man vermeiden, dass bestimmte Daten via Webbrowser abrufbar sind, müssen sie außerhalb dieses Unterverzeichnisses gespeichert werden. Der bisherige Verzeichnisname `/u/www/username` (z.B. `/u/www/ihw`) funktioniert auch weiterhin.

5) FastCGI steht nur für PHP-Skripts zur Verfügung, für „normale" CGI-Skripts wird weiterhin ein eigener Prozess gestartet.

Der Zugang zum Upload-Server erfolgt auf denselben Wegen wie bisher zum WWW-Server: Die Datenübertragung kann mittels FTP oder (empfohlen) sFTP erfolgen; `\\upload.univie.ac.at\username` kann als Netzlaufwerk verbunden werden; auch Login mittels SSH und interaktives Arbeiten am Server ist möglich. Lediglich Telnet wird aus Sicherheitsgründen nicht mehr unterstützt. Auf dem Upload-Server sind dieselben Versionen von Perl und PHP installiert wie auf den Backends, sodass Applikationen dort interaktiv getestet werden können.

Logfiles und Statistiken

Wer eine Webseite publiziert, will verständlicherweise auch wissen, wie oft und von wem sie gelesen wird. Aus diesem Grund besteht schon seit vielen Jahren die Möglichkeit, die Logdateien einzusehen; sie werden auch automatisch von mehreren Statistikprogrammen ausgewertet.

Dieses beliebte Service ist nun schon etwas in die Jahre gekommen – die verwendeten Statistikprogramme sind nicht mehr die aktuellsten. Die Reorganisation des Webservers wurde daher zum Anlass genommen, auch dieses Service rundum zu erneuern. Dafür wird ein eigener Server eingesetzt, der die Logdateien von diversen Webservern einsammelt und zentral auswertet. Modernere Statistiken werden demnächst unter dem URL `http://webstats.univie.ac.at/` abrufbar sein.

Migration

Wie bereits erwähnt, erfolgt die Inbetriebnahme des neuen verteilten Server-Konzepts schrittweise. Auf dem bisherigen WWW-Server und künftigen Frontend wird der Software-Stand eingefroren, es gibt dort keinerlei Innovationen mehr. Neue Benutzungsberechtigungen werden seit dem 10. September 2007 ausschließlich für das neue System vergeben. Die Migration der bestehenden Accounts (mehr als 1500 Benutzungsberechtigungen, die individuell behandelt werden müssen) wird sich voraussichtlich über mehrere Monate erstrecken, wobei der ZID die jeweils verantwortlichen Subserver-BetreiberInnen rechtzeitig von der bevorstehenden Umstellung ihrer Webseiten verständigt. Im Großen und Ganzen besteht kein Grund zur Eile – mit einigen Ausnahmen:

- Einige Pilot-Anwendungen wurden bereits auf einen Backend-Server übersiedelt. Dabei handelt es sich hauptsächlich um „schwergewichtige" PHP-Applikationen, die hohe Zugriffszahlen aufweisen und den WWW-Server stark belastet haben.

- Wenn Sie schon jetzt umstellen möchten (beispielsweise weil Sie eine neuere PHP-Version brauchen), vereinbaren Sie einfach per eMail an `helpdesk.zid@univie.ac.at` einen Termin für die Migration. Während der Übersiedlung sind die betroffenen Seiten in der Regel nur für wenige Minuten nicht erreichbar: Falls es sich um statische HTML-Seiten handelt, sind keinerlei Änderungen nötig, und auch bei PHP- oder Perl-Skripts sind in den meisten Fällen nur minimale Anpassungen vorzunehmen (in der Regel ändert sich lediglich der Name der MySQL-Datenbank). Gelegentlich sind wegen Inkompatibilitäten zwischen den PHP- und MySQL-Versionen kleinere Code-Modifikationen erforderlich.

- Bei manchen WWW-Accounts gibt es individuelle Sonderlösungen und „Spezialkonstruktionen", die sich nicht automatisch migrieren lassen. Wir werden versuchen, in allen Fällen eine Lösung zu finden, teilweise könnten hier jedoch längere Vorbereitungsarbeiten nötig sein.

Im Endausbau dient der Frontend-Server WWW.UNIVIE.AC.AT nur mehr als reiner Proxy-Server, dessen „Intelligenz" sich darauf beschränkt, zu wissen, welche Webseiten auf welchen Backends liegen (siehe **Abb. 3**). Dann wäre auch der Einsatz eines *Load Balancers* möglich, sodass sich hinter der Adresse WWW.UNIVIE.AC.AT mehrere Frontend-Server verbergen, die sich die Arbeit teilen: Dies würde nicht nur die Skalierbarkeit noch weiter erhöhen, sondern auch für höhere Stabilität sorgen, weil dadurch das Frontend als *Single Point of Failure* wegfällt.

Administration

An der Administration der Benutzungsberechtigungen ändert sich durch das verteilte Server-Konzept nicht viel; Details zur Vergabe und Verwaltung sind unter `www.univie.ac.at/ZID/www-userid/` zu finden. Eine Neuerung ist jedoch, dass WWW-Accounts nunmehr mit einem „Ablaufdatum" versehen werden. Vor dem Zeitpunkt des Ablaufs wird der Verantwortliche kontaktiert und der Account formlos verlängert, sofern er noch benötigt wird. Damit soll u.a. sichergestellt werden, dass die Daten der Kontaktpersonen aktuell bleiben: Zur Zeit gibt es zahlreiche Accounts, die vermutlich nicht mehr benötigt werden, was sich aber kaum verifizieren lässt, da keine Kontaktpersonen mehr bekannt sind. Die Übersiedlung der bestehenden Accounts auf die neuen Backend-Server wird auch zum Anlass genommen, diese Altlasten zu „entsorgen".

Applikationen

Auf dem Webserver stehen mit PHP und Perl mächtige Werkzeuge zur Verfügung, um eigene Anwendungen zu installieren. Dabei hat sich gezeigt, dass etliche populäre Standard-Applikationen oft gewünscht werden und folglich zahlreiche Instanzen dieser Softwareprodukte am Webserver installiert sind: *Content Management Systeme* (CMS), Diskussionsforen, Gästebücher usw. Diese Instanzen unterscheiden sich meist nur marginal voneinander, haben aber oft unterschiedliche Software-Versionen – und manchmal auch unterschiedliche Sicherheitslücken. Hier wäre eine einzige zentrale Installation effizienter, die nur einmal gewartet werden muss, aber allen BenutzerInnen zur Verfü-

gung steht. Wir werden uns daher in Zukunft verstärkt um die Unterstützung solcher Applikationen auf unseren Webservern bemühen, wodurch Programmieren in PHP oder Perl in vielen Fällen überflüssig werden soll.

Ein erster Schritt in diese Richtung wurde mit dem Typo3-Projekt[6] gemacht: Hierbei wird ein leistungsfähiges und flexibles Content Management System zur Verfügung gestellt. Für Institute bzw. Projekte, die ihren Webauftritt im Rahmen des Typo3-Projekts erstellen, sind die in diesem Artikel beschriebenen Details weitgehend irrelevant: Für Typo3 gibt es dedizierte Backend-Server, und die Wartung und Pflege der betreffenden Webseiten erfolgt ausschließlich mit Hilfe von Typo3, sodass man sich um die Eigenschaften des darunterliegenden Webservers nicht zu kümmern braucht.

Erneuerung des Webauftritts der Universität Wien

Nicht nur die Hardware und Architektur des Webservers wird erneuert, auch Inhalt und Form der Webseiten sollen modernisiert werden: Zwar ist auf den verschiedenen Subservern eine Unmenge an Informationen zu finden, jedoch besteht der Webauftritt der Uni Wien aus zahlreichen weitgehend unabhängigen Einzelprojekten, die sich in der Qualität von Inhalt und Form, im Design und in der Organisation stark unterscheiden. Die DLE *Öffentlichkeitsarbeit und Veranstaltungsmanagement* hat den Auftrag, ein Gesamtkonzept für die Erneuerung des Webauftritts der Universität Wien zu erstellen.

Es ist klar, dass ein so umfangreiches Projekt nicht von heute auf morgen verwirklicht werden kann. Als erster Schritt werden daher die Startseite und die in der Hierarchie unmittelbar darunter liegenden Seiten erneuert; die modernisierte Startseite soll in Kürze online sein. Für diese Seiten wird ein eigener Backend-Server zur Verfügung stehen, um höchstmögliche Stabilität zu gewährleisten.

Wie auch immer der neue Webauftritt der Uni Wien im Detail aussehen wird: Mit dem Konzept einer Server-Farm mit Frontend, Backends und Datenbank-Servern steht eine flexible und skalierbare Hardware-Plattform und Software-Architektur zur Verfügung, die auf absehbare Zeit für alle Anforderungen gerüstet ist.

Peter Marksteiner

6) siehe Artikel *Webauftritte leicht gemacht: Typo3 an der Universität Wien* in *Comment 06/3*, Seite 37 bzw. unter `http://comment.univie.ac.at/06-3/37/`

Hochschulschriften-Service der Universitätsbibliothek Wien

Dem internationalen *state of the art* entsprechend können ab sofort Abschlussarbeiten von AbsolventInnen der Universität Wien (Diplomarbeiten, Dissertationen und Masterstheses) als elektronischer Volltext auf dem Server `http://othes.univie.ac.at/` abgerufen werden. AbsolventInnen haben hier die Möglichkeit, ihre Diplomarbeiten und Dissertationen zu veröffentlichen – sofern dadurch keine rechtlichen Bestimmungen verletzt werden – und damit ihre Abschlussarbeit weltweit zur Verfügung zu stellen.

