Web und Kommunikation

Schulungsunterlage
Berufsreifeprüfung

VOLKS
HOCH
SCHULE
GÖTZIS

1. Was ist das Internet?

Das Internet (wörtlich etwa „Zwischennetz“ oder „Verbundnetz“, von engl.: interconnected Networks: „untereinander verbundene Netzwerke“) ist ein weltweites Netzwerk bestehend aus vielen Rechnernetzwerken, durch das Daten ausgetauscht werden. Es ermöglicht die Nutzung von Internetdiensten wie E-Mail, Telnet, Usenet, Dateiübertragung, WWW und in letzter Zeit zunehmend auch Telefonie, Radio und Fernsehen. Im Prinzip kann dabei jeder Rechner weltweit mit jedem anderen Rechner verbunden werden. Der Datenaustausch zwischen den einzelnen Internet-Rechnern erfolgt über die technisch normierten Internetprotokolle. Die Technik des Internet wird durch die RFCs der IETF (Internet Engineering Task Force) beschrieben. Umgangssprachlich wird „Internet“ häufig synonym zum World Wide Web verwendet, da dieses einer der meistgenutzten Internetdienste ist, und im wesentlichen zum Wachstum und der Popularität des Mediums beigetragen hat.

2. Das WWW - World Wide Web

Das World Wide Web (kurz Web, WWW oder deutsch: Weltweites Netz; wörtlich: web „Gewebe, Netz“) ist ein über das Internet abrufbares Hypertext-System. Es wurde am 30. April 1993 weltweit zur allgemeinen Benutzung freigegeben.
Hierzu benötigt man einen Webbrowser, um die Daten vom Webserver zu holen und zum Beispiel auf dem Bildschirm anzuzeigen. Der Benutzer kann den Hyperlinks im Dokument folgen, die auf andere Dokumente verweisen, gleichgültig ob sie auf demselben Webserver oder einem anderen gespeichert sind. Hierdurch ergibt sich ein weltweites Netz (oder Gewebe) aus Webseiten. Das Verfolgen der Hyperlinks wird oft als Internetsurfen bezeichnet.
Das WWW wird im allgemeinen Sprachgebrauch oft mit dem Internet gleichgesetzt, obwohl es jünger ist und nur eine mögliche Nutzung des Internets darstellt (so wie wiederum das Internet nur einer von verschiedenen möglichen Serververbünden ist). Es gibt durchaus Internet-Dienste, die nicht in das WWW integriert sind (am bekanntesten ist E-Mail, aber z. B. auch IRC und Telnet). Zu dieser Verwirrung haben nicht zuletzt die Webbrowser beigetragen, die nicht nur das eigentliche HTTP-Protokoll (siehe unten) benutzen können, sondern dem Nutzer auch noch andere Dienste wie Mail und FTP zugänglich machen.

2.1 Kernstandards des WWW

- ***HTTP als Protokoll, mit dem der Browser Informationen vom Webserver anfordern kann.***
- ***HTML als Dokumentenbeschreibungssprache, die festlegt, wie die Information gegliedert ist und wie die Dokumente verknüpft sind (Hyperlinks).***
- ***URLs als eindeutige Adresse bzw. Bezeichnung einer Ressource (z. B. einer Webseite), die in Hyperlinks verwendet wird.***