Mit Hilfe strukturierter Metadaten werden die auf diesem Server gespeicherten Dokumente bibliographisch beschrieben und über nationale und internationale Bibliothekskataloge, Suchmaschinen und andere Nachweisinstrumente erschlossen und somit suchbar gemacht. Die Zitierfähigkeit wird durch eine dauerhafte und stabile Internetadresse garantiert. Darüber hinaus trägt die elektronische Veröffentlichung zum Schutz vor Plagiierung bei, da durch die bessere Zugänglichkeit Abschreibende leichter enttarnt werden können. Sollten auch Sie Interesse haben, Ihre Abschlussarbeit in elektronischer Form einer breiten

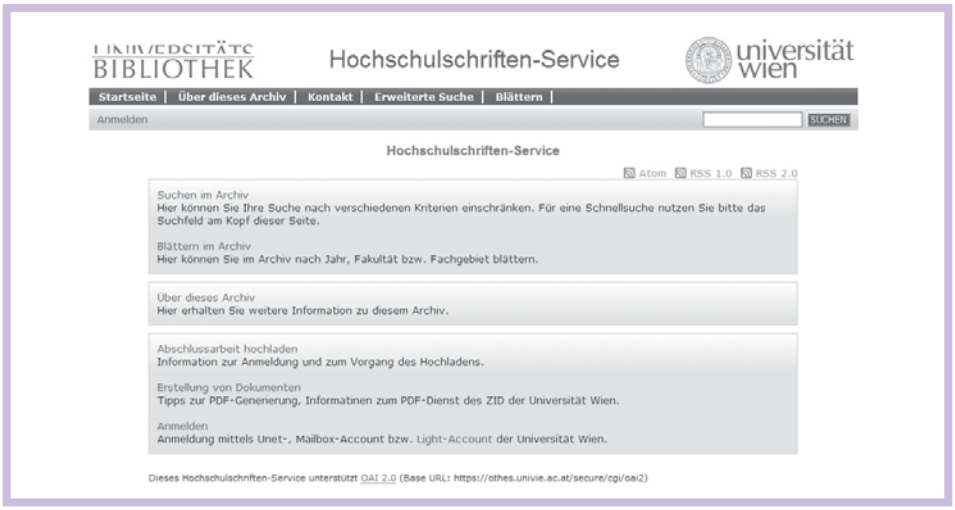

Abb. 1: Startseite des neuen Hochschulschriften-Service (http://othes.univie.ac.at/)

Öffentlichkeit zugänglich zu machen, gehen Sie folgendermaßen vor:

1. Um auf die Eingabe-Seite zu gelangen, müssen Sie sich mit Ihrer u:net- oder Mailbox-UserID anmelden. Sollten Sie keinen gültigen Account der Uni Wien mehr besitzen, können Sie eine befristete Light-UserID per eMail an `thesis-help.ub@univie.ac.at` beantragen.

2. Nach der Anmeldung tragen Sie in die vorgegebenen Felder die Metadaten ein: Autor, Titel etc. Beachten Sie bitte, dass dem internationalen Standard entsprechend ein kurzes Abstract (maximal 250 Worte) anzugeben ist. Die Eingabe-Oberfläche bietet die Möglichkeit, jederzeit abzubrechen und zu einem späteren Zeitpunkt fortzufahren.

3. Die Abschlussarbeit ist als **ein** Dokument im PDF-Format – in der von Adobe spezifizierten Version PDF 1.4. – hochzuladen. Falls Sie keinen Zugang zu einem PDF-Konverter haben, können Sie das PDF-Service des ZID verwenden (siehe `http://othes.univie.ac.at/pdf.html`).

4. Nach Prüfung der Angaben erfolgt die Freigabe durch die Universitätsbibliothek Wien.

Mag. Adelheid Mayer
(DLE Bibliotheks- und Archivwesen)

Umstellungen beim Mailing

Geänderte Servernamen für Studierende

Um das Mailsystem der Uni Wien weiter zu vereinheitlichen, wurden im August 2007 einige Veränderungen vorgenommen. Als Folge davon können nun sowohl Uni-MitarbeiterInnen als auch Studierende den **Posteingangsserver IMAP.UNIVIE.AC.AT** verwenden. Der bisherige Server für Studierende (IMAP.UNET.UNIVIE.AC.AT) funktioniert auch weiterhin; wir empfehlen aber allen Studierenden, den neuen Servernamen in die Konfiguration des eigenen Mailprogramms einzutragen (Details siehe `www.univie.ac.at/ZID/anleitungen-mailing/`). Insbesondere wenn die Datenübertragung vom Server zum PC mittels SSL verschlüsselt werden soll, ist es ratsam, den neuen Servernamen anzugeben: Wenn SSL aktiviert ist und noch der alte Name verwendet wird, erhält man bei jedem Verbindungsaufbau zum Posteingangsserver eine Fehlermeldung bezüglich des Serverzertifikats.

Für den Versand von eMail kommt nach wie vor der **Postausgangsserver MAIL.UNIVIE.AC.AT** zum Einsatz. Auch hier kann die Verbindung vom PC zum Server mittels SSL (über Port 465) verschlüsselt werden. Außerdem empfehlen wir, SMTP-Authentifizierung zu aktivieren, um den Mailversand über unseren Server auch von außerhalb des Uni-Datennetzes – z.B. mit mobilen Geräten – zu ermöglichen.

Die neuen Einstellungen für die Konfiguration Ihres Mailprogramms finden Sie in der Tabelle unten. Noch ein Hinweis: Im Zuge des Software-Updates in den PC-Räumen (siehe Seite 19) wurden dort die Einstellungen des Mailprogramms Thunderbird automatisch richtig gesetzt. Wenn Sie mit Thunderbird in den PC-Räumen der Uni Wien arbeiten, müssen Sie also keinerlei Änderungen vornehmen.

Thomas Riener

	Studierende	MitarbeiterInnen
Mailadresse	a*Matrikelnummer*@unet.univie.ac.at	*vorname.nachname*@univie.ac.at
Protokoll	IMAP (alternativ POP3)	IMAP (alternativ POP3)
	Posteingangsserver	
Servername	**IMAP.UNIVIE.AC.AT**	**IMAP.UNIVIE.AC.AT**
Benutzername	u:net-UserID (a*Matrikelnummer*)	Mailbox-UserID (z.B. `zufallr0`)
Passwort	u:net-Passwort (5–8 Zeichen)	Mailbox-Passwort (5–8 Zeichen)
SSL	Port 993 (alternativ POP3: 995)	Port 993 (alternativ POP3: 995)
	Postausgangsserver	
Servername	**MAIL.UNIVIE.AC.AT**	**MAIL.UNIVIE.AC.AT**
SMTP-Auth	ja	ja
Benutzername	u:net-UserID (a*Matrikelnummer*)	Mailbox-UserID (z.B. `zufallr0`)
Passwort	u:net-Passwort (5–8 Zeichen)	Mailbox-Passwort (5–8 Zeichen)
SSL	Port 465	Port 465

Neuer VPN-Server: Bitte verschlüsseln Sie Ihre Verbindung!

Manche Netzwerkdienste der Uni Wien wie z.B. das Datenbank-Service der Universitätsbibliothek sind nur mit einer IP-Adresse der Universität verwendbar – d.h. entweder direkt aus dem Uni-Datennetz, über einen Wählleitungs- oder Breitbandzugang der Universität oder aber über eine VPN-Verbindung (*Virtual Private Network*, Näheres unter `www.univie.ac.at/ZID/vpn/`). Da künftig keine direkten Breitbandanbindungen zum Universitätsdatennetz mehr angeboten werden (siehe Seite 6), ist mit einem entsprechenden Zuwachs bei den VPN-Verbindungen zu rechnen.

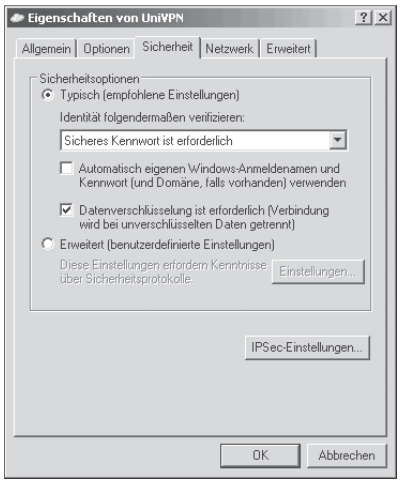

Abb. 1: Umstellen auf verschlüsselte Verbindung (Windows XP)

Um dieser Entwicklung Rechnung zu tragen, wurde der VPN-Server der Uni Wien am 2. Oktober 2007 durch eine neue Maschine ersetzt, die deutlich mehr gleichzeitige VPN-Verbindungen abwickeln kann.

Eine Eigenschaft des neuen Servers ist, dass er nur verschlüsselte Verbindungen zulässt. Diese sind inzwischen aber auch mit den mitgelieferten „Bord-Mitteln" von Windows XP/Windows Vista und Mac OS X 10.4.x/10.5.x leicht zu realisieren. Die dafür nötige Konfigurationsumstellung bereits installierter VPN-Klienten unter Windows ist nicht besonders schwierig:

- Klicken Sie unter ***Systemsteuerung – Netzwerkverbindungen*** mit der *rechten* Maustaste auf das Icon der VPN-Verbindung, wählen Sie im Kontextmenü die Option ***Eigenschaften*** und dann die Registerkarte ***Sicherheit***.
- Wählen Sie hier bei *Sicherheitsoptionen* den Punkt ***Typisch (empfohlene Einstellungen)*** und aktivieren Sie das Kontrollkästchen bei ***Datenverschlüsselung ist erforderlich*** (siehe **Abb. 1**).
- Klicken Sie anschließend auf die Schaltfläche ***IPSec-Einstellungen*** (unter Windows Vista ist diese auf der Registerkarte *Netzwerk* zu finden) und geben Sie als Passwort ***vpnsec*** ein.