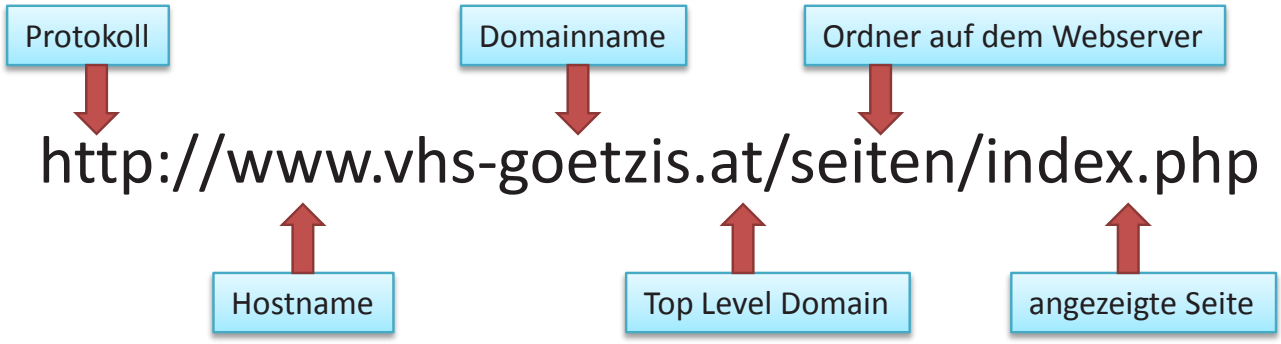
2.2 URL

Als Uniform Resource Locator (URL, dt. „einheitlicher Quellenanzeiger“) bezeichnet man eine Unterart von Uniform Resource Identifiern (URIs). URLs identifizieren und lokalisieren eine Ressource über das verwendete Netzwerkprotokoll (beispielsweise http oder ftp) und den Ort (engl. location) der Ressource in Computernetzwerken.

Da URLs die erste und häufigste Art von URIs darstellen, werden die Begriffe häufig synonym verwendet.

In der Umgangssprache wird URL häufig als Synonym für Internetadresse verwendet.
Die URL zur VHS Götzis ist beispielsweise http://www.vhs-goetzis.at/seiten/index.php.
Der Aufbau der URL im Detail:

2.3 ISP oder Internetdienstanbieter



Internetdienst(e)anbieter oder Internetdienstleister (engl.: Internet Service Provider, abgekürzt ISP), im deutschsprachigen Raum auch oft nur Provider, weniger häufig auch nur Internetanbieter oder Internetprovider genannt, sind Anbieter von Diensten, Inhalten oder technischen Leistungen, die für die Nutzung oder den Betrieb von Inhalten und Diensten im Internet erforderlich sind. Die in Österreich bekanntesten sind AON, CHELLO und in Vorarlberg TELEPORT und UPC. Der Zugang ist kostenpflichtig

2.4 Webbrowser

Webbrowser, oder allgemein auch Browser (engl., deutsche Aussprache [brauza]) genannt, für „Durchstöberer", „Blätterer" sind spezielle Computerprogramme zum Betrachten von Webseiten im World Wide Web. Das Durchstöbern des World Wide Webs beziehungsweise das aufeinanderfolgende Abrufen beliebiger Hyperlinks als Verbindung zwischen Webseiten mit Hilfe solch eines Programms wird auch als Internetsurfen bezeichnet. Neben HTML-Seiten können sie verschiedene andere Arten von Dokumenten anzeigen. Webbrowser stellen die Benutzeroberfläche für Webanwendungen dar. Die verbreitetsten sind **Internet Explorer, Chrome, Firefox** und **Safari.**

2.4.1 Cookies

Cookies sind kleine Textdateien, die Websites auf Ihrem Computer ablegen, um Informationen zu Ihnen und Ihren Präferenzen zu speichern. Cookies werden zur Personalisierung von Websites und zum Sammeln von Informationen über die Verwendung von Websites eingesetzt. Auf vielen Websites werden in Cookies Informationen gespeichert, um die Konsistenz zwischen verschiedenen Abschnitten der Site zu ermöglichen, z.B. bei einem Einkaufswagen oder personalisierten Seiten. Auf einer vertrauenswürdigen Website können Cookies die Nutzungsmöglichkeiten verbessern, da sich die Site dadurch Ihre Voreinstellungen merken kann oder Sie sich nicht jedes Mal neu anmelden müssen. Manche Cookies, etwa die von Werbebannern gespeicherten, gefährden jedoch Ihre Privatsphäre, indem sie die von Ihnen besuchten Sites nachverfolgen.

2.5 Suchmaschinen

Eine Suchmaschine ist ein Programm zur Recherche von Dokumenten, die in einem Computer oder einem Computernetzwerk wie z. B. dem World Wide Web gespeichert sind. Internet-Suchmaschinen haben ihren Ursprung in Information-Retrieval-Systemen. Sie erstellen einen Schlüsselwort-Index für die Dokumentbasis, um Suchanfragen über Schlüsselwörter mit einer nach Relevanz geordneten Trefferliste zu beantworten. Nach Eingabe eines Suchbegriffs liefert eine Suchmaschine eine Liste von Verweisen auf möglicherweise relevante Dokumente, meistens dargestellt mit Titel und einem kurzen Auszug des jeweiligen Dokuments. Dabei können verschiedene Suchverfahren Anwendung finden.