Schon funktioniert Ihre VPN-Verbindung zum neuen Server auch mit IPSec-Verschlüsselung. Genaue Anleitungen sind unter `www.univie.ac.at/ZID/anleitungen-vpn/` zu finden.

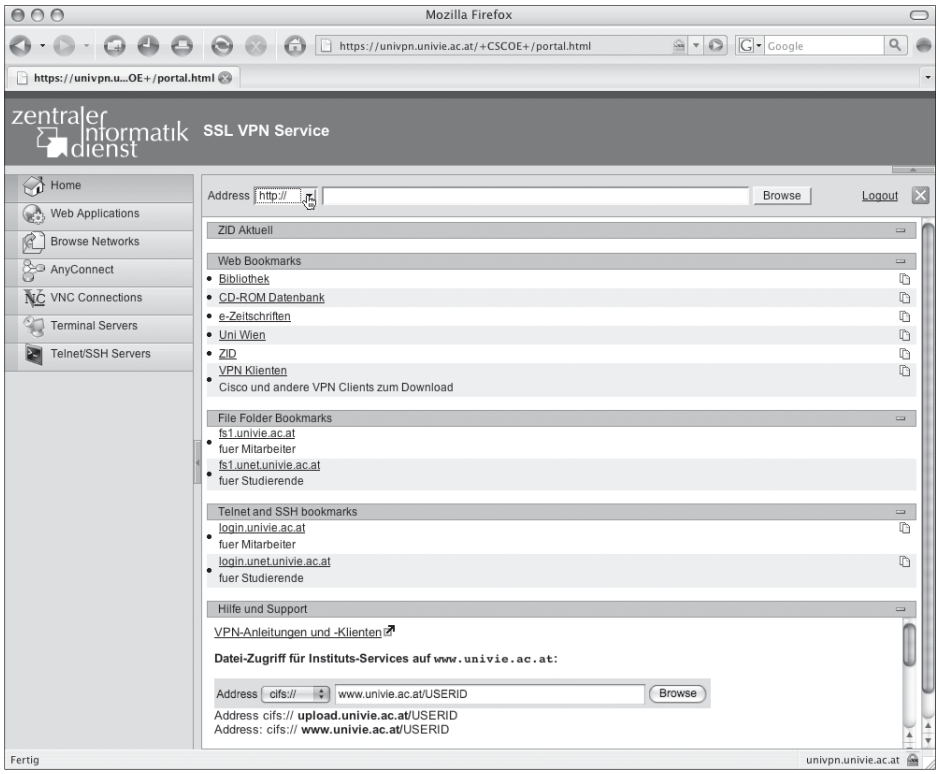

Abb. 2: Startseite des neuen WebVPN-Servers der Universität Wien

Wie bisher ist unter `https://univpn.univie.ac.at/` auch ein VPN-Zugang via Webbrowser möglich. Hier bietet der neue Server ebenfalls zahlreiche neue Optionen – beispielsweise sind jetzt vorkonfigurierte Links zu wichtigen Uni-Servern verfügbar, sodass nun unter anderem auch ein VPN-Zugriff auf die Fileserver der Universität mit einem Mausklick erfolgen kann (siehe **Abb. 2**).

Die Auswahlliste neben dem Punkt *Address* (oben links) enthält eine Reihe von Netzwerkprotokollen, die über die WebVPN-Verbindung verwendet werden können. Weiter unten auf der Startseite des VPN-Servers sind unter dem Punkt *Hilfe und Support* die wichtigsten Daten für den VPN-Zugriff auf Universitätsserver zusammengefasst.

Franz Kaltenbrunner

Gute Seiten – Schlechte Seiten

Die Suche nach Strategien, das Websurfen sicherer zu machen

Feuer ist am Dach, wenn ein Computer, statt seinem Eigentümer (m/w) treu zu dienen, ihn im Auftrag fremder Mächte ausspioniert, ihn ungefragt mit Werbung traktiert oder einfach „nur" unbemerkt kriminellen Nebengeschäften nachgeht – wenn also böse Software, so genannte *Malware*, auf dem Rechner ihr Unwesen treibt. Doch wo kam sie her? Allzu oft lautet die Antwort: Der User hat sie höchstpersönlich aus dem Web heruntergeladen und auf seinem Computer installiert. Nicht ganz absichtlich, aber letztlich eben doch.

Neben Webseiten mit Malware gibt es zum Beispiel auch so genannte *Phishing*-Seiten[1], die dem Anwender z.B. die Bankdaten herauslocken, um sein Konto leer zu räumen, oder Webseiten, die ihm – völlig untechnisch – mit einem Gratis-Service ein überteuertes Abonnement andrehen (siehe **Abb. 1**). Das Spektrum der „bösen Webseiten" ist nur schwer einzugrenzen, und manch einer würde gern in einem Aufwaschen auch gegen Bombenbastelanleitungen, Pornoseiten und vieles mehr vorgehen. Dieser Artikel gibt einen Überblick über die Methoden, mit denen man derzeit der Bedrohung durch böswillige Webseiten zu begegnen versucht. Gleich vorweg: Der Stein der Weisen ist noch nicht gefunden worden.

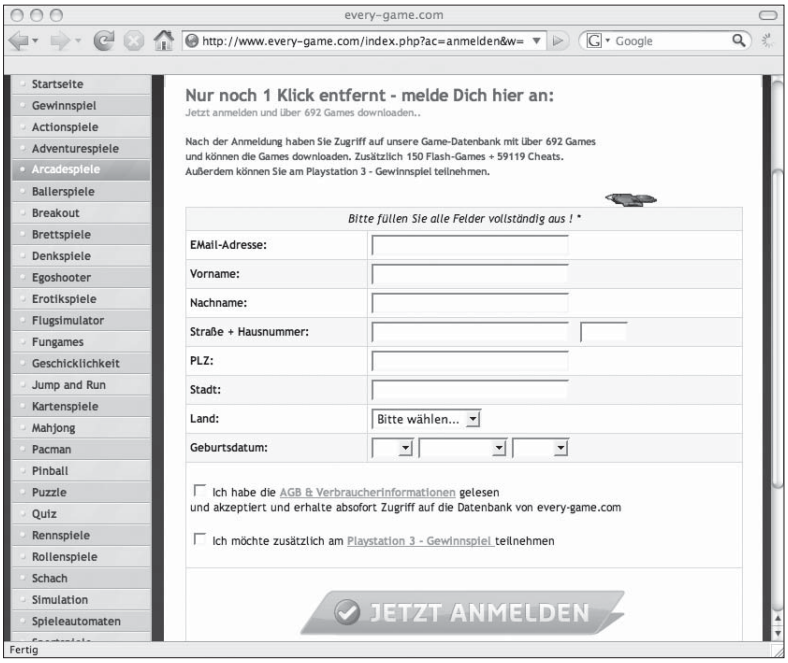

Abb. 1: Ein Dauerbrenner bei Konsumentenschutzorganisationen: Nur wer sich mit dem Scrollbalken bis zum Ende der Seite vorarbeitet, sieht, dass er hier einen Vertrag abschließt und sich zur Zahlung von EUR 59,95 verpflichtet.

Fahrlässige Gemeingefährdung?

Computerzwischenfälle sind wie Wohnungsbrände häufiger auf Fahrlässigkeit als auf technische Gebrechen zurückzuführen. Anders als beim Zündeln neben der Gasflasche ist es in der Computerwelt aber für den Laien oft schwierig oder unmöglich, die drohende Gefahr zu erkennen. Auch wer nicht auf alles klickt, das nicht bei drei auf den Bäumen ist, sondern nur Musik oder Videos von einer Webseite herunterlädt, ein paar nützliche Tools für sein Windows oder Word ausprobiert oder gemäß der eMail-Anleitung von „Administrator" seinen Computer mit dem neuesten Sicherheitsprogramm versieht, kann dadurch böse Software installieren:

- Der **Download von Musik oder Filmen** mag urheberrechtlich nicht immer korrekt sein, sicherheitstechnisch ist das aber irrelevant. Dennoch gelangen die Schadprogramme häufig auf diesem Weg auf den Rechner, weil die angeblichen Musikstücke nicht, oder nicht nur, Musik enthalten. Beispielsweise kann sich die Malware als selbstextrahierendes Archiv tarnen – der User muss also nur doppelklicken und hat sie schon gestartet. Wenn dabei zusätzlich auch noch die gewünschte Musik herauskommt, bemerkt er seinen fatalen Fehler nicht einmal.

- Ähnliches gilt für die nützlichen **Tools**, die zuhauf im Internet zu finden sind. Wer weiß schon so genau, ob sie wirklich nur das tun, was sie zu tun behaupten? Selbst bei Software, die einen guten Ruf hat, kann es sein, dass man auf irgendeiner Webseite eine manipulierte Version davon erwischt – und schon ist das Malheur passiert.

- Auch das gutgläubige **Befolgen von Anweisungen** oder Tipps, die man per eMail erhalten hat, ist gefährlich. Diese stammen nämlich oft von Schwindlern, die sich z.B. als Microsoft, Netzwerkadministrator oder dergleichen ausgeben, um den Anwender dazu zu bringen, höchstpersönlich genau die Software zu installieren, die er lieber nicht auf dem PC haben möchte.

- Für die folgenden Betrachtungen ist es sinnvoll, auch noch ein Szenario aus der Kategorie der technischen Gebrechen einzubeziehen: Der User klickt auf einen

1) Näheres dazu finden Sie im Artikel *Phishing – Bitte nicht anbeißen!* in *Comment 06/2*, Seite 37 bzw. unter `http://comment.univie.ac.at/06-2/37/`.

Link (z.B. aus der Ergebnisliste einer Google-Suche), ruft also nichtsahnend eine Webseite auf, und schwuppdiwupp ist die Malware am Rechner. Dafür müssen drei Voraussetzungen gegeben sein: Es gibt eine Sicherheitslücke im Browser, diese ist noch nicht durch ein Update behoben worden, und die aufgerufene Seite nützt das aus. Hier ist man als Anwender völlig chancenlos, außer durch totale Web-Abstinenz.

Technisch gesehen ist in den geschilderten Szenarien – und in vielen weiteren – der User selbst schuld am Schaden, den er erleidet. Doch was genau hat er falsch gemacht? Nicht jeder kann ein Sicherheitsexperte sein (und selbst diese sind nicht allwissend), daher kann man dem Normalverbraucher nur selten einen Vorwurf machen, wenn er auf solche Tricks hereinfällt. Was beim Zündeln unter fahrlässige Gemeingefährdung fallen würde, ist also in der IT-Welt ein nicht vorwerfbarer Fehlgriff – Freispruch!

Wie kann man sich schützen?

Gegen die Bedrohung durch Malware gibt es vier klassische Gegenstrategien: Virenscanner, regelmäßige Software-Updates, die Verwendung exotischer Software und Misstrauen.

- Der **Virenscanner** am PC ist eine Selbstverständlichkeit und sollte idealerweise einschreiten, sobald der User eine schadensträchtige Datei auf seinen Rechner holt. Allerdings können Virenscanner nur bekannte Malware und hinreichend ähnliche Programme erkennen. Neu geschriebene Malware wird erst erkannt, sobald sie entdeckt wurde, die Antivirus-Hersteller entsprechende Updates bereitgestellt haben und diese auch am PC installiert wurden. Daraus folgt zweierlei: a) Die Virenscanner-Dateien müssen permanent aktualisiert werden, alles andere wäre grob fahrlässig. b) Es gibt stets Malware, die trotz Virenscanner auf den PC gelangen kann.

- Dass Betriebssystem und Anwendungsprogramme regelmäßig mittels **Updates** auf den neuesten Stand gebracht werden müssen, hat ähnliche Gründe: Um zu verhindern, dass manipulierte Webseiten Malware auf einem PC einschleusen, muss jede Sicherheitslücke so rasch wie möglich geschlossen werden. In einigen Fällen kann durch ein Update auch verhindert werden, dass eine Malware ihre volle Wirkung entfaltet. Regelmäßige Updates helfen mit, den Zeitraum, in dem eine Infektion erfolgen kann, kurz zu halten – und senken somit das Risiko.

- Die überwältigende Mehrheit aller Rechner im Internet sind Windows-PCs, die MS-Internet Explorer als Webbrowser verwenden. Für **exotische Software** (und dazu zählt in diesem Zusammenhang schon ein Apple-Rechner mit Safari als Browser) spezielle Malware zu entwickeln bzw. Webseiten zu basteln, die ihre speziellen Sicherheitslücken ausnützen, zahlt sich für die Bösewichte kaum aus. Daher kann auch die Wahl alternativer Software risikominimierend wirken. In der Praxis steht dem allerdings der Nachteil gegenüber, dass manche Webseiten damit nicht funktionieren, weil deren Designer sich statt an Standards an einer spezifischen Version des Internet Explorer orientiert haben.

- Anwendern wird stets ein **gesundes Misstrauen** empfohlen. Eine gute Idee ist, wenn Sie die für Sie zuständigen EDV-Vertrauenspersonen frühzeitig kennenlernen und im Fall von ungewöhnlichen Aufforderungen einfach rückfragen (Kontaktpersonen und -telefonnummern dürfen natürlich nicht der möglicherweise gefälschten Nachricht entnommen, sondern müssen unabhängig davon eruiert werden). In allen anderen Belangen ist Otto Normalverbraucher aber mit dem guten Rat, misstrauisch zu sein, überfordert. Es sind nämlich keineswegs immer Schmuddel- und Raubkopier-Seiten, auf denen Cyberkriminelle auf Opfer lauern – aus der Seriosität eines Anbieters folgt nicht die Sicherheit seiner Webseiten. Ein Klassiker unter den vielen Gründen dafür sind Werbebanner: Der Bösewicht mietet Bannerplatz auf einer Webseite und stellt dort „vergiftete“ Werbebanner ein, und schon sind reihenweise seriöse Seiten zu Hackerseiten geworden. Wie soll man so etwas mit dem Hausmittel des Misstrauens rechtzeitig erkennen?

Diese klassischen Methoden, digitaler Unbill aus dem Weg zu gehen, sind also nach wie vor wirksam und wichtig, gewähren allerdings keinen hundertprozentigen Schutz.

Elektronische Ratgeber

Etwas, das den Anwender davor bewahrt, nichtsahnend böse Webseiten zu betreten, wäre ein großer Fortschritt. Ein solcher Mechanismus müsste allerdings einige Voraussetzungen erfüllen:

- *Benutzerfreundlichkeit*: Die Bedienung des Browsers darf nicht verkompliziert werden – sichere Seiten müssen weiterhin per Mausklick aufgehen, vor unsicheren Seiten muss ohne weiteren Bedienungsschritt gewarnt werden.

- *Transparenz*: Im Falle einer Warnung muss diese so nachvollziehbar sein, dass der Anwender entscheiden kann, ob er die Seite dennoch besuchen will.

- *Privacy*: Es muss gewährleistet sein, dass das Surfverhalten des Users nicht nach außen ausgeplaudert wird.

- *Treffsicherheit*: Es muss zuverlässig vor gefährlichen Seiten, aber möglichst nie vor ungefährlichen Seiten gewarnt werden.

So phantastisch sich das anhören mag, es gibt tatsächlich bereits Ansätze, die User vor dem Bösen zu beschützen. Diese können im Wesentlichen einer von drei Kategorien zugeordnet werden:

- *Maßnahmen bei der Internet-Infrastruktur* (Sperre von Domainnamen oder des Zugangs zu „bösen Seiten"),
- *freiwillige Selbstzensur* von „guten Seiten" (Links auf „böse Seiten" werden nicht angezeigt oder erschwert zugänglich gemacht) oder
- *Filter auf der Seite des Users*, d.h. im Webbrowser[2].

Bevor diese Kategorien näher betrachtet werden, bleibt aber noch eine Frage zu klären: Was ist eigentlich „böse"? Moralische Begriffe umschreiben im IT-Kontext bestenfalls eine Zielrichtung, bedürfen jedoch einer Präzisierung. Die nachfolgend vorgestellten Maßnahmen wenden auch tatsächlich verschiedene Definitionen für „böse Seiten" an, z.B.

- Seiten, die durch Ausnutzung von Sicherheitslücken einen Computer gegen den Willen seines Besitzers manipulieren;
- Seiten, die den Download von Malware anbieten[3];
- Seiten, die sich als Login-Seiten für Online-Banking oder dergleichen ausgeben, um auf betrügerische Weise fremde Zugangsdaten zu erhalten (*Phishing*);
- Seiten, die auf Seiten verweisen, die eines oder mehrere der obigen Kriterien erfüllen;
- ganze Sites, die mindestens eine Seite enthalten, die eines oder mehrere der obigen Kriterien erfüllt. Der Site-Begriff ist allerdings selbst problematisch: Meist wird auf den Domainnamen abgezielt – was z.B. im Falle der Uni Wien die voneinander völlig unabhängigen Websites zahlreicher Institute und Einrichtungen in einen Topf wirft.

Maßnahmen bei der Internet-Infrastruktur: Erst schießen, dann fragen?

Wenn eine „böse Seite" entdeckt wird, wäre es die schnellste Lösung, sie einfach aus dem Verkehr zu ziehen, indem man den Zugang zu ihrem Server sperren lässt; das würde allerdings bedeuten, mit Kanonen auf Spatzen zu schießen. Der logischere und zielführendere – leider aber auch oft vernachlässigte – Weg ist es, den Eigentümer der verseuchten Webseite zu verständigen. Dieser hat die „böse Seite" nur selten selbst bzw. absichtlich installiert und daher in der Regel großes Interesse daran, seinen Webauftritt wieder zu bereinigen. Sollte er nicht kooperieren wollen, kann man sich an seinen Internetprovider wenden: Seriöse Provider haben für den Notfall genügend Handhabe in ihren Geschäftsbedingungen, um Kunden, die das Netz vorsätzlich missbrauchen, wieder loszuwerden.

Hin und wieder kann es vorkommen, dass kurzfristig eine Maßnahme gegen eine „böse Seite" gesetzt werden müsste, dies aber nicht im Einvernehmen mit dem Eigentümer der Seite oder seinem Provider möglich ist – sei es, weil die zuständigen Personen nicht erreichbar bzw. nicht eruierbar sind oder weil sie weder über das notwendige Fachwissen noch über einen kompetenten Dienstleister verfügen. In solchen schwerwiegenden Einzelfällen mag es gerechtfertigt sein, an eine netzweite Sperre zu denken. Dabei muss man sich allerdings einer Reihe kniffliger Fragen stellen:

- Ist die Maßnahme tatsächlich notwendig?
- Ist die Maßnahme tatsächlich ausreichend?
- Ist sie angemessen oder gibt es gelindere Mittel?
- Wie wird sie den Betroffenen (dem, der eine Seite nicht abrufen kann und dem, dessen Seite gesperrt wurde) kommuniziert?
- Wie kann ihre Ursache behoben werden?
- Ist sichergestellt, dass die Maßnahme nach Behebung der Ursache unverzüglich wieder aufgehoben wird?

Jeder Sperre haftet ein Stück Niederlage an, weil das Wichtigste – nämlich das Problem zu analysieren und zu sanieren – nicht gelungen ist. Deshalb sollte sie immer als letztes Mittel angesehen und entsprechend sparsam eingesetzt werden.