Die wesentlichen Bestandteile bzw. Aufgabenbereiche einer Suchmaschine sind:

- *Erstellung und Pflege eines Indexes (Datenstruktur mit Informationen über Dokumente),*
- *Verarbeiten von Suchanfragen (Finden und Ordnen von Ergebnissen) sowie*
- *Aufbereitung der Ergebnisse in einer möglichst sinnvollen Form.*

2.6 RSS Feed

RSS (Bedeutung siehe unten) ist ein Service auf Webseiten, der, ähnlich einem Nachrichtenticker, die Überschriften mit einem kurzen Textanriss und einen Link zur Originalseite enthält. Die Bereitstellung von Daten im RSS-Format bezeichnet man auch als RSS-Feed (engl. to feed – im Sinne von versorgen, einspeisen, zuführen). Er liefert dem Leser, wenn er einmal abonniert wurde, automatisch neue Einträge. Es handelt sich um ein Pull-Verfahren. Der Client sendet also in regelmäßigen Abständen Anfragen zur Aktualisierung des RSS-Feed an den Server.

2.6.1 Funktionsweise

Nachdem der RSS-Feed abonniert wurde, kann der Abonnent die Nachrichten im Feed-Reader einlesen. Der Abonnent des RSS-Feed kann dann direkt den angebotenen Links folgen und dort die vollständige Meldung lesen. Die Adresse eines RSS-Feed sieht der einer „normalen“ Webseite sehr ähnlich.

2.6.2 Lesen

Durch Eingabe der Adresse des Feeds im entsprechenden Feedreader wird dieser „abonniert“. Neu veröffentlichte Inhalte werden dann vom Feedreader selbsttätig in regelmäßigen, vom Empfänger festgelegten Abständen auf die Endgeräte – PCs oder auch Mobiltelefone – der Abonnenten geladen.
Zum Lesen eines RSS-Feeds dienen herkömmliche Webbrowser oder spezielle Programme, die auf die Ähnlichkeit zum Nachrichtenticker angepasst sind. Letztere nennt man (synonym) RSS-Aggregatoren, RSS-Reader oder Feedreader. Auch einige aktuelle E-Mail-Programme bieten bereits RSS-Lesefunktionen, ältere können durch Plugins erweitert werden. Daneben gibt es auch Anwendungen wie Bildschirmschoner.
Im Unterschied zur Benachrichtigung per E-Mail geht die Initiative bei RSS vom Empfänger aus, der den Feed abonniert hat. Das bedeutet, dass der Anbieter die Leser nicht auswählen kann, sich im Gegenzug aber auch nicht um eine Verwaltung des Leserstammes (zum Beispiel mit einer Mailinglisten-Software) kümmern muss. Der Leser muss nicht offenlegen, dass er die Quelle beobachtet und kann Quellen wesentlich leichter abonnieren bzw. das Abonnement widerrufen, indem er einfach die Einstellung in seinem RSS-Aggregator vornimmt.

2.6.3 Verwendung

RSS wird verwendet, um Artikel einer Website oder deren Kurzbeschreibungen (insbesondere Nachrichtenmeldungen) zu speichern und in maschinenlesbarer Form bereitzustellen. Ein sogenannter RSS-Feed oder Newsfeed (engl. etwa Nachrichteneinspeisung) besteht aus einer XML-Datei, die den reinen strukturierten Inhalt – beispielsweise einer Nachrichtenseite – bereithält, aber keinerlei Layout, keine Navigation oder sonstige Zusatzinformationen beinhaltet. Zahlreiche Webangebote, die regelmäßig Artikel publizieren, stellen eine automatisch generierte RSS-Datei mit den neuesten Artikeln zur Verfügung.