Domainsperre

Um im Internet eine Ressource (eine Webseite, eine eMail-Adresse, ...) zu erreichen, bedient man sich meistens eines Domainnamens – beispielsweise `google.at`. Domains sind hierarchisch organisiert, d.h. `google.at` kann nur durch die Verwaltungsinstanz (die so genannte *Registry*) von `.at` eingerichtet werden. In der Hierarchie ganz oben stehen die Länderdomains wie `.at` für Österreich sowie eine Handvoll kategorisierender Domains wie `.com`, `.org` oder `.net`. Der hierarchische Aufbau ist insofern entscheidend, als die übergeordnete Registry (für die österreichischen Domains ist das die *nic.at Internet Verwaltungs- und Betriebsgesellschaft m.b.H.*, siehe `www.nic.at`) rein technisch die Möglichkeit hat, jede Domain in ihrem Bereich aus dem Verkehr zu ziehen – und mit ihr allfällige darunter abrufbare „böse Seiten".

Eine Registry spielt in der virtuellen Welt eine Rolle, die der einer Hoheitsverwaltung gleichkommt – sie allein entscheidet, ob eine Domain und die damit verbundene Firma im Internet existiert oder nicht. Daher muss auch eine Registry Ansprüchen wie Rechtsstaatlichkeit, Unparteilichkeit usw.

2) Es gibt auch Filterkomponenten, die ähnlich einer Firewall an der Verbindung zwischen einem Firmennetz und dem Internet installiert werden. Der ZID der Universität Wien setzt keine solchen Geräte ein und für den Privatanwender kommen sie ebenfalls nicht in Betracht, deshalb wird hier nicht näher auf diese Variante eingegangen.

3) Malware umfasst hier neben alten Bekannten wie Viren, Würmern und Trojanischen Pferden auch Software, die den Anwender ausspioniert (*Spyware*), die Fremden den Zugriff auf den Rechner ermöglicht (*Backdoors*), die in penetranter Weise Werbeeinblendungen vornimmt (*Adware*) oder die ihre Existenz verschleiert und sich nicht wieder deinstallieren lässt (*Rootkits*).

genügen: Einem Domaininhaber, der die formalen Erfordernisse erfüllt (korrekte Kontaktdaten, Entrichtung der Gebühren, funktionierende Nameserver, ...), steht seine Domain zu, bis ein ordentliches Gericht anders entscheidet.

Dennoch werden Registries immer wieder aufgefordert, „böse" Domains zu sperren. Groß sind etwa die Begehrlichkeiten diverser Banken, die Domains von Phishing-Sites zügig stillzulegen. Das ist durchaus verständlich, aber aus den geschilderten Gründen nicht einfach so auf Zuruf möglich. Wie wichtig dieses Festhalten der Registries an rechtsstaatlichen Prinzipien ist, zeigt ein Beispiel aus der jüngsten Vergangenheit: Die Antispam-Organisation Spamhaus (`www.spamhaus.org`) beanstandete bei der Firma nic.at bestimmte `.at`-Domains als „Spamschleudern", konnte deren Sperre jedoch mangels hinreichender Argumente nicht durchsetzen. Daraufhin nahm Spamhaus die Mailserver von nic.at in ihre Blacklist[4] auf, was die eMail-Korrespondenz der österreichischen Registry massiv behinderte. Auch der Universität Wien, die die Domainverwaltungs-Technik für nic.at betreibt, wurde mit Blacklisting gedroht. Spamhaus verspielte mit diesem Willkürakt das Vertrauen zahlreicher Mailserver-Betreiber, die sich darauf verlassen hatten, dass auf dieser Blacklist ausschließlich Spamversender aufscheinen. Wenn eine private Organisation wie Spamhaus derart überreagiert und ihren Einfluss als Druckmittel missbraucht, ist Gegenwehr möglich (viele Serverbetreiber entfernten die Spamhaus-Blacklist aus der Konfiguration ihrer Mailserver); nachdem aber österreichische Firmen nicht einfach aus Österreich abwandern können, muss nic.at als nationale Registry höhere Maßstäbe setzen.

Gegen Domainsperren spricht auch, dass diese nicht bloß die Webseiten betreffen, die sich unter dem um `www` ergänzten Domainnamen finden. Zum einen sind oft auch andere abgeleitete Namen für Webserver in Gebrauch – so wie es nicht nur `www.univie.ac.at`, sondern auch `www.unet.univie.ac.at`, `homepage.univie.ac.at` und viele mehr gibt. Zum anderen können zahllose weitere Services – z.B. Mailserver – mit einem Domainnamen verbunden sein, die in keinerlei Zusammenhang mit einer allfälligen „bösen Seite" innerhalb der Domain stehen. Eine Sperre der Domain würde all diese weiteren Services ebenfalls blockieren und einen unabschätzbaren Kollateralschaden verursachen. Es sollte daher selbstverständlich sein, zuerst den Serverbetreiber zu kontaktieren, bevor man weitere Schritte in Erwägung zieht.

Die Befürworter der Domainsperr-Idee haben allerdings auch ein gutes Argument auf ihrer Seite: Insbesondere bei Phishing-Attacken ist häufig zu beobachten, dass eigens dafür verwendete Domainnamen zum Einsatz kommen, die nicht etwa auf „den Server" mit den gefälschten Seiten verweisen, sondern in schnellem Wechsel auf tausende davon. Werden einige dieser Phishing-Server aus dem Verkehr gezogen, ändert das gar nichts, weil es noch zahllose andere gibt. Eine solche Phishing-Attacke lässt sich nur durch Unschädlichmachen der Domain beenden. Registries können zu diesem Zweck durchaus sinnvolle Maßnahmen treffen und tun dies auch in unterschiedlichem Maße: genauere Identitätsprüfung der Domaininhaber, Beschränkung der Zahl der Nameserver für eine Domain, Beschränkung der Häufigkeit, mit der diese gewechselt werden können, usw.

Eine Domain kann zwar nur durch die jeweils zuständige Registry weltweit gesperrt werden, jeder Netzbetreiber kann sie aber natürlich im eigenen Wirkungsbereich blockieren. An der Uni Wien gilt, nicht zuletzt wegen der Zensurnähe solcher Maßnahmen, das Prinzip der vorsichtigen Zurückhaltung: Grundsätzlich wird nichts gesperrt. Sollte wider Erwarten doch einmal ein besonderer Ausnahmefall eintreten, der solche akuten Sofortmaßnahmen erfordert, wird dies auf den ZID-Webseiten und über die Mailingliste `zid-tech` (Näheres dazu siehe `http://lists.univie.ac.at/mailman/listinfo/zid-tech/`) bekannt gemacht.

Sperre von IP-Adressen

Die IP-Adresse (z.B. `131.130.1.78` – nicht zu verwechseln mit dem landläufig als „Internet-Adresse" bezeichneten URL, z.B. `http://www.univie.ac.at/`) ist für den Anwender normalerweise nicht wahrnehmbar und bezeichnet, stark vereinfacht ausgedrückt, die Netzwerkschnittstelle eines bestimmten Rechners im Internet. Indem man allen Datenverkehr mit seiner IP-Adresse unterbindet, könnte man einen Rechner theoretisch ganz vom Netz abkoppeln und so die „bösen Seiten" aus dem Verkehr ziehen. In der Praxis ist das nicht ganz so einfach: Das Internet wurde wegen seiner militärischen Zielsetzungen so entworfen, dass es auch dann noch funktioniert, wenn mehrere zentrale Knoten ausfallen. Eine Folge davon ist, dass es keine einzelne Stelle gibt, an der eine IP-Adresse netzweit blockiert werden könnte. Fragen, wie sie sich bei Domainsperren stellen, lassen sich hier also einfach auf technischer Ebene abschlägig beantworten. Nicht einmal dem Reich der Mitte, das durch die Chinesische Mauer bereits zweieinhalb Jahrtausende Erfahrung im Abschotten hat, ist es gelungen, sein Internet wirksam gegen unerwünschte Einflüsse abzudichten.

Allein der Betreiber des Netzes, in dem sich eine IP-Adresse befindet, kann diese wirksam blockieren[5] – und er hat auch die Möglichkeit, den betroffenen Administrator zu benachrichtigen. Wenn ein Rechner böse Dinge tut und kurzfristig niemand erreichbar ist, der das abstellen könnte, kann es eine sinnvolle Sofortmaßnahme sein, ihn vorübergehend vom Netz zu nehmen.

---

4) Als *Blacklist* bezeichnet man in diesem Zusammenhang eine „schwarze Liste" von bekannten Spamversendern, die Mailserver-Betreiber zur Spambekämpfung heranziehen können.

5) Gerade bei größeren Netzen kann das allerdings zu einem beliebig komplizierten und langwierigen Unterfangen werden. Für den Bereich der Universität Wien wurde einiges an Arbeit investiert, um die notwendigen Werkzeuge und Abläufe für eine praktikable Internet-Notbremse zu entwickeln.

6) siehe `www.heise.de/newsticker/meldung/96100/`

7) siehe `www.stopbadware.org/home/reportsearch`

Umgekehrt kann man als Netzwerk-Administrator auch den Verkehr des eigenen Netzes mit bestimmten IP-Adressen unterbinden. Das ist aber nur in ganz extremen Ausnahmefällen angemessen: Der Betreiber der ausgesperrten Adresse hat ja keine Möglichkeit, von der Sperre zu erfahren und deren Aufhebung zu veranlassen, sobald er sein Problem bereinigt hat. Das Ergebnis ist, dass sich im Laufe der Zeit die gesperrten Adressen häufen und das Internet löchrig wie ein Emmentaler Käse wird. Ähnlich wie bei Domainsperren ist auch hier der mögliche Kollateralschaden gewaltig, da unter einer IP-Adresse mehrere Websites lagern können: Einem deutschen Provider ist es kürzlich gelungen, mit einem Handstreich statt einer einzigen gleich tausende Sites zu sperren.[6] Auch das Sperren von IP-Adressen ist somit kein allgemein brauchbarer Weg, das Internet sicherer zu machen.

Insgesamt betrachtet schneiden die Maßnahmen bei der Internet-Infrastruktur nicht gut ab. An der Benutzerfreundlichkeit gibt es zwar nicht viel zu bemängeln, und auch die Privatsphäre bleibt weitestgehend gewahrt. Die Transparenz fehlt jedoch völlig: Eine Erklärung, warum eine gesperrte Seite nicht erreichbar ist, erhält der Anwender nicht. Er hat auch keine Möglichkeit, die Seite dennoch aufzurufen. Die Treffsicherheit lässt wegen des erwähnten Kollateralschadens ebenfalls zu wünschen übrig.

Freiwillige Selbstzensur: Die weiße Weste beim Verlinken

Wer bei Google sucht, findet meistens auch etwas. Nicht immer ist es das, was er finden wollte, und manchmal ist es sogar eine Webseite, die Google als „böse Webseite“ einstuft. In diesem Fall steht eine kurze Warnung beim Suchergebnis (siehe **Abb. 2**), und ein Klick auf selbiges führt zu einer Warnungsseite, dem so genannten *Interstitial* (siehe **Abb. 3**). Dieses weist den User abermals auf die Gefahr hin und legt ihm nahe, doch lieber anderswo hinzugehen bzw. sich bei StopBadware (`www.stopbadware.org`) näher zu informieren. Nur auf eigenes Risiko dürfe man die betreffende Seite ansurfen. Offenbar will Google also eine weiße Weste wahren und nicht in den Verdacht geraten, auf „böse Seiten“ zu verlinken – das würde ja implizieren, dass Google selbst auch eine böse Site ist.

Bei nach Googles Ansicht ungefährlichen Seiten ist über die Bedienungsfreundlichkeit des Service nicht zu klagen: Alles ist problemlos erreichbar. Bei Seiten, die mit Googles Bann belegt sind, hat jedoch nur derjenige die Zügel in der Hand, der auch firm in *Cut & Paste* und URL-Leisten ist: Die Warnseite enthält keinen anklickbaren Link. Für weniger geübte Anwender stellt das eine Entmündigung dar, die einer Suchmaschine eigentlich nicht zusteht.

Wer versucht, Googles Urteile nachzuvollziehen, gelangt in ein Dickicht von Policies und vagen Andeutungen. Google verweist auf die Webseite von StopBadware; diese arbeitet

Abb. 2: In der Liste der Google-Suchergebnisse ist der Hinweis auf die Gefährlichkeit einzelner Seiten etwas unscheinbar.

Abb. 3: Der Versuch, auf eine als gefährlich eingestufte Seite zu gelangen, führt zu dieser Warnung.

jedoch überdeutlich heraus, dass Google völlig unabhängig von StopBadware entscheide, welche Seiten „gut“ und welche „böse“ seien. Wer aber mit der Einstufung Googles nicht zufrieden sei, solle dennoch bei StopBadware eine Prüfung beantragen, deren Ergebnis Google wohlwollend prüfen werde. Alles klar?

StopBadware dokumentiert die eigenen Kriterien, nach denen Seiten als Malware eingestuft werden, erklärt dabei aber, „auch“ Meldungen von Google und nicht näher genannten *Trusted Third Parties* zu übernehmen. Beim Herumstöbern in StopBadwares Datenbank fiel auf, dass alle 102 dort verzeichneten österreichischen Sites (Stand von Anfang September 2007) von Google gemeldet wurden. Eine gründlichere Suche ergab, dass von den – laut Homepage – 229 735 so genannten *Reported Sites* sage und schreibe 49 eine Einstufung durch StopBadware selbst erhalten hatten.[7] In jedem dieser Fälle ist jedoch in den Erläuterungen zu lesen, die Seite sei nicht von Forschern von StopBadware *reviewed* worden – das verstehe, wer will. Ein Hinweis auf eine andere *Trusted Third Party* als Google war übrigens nicht zu entdecken.

Doch einmal abgesehen von diesem Pingpong-Spiel hinter den Kulissen: Wie sinnvoll und hilfreich ist Googles Selbstzensur für den User?

- Was die *Treffsicherheit* anbelangt, sollte man meinen, dass eine Suchmaschine, die große Teile des Web ohnehin schon vom Indizieren kennt, auch alle darin versteckte Badware aufspüren oder zumindest deren Abwesenheit zweifelsfrei feststellen kann. Doch weit gefehlt: Im Praxisversuch war es nicht sehr schwierig, durch Eingabe von Keywords aus der Schmuddel- oder Raubkopierecke zu Seiten zu gelangen, vor denen Google nicht warnt, die aber sehr wohl Malware enthalten – in erster Linie *Dialer* (das sind Programme, die das Modem dazu überreden, nicht den Provider, sondern teure Mehrwertnummern anzurufen). Andererseits findet man in den StopBadware-Foren immer wieder glaubwürdige Klagen darüber, dass Sites ohne erkennbaren Grund für gefährlich erklärt werden, StopBadware die betroffenen Webmaster lediglich an Google verweist und der Fall dort im Sande verläuft.[8)]

- Ad *Privatsphäre*: Google kennt zwangsläufig die vom User eingegebenen Suchwörter und seine IP-Adresse – dass es durch den Aufruf der Warnungsseite auch noch erfährt, wenn eine „böse Seite" angeklickt wurde, ist da fast schon nebensächlich.

- Zur *Wirksamkeit* des Ganzen ist zu sagen, dass Google zwar seine eigenen Suchergebnisse weißwaschen, aber nicht verhindern kann, dass der User anderswo auf einen Link zur „bösen Seite" klickt. Das Service deckt somit nur ein kleinen Bruchteil der Risiken ab.

Foren-Postings deuten darauf hin, dass Google bzw. StopBadware fallweise die Webmaster jener Sites verständigt, bei denen ein Problem gefunden wird, dass es dafür aber noch keine fixen Prozesse gibt. Es ist bedauerlich, dass hier die Chance vertan wird, Probleme in direkter Zusammenarbeit zu beseitigen und damit echten Nutzen zu stiften. In Summe wundert man sich, dass Google mit einem derart unausgegorenen Flickwerk offiziell in Betrieb gegangen ist, und das schon vor über einem Jahr.

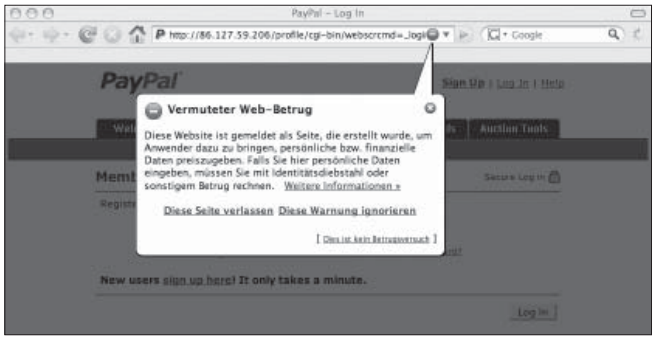

Abb. 4: Firefox-Warnung vor einer Phishing-Seite

Filter auf der Seite des Users: Helferlein im Webbrowser

Sowohl MS-Internet Explorer als auch Mozilla Firefox haben in jüngeren Versionen einen Schutz vor Phishing-Seiten eingebaut. Weiters gibt es einige Plugins, die vor verschiedenen Arten von „bösen Seiten" schützen sollen und unterschiedliche Methoden und Datenquellen nutzen. All diesen Produkten ist gemeinsam, dass sie den URL der Seite, die in den Browser geladen werden soll, mit einer Datenbank abgleichen, die „böse Seiten" verzeichnet. Erweist sich eine Seite als „böse", wechselt zum Beispiel ein Kästchen in einer Menüleiste von grün auf rot oder es wird eine Warnseite eingeblendet.

Die Integration in den Browser hat bestechende Vorteile:

- Der Anwender entscheidet selbst, welche Filter er einsetzen möchte und welche nicht. Diese Freiheit birgt aber auch ein Risiko, das bereits von Virenscannern bekannt ist: Malware, die trotz aller Vorkehrungen einen Weg auf den Computer findet, kann die Filter ebenfalls (und hinterrücks) wieder ausschalten.

- Die Bedienung kann gleichzeitig einfacher und mächtiger gestaltet werden – z.B. durch Popups, die die Gefährlichkeit einer Seite bereits anzeigen, wenn sich der Mauszeiger nur über dem dorthin führenden Link befindet, oder durch ausführliche Hintergrundinformationen in den Werkzeugleisten des Browsers.

- Jede aufgerufene Seite kann individuell überprüft werden. Dies steht im krassen Gegensatz zu Sperren ganzer Domains bzw. Server wegen einer einzelnen Seite, die der Anwender möglicherweise ohnehin nicht besucht hätte. Die Prüfung geht auch über Googles Ansatz hinaus, der nur die Links auf der eigenen Suchergebnis-Seite umfassen kann.

- Sofern die „Böse-Seiten-Datenbank" auf dem PC des Anwenders gespeichert ist und regelmäßig aktualisiert wird, werden keine Informationen über die vom User aufgerufenen Seiten nach außen weitergegeben. Aus technischen Gründen wird allerdings dennoch oft die Online-Abfrage bevorzugt.