2.7 Podcasting

Podcasting bezeichnet das Produzieren und Anbieten von Mediendateien (Audio oder Video) über das Internet. Das Kofferwort setzt sich aus den beiden Wörtern iPod und Broadcasting zusammen. Ein einzelner Podcast (deutsch: ein Hörstück, genauer Hördatei oder Bewegtbilddatei) ist somit eine Serie von Medienbeiträgen (Episoden), die über einen Feed (meistens RSS) automatisch bezogen werden können.
Man kann Podcasts als Radio- oder Fernsehsendungen auffassen, die sich unabhängig von Sendezeiten konsumieren lassen. Podcasting wäre so als Teilbereich von Video/Audio-on-Demand (Video/Audio auf Abruf) zu betrachten.

3. Sicherheit

Von der privaten Nutzung des Internets und E-Mails über gewerbliche Anwender jeglicher Art bis hin zum Einsatz von IT in kritischen Infrastrukturen wie Energie- oder Gesundheitsversorgung – das private, wirtschaftliche und öffentliche Leben ist heute ohne Computertechnologie kaum vorstellbar.
IT und damit auch Internet-Sicherheit ist indes nicht mehr allein ein technisches Problem: fast wöchentliche Meldungen über neu entdeckte Sicherheitslücken in Softwareprogrammen oder Viren und dadurch verursachte Schäden werfen zunehmend die Frage nach der rechtlichen Verantwortlichkeit der an der Herstellung und dem Einsatz von IT-Produkten Beteiligten auf, angefangen beim Hersteller, über die IT-Dienstleister, wie etwa die Provider (Host-, Access-Provider), bis hin zu den IT-Anwendern in Haushalten und Unternehmen.

3.1 Die wichtigsten Regeln

Nachstehend angeführte Regeln sind nur die wichtigsten Grundregeln. Wenn Sie diese aber beherzigen vermeiden Sie bereits 95 % der Probleme.

3.1.1 Schutzprogramme

Verschiedene Programme helfen, Schadprogramme zu identifizieren und zu beseitigen
- *zum Schutz vor Viren und Würmern: ein Virenscanner*
- *zum Schutz vor Trojaner, Spyware und Hijacker: Anti-Spyware- und Anti-Trojaner-Tools*
- *Mit einer Personal Firewall können Angriffe von außen (z.B. Wurm Blaster) wie von innen (z.B. durch Trojaner) blockiert werden.*

3.1.2 Sichere Internet-Programme

Wenn der PC sicher im Internet sein soll, dann müssen Emailprogramm, Browser und alle anderen Programme, die auf das Internet zugreifen, sicher eingestellt sein.

3.1.3 Regelmäßiges Updaten

Für das Betriebssystem, die Internet- und Schutzprogramme sollten regelmäßig und zeitnah die neuesten Sicherheitsupdates installiert werden. Virenscanner sollten mehrmals die Woche auf den neuesten Stand gebracht werden, was aber normalerweise ohnehin automatisch passiert.

3.1.4 Eingeschränkter Nutzer

Für das normale Arbeiten und insbesondere für die Nutzung von Internetprogrammen empfiehlt sich die Einrichtung eines eingeschränkten Nutzerkontos. Falls es doch einmal dazu kommt, dass ein Schadprogramm installiert wird, kann es dort weniger Schaden anrichten und ist leichter zu beseitigen. Für administrative Aufgaben kann ein separates Administratorkonto verwendet werden.

3.1.5 Lieber einmal zu viel vorsichtig als einmal zu wenig:

- *Unbekannte Dateien und Emailanhänge vor dem Öffnen nach Viren scannen.*
- *Bei Anfrage der Firewall unbekannten Programmen nicht einfach den Zugang zum Internet gewähren.*
- *Zum Schutz vor Spam nicht die Haupt-Emailadresse öffentlich angeben, für Registrierungen, Gästebucheinträge u.ä. eine Zweitadresse einrichten.*

3.2 Sichere Seiten

Für kritische Anwendungen wie Telebanking, Zahlungsvorgänge u. ä. werden sogenannte sichere Seiten verwendet. Sie erkennen sichere Seiten an 2 Merkmalen. Zum Einen sehen Sie in der Adressleiste http**s**://, wobei das s für SECURE steht 

, zum Anderen ist in der Statusleiste am unteren Bildschirmrand ein Schlossymbol  eingeblendet. Entscheidend ist dass das Schloss geschlossen ist. Die Datenübertragung bei sicheren Seiten erfolgt verschlüsselt.