---

8) siehe `http://groups.google.com/group/stopbadware/browse_thread/thread/2614b64b3633f34`

9) siehe `www.microsoft.com/germany/windows/products/windowsvista/features/details/ie7antiphishing.mspx`

10) siehe `http://toolbar.live.com/?mkt=de-de`

11) siehe `www.3sharp.com/projects/antiphishing/gone-phishing.pdf`

12) siehe das unter `www.microsoft.com/mscorp/safety/technologies/antiphishing/default.mspx` downloadbare *Anti-Phishing White Paper*

13) siehe `www.codecon.org/2006/program.html#siteadvisor`

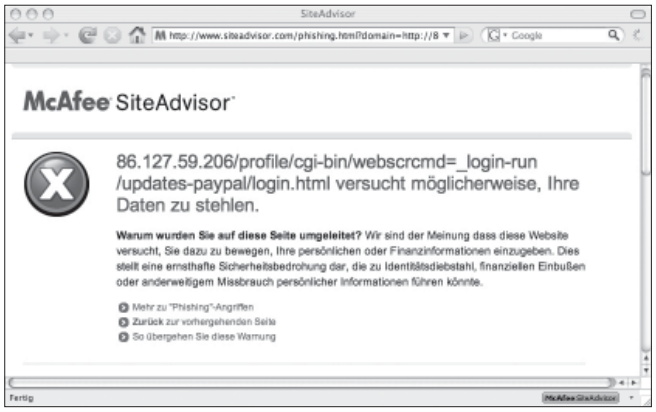

Abb. 5: SiteAdvisor-Warnung vor einer Phishing-Seite

Um die verwendeten Methoden vorzustellen, werden hier vier Anwendungen exemplarisch näher beleuchtet: Microsofts Phishing Filter, der Phishing Filter von Firefox, McAfee SiteAdvisor und WOT.

Microsoft Phishing Filter

In Internet Explorer 7, der bei Windows Vista mitgeliefert wird und auch auf Windows XP ab Service Pack 2 installiert werden kann, ist der Microsoft Phishing Filter bereits enthalten, muss jedoch erst eingeschaltet werden.[9)] Als Kompromiss zwischen Aktualität der Datenbasis und Wahrung der Privatsphäre kombiniert der Filter lokale Listen (sowohl von bekannten „guten" als auch von bekannten „bösen" Websites) und heuristische Seitenanalysen im PC des Anwenders mit einer Online-Abfrage bei den verbleibenden Zweifelsfällen. Eine ganz ähnliche Funktionalität bietet Microsofts *Windows Live Toolbar*.[10)] Diverse von Microsoft in Auftrag gegebene Studien bescheinigen dem Filter hervorragende Trefferraten.[11)]

Woher Microsoft allerdings die Informationen über die Phishing-Seiten bezieht, geht aus der Dokumentation[12)] nicht klar hervor. Naheliegend wäre, bekannte Meldestellen (`www.apwg.org`, `www.phishtank.com` etc.), Microsofts eigene Suchmaschine sowie URLs aus eMails heranzuziehen, die sich in Microsofts Spamfilter bzw. bei Hotmail verfangen haben. Offenbar werden diese Seiten mittels heuristischer Analyse selektiert und zu einer Liste verdächtiger Seiten zusammengestellt. Die weitere Beurteilung erfolgt quasi per Volksabstimmung: Über ein Menü kann jeder Anwender seine Meinung darüber abgeben, ob die dargestellte Seite seiner Meinung nach legitim ist oder nicht. Ob auch eine professionelle Beurteilung seitens Microsoft erfolgt, erschließt sich nicht.

Leider verständigt Microsoft die Betreiber der Sites, die eine Phishing-Seite enthalten, nicht. Damit nicht genug: Die einzige Möglichkeit nachzusehen, ob z.B. die eigenen Seiten als Phishing-Seiten gelistet sind, besteht über den Internet Explorer oder die Windows Live Toolbar. Dasselbe gilt, wenn man mit Microsoft in Kontakt treten will, um Einwände gegen ein irrtümliches Listing zu erheben oder zu melden, dass die Phishing-Seiten entfernt wurden. Damit sind Personen, die kein Betriebssystem von Microsoft verwenden, vom gesamten Verfahren ausgeschlossen. Leider deutet auch nichts auf eine Zusammenarbeit bzw. einen Abgleich mit bereits etablierten Verzeichnissen und Organisationen hin. Wie Google hat auch Microsoft eine immense Chance vertan, wirklich zur Sicherheit im Internet beizutragen.

Firefox Phishing Filter

Ähnlich Microsofts Phishing Filter hat auch Firefox ab Version 2 einen Schutz vor Phishing-Seiten eingebaut (siehe **Abb. 4**). Dieser ist standardmäßig aktiviert und greift nur auf eine lokale Datenbank zu, sodass die Privatsphäre des Anwenders gewahrt bleibt. Um bessere Ergebnisse zu erzielen, wird jedoch empfohlen, die Konfiguration derart zu ändern, dass der URL jeder aufzurufenden Seite online bei Google geprüft wird. Dieser Rat ist schwer nachzuvollziehen: Da die lokale Datenbank laut Dokumentation ohnehin alle 30 bis 60 Minuten aktualisiert wird und es viel länger dauert, bis eine Phishing-Seite gemeldet und überprüft wurde, ist der Zeitgewinn vernachlässigbar. Wenn man bedenkt, dass Firefox bei jeder Online-Abfrage den gesamten URL inklusive allfälliger Parameter übermittelt, wiegt der Verlust an Privatsphäre wohl deutlich schwerer.

Firefox benutzt die Datenbestände von Google, um zu entscheiden, welche Seiten gut und welche böse sind. Daher gilt für seine Zuverlässigkeit das bereits weiter oben über Google und StopBadware Gesagte. Ebenso wie Internet Explorer bietet auch Firefox ein in den Browser integriertes Menü, um Phishing-Seiten zu melden.

In der nächsten Firefox-Version soll der Schutz auch sonstige Malware umfassen. Die zu Redaktionsschluss jüngste Entwicklerversion (Gran Paradiso Alpha 8) hat in einem kurzen Test aber keinerlei Erfolg gezeigt – hier muss man sich wohl noch etwas in Geduld fassen.

McAfee SiteAdvisor

SiteAdvisor ist als kostenloses Plugin für Internet Explorer und Firefox erhältlich. Das Plugin vergleicht die Domainnamen der im Browser aufgerufenen Seiten mit der Datenbank von McAfee und zeigt im Fall eines Treffers eine deutliche Warnung an (siehe **Abb. 5**).

Entscheidend ist naturgemäß die Qualität der abgefragten Datenbank. Hier haben sich die Entwickler – übrigens keine Mitarbeiter von McAfee, sondern frisch gebackene Absolventen des *Massachusetts Institute of Technology* (MIT) – etwas einfallen lassen: So wie es auch die Suchmaschinen tun, lassen sie die Webseiten im World Wide Web automatisch abgrasen und laden die gefundenen Seiten und Dateien in simulierte (virtuelle) PCs. SiteAdvisor schaut quasi mit der Röntgenkamera in diese PCs hinein, und wenn bestimmte Veränderungen am System oder Programm-Merkmale erkannt werden, die für Malware typisch sind, wird die betreffende Website als „böse" markiert.[13)]

So einleuchtend das Konzept klingen mag – in der Praxis erfüllt SiteAdvisor die Erwartungen leider doch nicht. Das konnten wir am eigenen Leib (genauer: an der eigenen Domain) spüren, als `univie.ac.at` als gefährlich eingestuft wurde.

Das Offensichtliche zuerst: Es reicht nicht, lediglich den Domainnamen als Kriterium für die Gefährlichkeit einer Webseite heranzuziehen. Am Beispiel der Universität Wien zeigt sich, dass es völlig überzogen und für den Anwender gar nicht hilfreich ist, alle Webseiten einer Domain über einen Kamm zu scheren und als „böse" zu markieren – selbst wenn sich vielleicht irgendwo in den Tiefen dieses Webspace eine Malware eingeschlichen haben sollte. Um nützlich zu sein, müsste SiteAdvisor einzelne Seiten oder wenigstens Verzeichnisbäume bewerten. Kaum tröstlich, aber doch ein positiver Aspekt: McAfee erfährt nicht, welche Seiten genau vom Anwender aufgerufen wurden, sondern nur deren Domainnamen.

Immerhin kann man bei SiteAdvisor leicht online nachvollziehen, wie eine Bewertung zustande gekommen ist. Hierbei staunten wir nicht schlecht, als wir feststellen mussten, dass Dateien auf unserem FTP-Server (der mit dem Webserver nichts zu tun hat) für McAfees Warnung vor unserer Domain verantwortlich waren.[14)]

Noch größere Augen bekamen wir dann, als wir sahen, warum der FTP-Server der Uni Wien in Verruf geraten war: Ganze zwei Dateien aus der umfassenden und immerhin seit 1995 existierenden Softwaresammlung WinSite, die wir dort als Kopie für unsere User zur Verfügung stellten,[15)] waren vom Automatismus als „böse" eingestuft worden. Der letzte Download, den SiteAdvisor von unserem FTP-Server gemacht hatte, lag allerdings bereits ein Jahr zurück – die Grundlage für das ohnehin höchst zweifelhafte Urteil von SiteAdvisor war also hoffnungslos veraltet.

Noch ein Minus: Selbst die Entwickler solcher automatisierter Tests sind der Meinung, dass diese nicht immer funktionieren, sondern in manchen Fällen ein Mensch zwischen „gut" und „böse" entscheiden muss.[16)] In unserem Beispiel ist die Exaktheit wohl dem Rechenstift zum Opfer gefallen – unsere Bitte an McAfee, die unsinnige Bewertung unserer Domain und die der ebenfalls betroffenen TU Wien zu korrigieren, wurde höflich aber abschlägig beantwortet, mit der Begründung, dass die gesamte Überprüfung automatisiert und daher nicht beeinflussbar sei.

Schließlich bleibt noch zu erwähnen, dass auch McAfee das, was den meisten Nutzen für die Anwender brächte, nicht tut: nämlich die Sitebetreiber von dem (vermeintlichen) Problem in Kenntnis setzen.

Wenn McAfee, einer der traditionsreichsten Hersteller von Antivirus-Produkten, einen in den Browser integrierten Schutz vor „bösen Seiten" herausbringt, kann man ein seriöses Produkt erwarten. Mit dieser halbgaren Bastellösung, so interessant und vielversprechend die technischen Ansätze auch sind, hat sich McAfee aber nicht mit Ruhm bekleckert.

WOT

Wie SiteAdvisor ist WOT ein von frisch gebackenen – diesmal finnischen – Studienabsolventen entwickeltes Bewertungsservice, das sich gegenwärtig jedoch nur mit Firefox nutzen lässt. Auch WOT differenziert nicht die einzelnen Seiten einer Website, sondern gleicht nur den Domainnamen mit einer Datenbank ab.

Das Besondere an WOT ist, dass nicht einfach zwischen „gut" und „böse" unterschieden wird, sondern neben einer Gesamtwertung drei verschiedene Gesichtspunkte beurteilt werden: Vertrauenswürdigkeit als Geschäftspartner, Umgang mit der Privatsphäre und „Kindersicherheit" nach US-amerikanischen Wertmaßstäben (siehe **Abb. 6**).

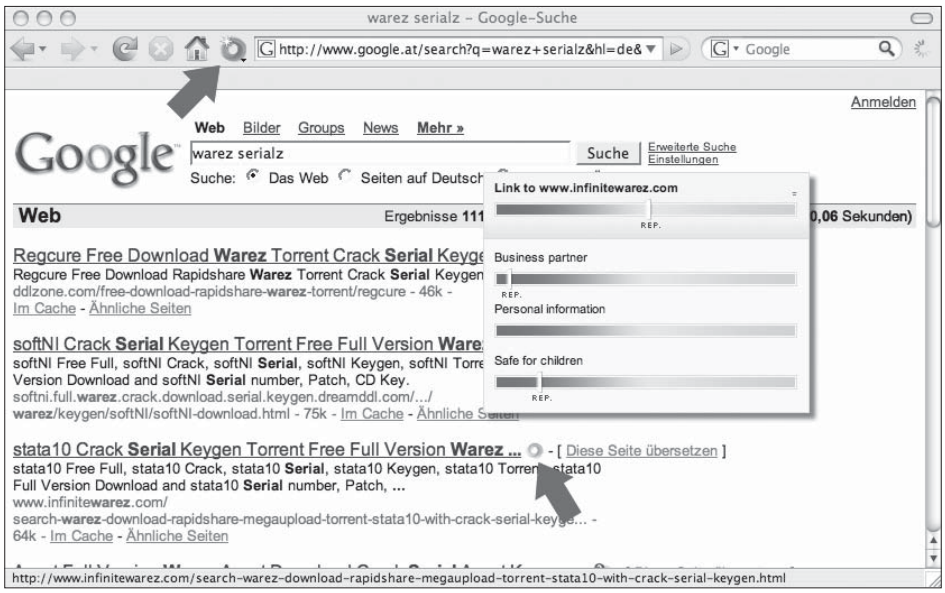

Abb. 6: WOT teilt Seiten nicht nur in „gut" oder „böse" ein, sondern bietet eine differenzierte Beurteilung.

Ganz im Gegensatz zu SiteAdvisor beruht die Beurteilung von Websites hier überhaupt nicht auf technischen Kriterien, sondern ergibt sich vielmehr aus den Bewertungen der WOT-Benutzerschaft. Um speziell bei neuen Seiten (wie es z.B. Phishing-Seiten regelmäßig sind) schnell eine Bewertung anbieten zu können, bezieht WOT auch Informationen von über hundert weiteren Systemen mit ein, beispielsweise vom Phishingseiten-Verzeichnis `phishtank.com`.

Dieser basisdemokratische Ansatz ruft natürlich gerade bei Frage-

stellungen, bei denen Sicherheitsspezialisten gefordert sind, einige Skepsis hervor. Erstaunlicherweise scheint das System aber gar nicht schlecht zu funktionieren, jedenfalls sind im – freilich nicht repräsentativen – Test keine groben Schnitzer aufgefallen. Auch die subjektive Zufriedenheit der Anwender im WOT-Forum scheint recht groß zu sein, gerade im Vergleich zu SiteAdvisor.

Fazit

Obwohl einige der Ansätze, die derzeit verfolgt werden, um den Anwender vor „bösen" Webseiten zu schützen, durchaus vielversprechend scheinen, sind derartigen Werkzeugen einige grundlegende Grenzen gesetzt:

- Eine Schwierigkeit liegt darin, die **Zielsetzung** genau zu definieren. Wenn in diesem Artikel durchgehend die moralinsauer anmutenden Begriffe „gute Seiten" und „böse Seiten" verwendet wurden, dann deshalb, weil es unzählige mögliche Definitionen dafür gibt: Mit diffusen Begriffen kann die Informationstechnologie traditionell sehr schlecht umgehen. Ein Ausweg könnte darin bestehen, den mündigen Anwender im Einzelfall genau und verständlich darüber zu informieren, welche Arten von Gefahren oder Unannehmlichkeiten es gibt, und ihn wählen zu lassen, welche von ihm ferngehalten werden sollen.

- Ein gravierenderes Problem ist das der **Menge**. Derzeit ist nicht absehbar, dass vollautomatische Systeme jemals eine brauchbare Klassifizierung zuwege bringen werden. Eine manuelle Prüfung erfordert aber einen ungeheuren Personaleinsatz, der nur für ein eher enges Anwendungsgebiet – etwa Phishing-Seiten – bezahlbar erscheint. Es muss deshalb damit gerechnet werden, dass alle diese Systeme noch länger ein Problem mit der Treffsicherheit haben werden.

- Eine weitere Komplikation entsteht durch die Möglichkeit, Webseiten **dynamisch** umzugestalten. Bereits jetzt gibt es zahlreiche Webseiten, die sich z.B. den Google-Robots anders präsentieren als dem normalen Anwender. Warum sollten „böse Seiten" nicht ebenfalls eine harmlose Variante vorhalten, die sie den Malware-Fahndern zeigen? Im einfachsten Fall reicht es bereits, ein durch einen Computer nur sehr schwer lösbares Bildrätsel – z.B. ein so genanntes *Captcha*[17] – vor die eigentliche Malware zu setzen, damit diese nicht von Automaten entdeckt werden kann.

- Eine besondere Gefahr ergibt sich aus dem **falschen Sicherheitsgefühl**: Wer sich auf den Ratschlag eines Webseiten-Gutachters verlässt und dabei nicht bedenkt, dass auch dieser nur einen Teil der „bösen" Seiten erkennen kann, gerät möglicherweise in Versuchung, die anderen Sicherheitsmaßnahmen zu vernachlässigen – und fällt den unerkannten Bösewichten dann völlig wehrlos zum Opfer.

- Das Gegenstück zur unerkannten Gefahr ist der **falsche Alarm**. Geschieht dies zu häufig, werden die Anwender (zu Recht) das Vertrauen in das System verlieren und es umgehen. Damit ist die Schutzwirkung dahin.

- Bei den derzeit wohl aussichtsreichsten Kandidaten für gute Schutzsysteme, den Browser-Plugins, sind auch die möglichen **Nebenwirkungen** zu bedenken. Schließlich handelt es sich um Software, die obendrein noch mit anderer Software zusammenarbeiten muss, was das Gesamtsystem noch komplexer macht. Erhöhte Komplexität führt in der Datenverarbeitung traditionellerweise zu erhöhter Fehleranfälligkeit und zu mehr Sicherheitslücken.

- Selbstverständlich ist davon auszugehen, dass alle diese Schutztechnologien auch das Interesse verschiedener **(para)staatlicher Organe** wecken. Diese könnten auf die Idee kommen, ihrer Meinung nach schädliche Inhalte – anfangs z.B. Informationen zur Herstellung von Sprengstoffen – zu unterdrücken. Eine andere Möglichkeit wäre, natürlich nur im begründeten Einzelfall (erst bei Terrorismus und Kinderpornographie, später wohl auch bei illegalem Filesharing), auf die Protokolle der Filter-Datenbanken und damit auf das Surfverhalten des Anwenders zuzugreifen.

Den Anstrengungen, die Anwender zuverlässig vor „bösen Webseiten" zu schützen, weht ein rauer Wind entgegen. Dennoch ist es wichtig, alle verfügbaren Mittel in dieser Richtung auszuschöpfen. Dabei darf auch keinesfalls vergessen werden, dass „böse" Webseiten nur teilweise ein technisches Problem sind. Beispielsweise müssen auch die rechtlichen Rahmenbedingungen geschaffen werden, um mittels Computer verübte Verbrechen international verfolgen zu können. Weiters müssen die Netzbetreiber die logistischen und vertraglichen Voraussetzungen schaffen, um missbräuchlich verwendete Rechner, die sich in ihrem Einflussbereich befinden, rasch aus dem Verkehr ziehen und sanieren zu können.

Die Industrie hat ganz offensichtlich den Bedarf erkannt, das Websurfen sicherer zu gestalten. Die bisher vorliegenden Ergebnisse sind unbefriedigend und noch zu sehr im Bastelstadium, um guten Gewissens empfohlen werden zu können. Man kann gespannt und hoffnungsvoll sein, was die Zukunft bringt.

Alexander Talos

14) Pikanterweise hat SiteAdvisor den FTP-Server nicht auf seine *Rote Liste* gesetzt, wohl aber `www.univie.ac.at` und `univie.ac.at`.

15) siehe Artikel *Softwarearchive auf dem FTP-Server der Universität Wien* in *Comment 97/1*, Seite 29 bzw. unter `http://comment.univie.ac.at/97-1/29/`

16) siehe `www.securityfocus.com/news/11376`

17) siehe `http://de.wikipedia.org/wiki/Captcha`