3.3 Verschlüsselung

Verschlüsselung nennt man den Vorgang, bei dem ein klar lesbarer Text (Klartext) (oder auch Informationen anderer Art, wie Ton- oder Bildaufzeichnungen) mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine „unleserliche“, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird. Als entscheidend wichtige Parameter der Verschlüsselung werden hierbei ein oder auch mehrere Schlüssel verwendet. Daten werden verschlüsselt, um sie vor fremden Zugriff zu schützen. Die Verschlüsselung im Internet dient drei grundlegenden Zielen:

- *Schutz der Vertraulichkeit: Die Nachricht darf nur für den lesbar sein, für den sie bestimmt ist.*
- *Schutz der Authentizität: Die Echtheit des Absenders soll sichergestellt werden. Ist der Absender wirklich jene Person, die als Absender angegeben wird?*
- *Schutz der Integrität: Die Nachricht darf auf dem Weg vom Absender zum Empfänger keinesfalls verändert werden.*

3.4 Digitale Zertifikate

Ein digitales Zertifikat ordnet einen digitalen Schlüssel einer bestimmten Person oder Organisation zu.
Am besten lassen sich digitale Zertifikate als digitale Ausweise im Internet beschreiben. Sie bestätigen, dass eine bestimmte Person eine bestimmte Signatur (einen bestimmten privaten Schlüssel) benutzt. Diese digitalen Zertifikate werden von Zertifizierungsstellen ausgegeben, die eine Identitätsprüfung der Person durchführen und sicherstellen, dass der Signator den privaten Schlüssel auch korrekt verwenden. Digitale Zertifikate werden auch benützt um die Korrektheit einer Website zu bestätigen.

4. Sicherheitsbedrohungen

Gefahren lauern überall – auch im Internet. Wer seine Daten nicht schützt, macht es Feinden einfach, diese bei der Übertragung mitzulesen, zu verändern oder sogar zu löschen. Man hört immer öfter von neuen Viren oder Würmern – Programmen also, die sich selbständig verbreiten oder über E-Mails versandt werden und Schäden auf Ihrem PC anrichten können. Aber auch von Trojanischen Pferden ist oft die Rede. Das sind dann Programme, die vom Nutzer unbemerkt sicherheitskritische Funktionen durchführen, indem sie beispielsweise Passwörter abfangen.

4.1 Malware

Als Malware (Kofferwort aus engl. malicious, „bösartig“ und Software) oder Schadprogramm bezeichnet man Computerprogramme, welche vom Benutzer unerwünschte und ggf. schädliche Funktionen ausführen. Da ein Benutzer im Allgemeinen keine schädlichen Programme duldet, sind die Schadfunktionen gewöhnlich getarnt oder die Software läuft gänzlich unbemerkt im Hintergrund.

4.1.1 Viren

Viren können für Ihren PC manchmal genauso gefährlich sein wie für Sie ein Grippevirus. Viren im Computer funktionieren auch genauso wie Krankheitsviren. Sie zeichnen sich nämlich vor allem durch zwei Sachen aus: Sie können sich selbst verbreiten und richten überall – wo sie sind – Schaden an. Wenn Sie sich einen „harmloseren“ Virus eingefangen haben, gibt Ihr Computer vielleicht seltsame Texte aus, oft werden aber Dateien und auch schon mal die ganze Festplatte gelöscht. Mittlerweile wird die Anzahl an weltweit existierenden schädlichen Programmen auf über 150.000 geschätzt. Jeden Monat entstehen Hunderte neue. Diese haben bislang weltweit Kosten und Schäden in Milliardenhöhe verursacht. Allein in Österreich ist jährlich von einer dreistelligen Millionensumme auszugehen. Und das mit steigender Tendenz.
Sie stellen aber auch ein gravierendes Sicherheitsproblem dar, wenn vertrauliche Daten unbemerkt weitergeleitet oder Betriebsgeheimnisse ausspioniert werden.
Anstecken kann sich Ihr PC immer dann, wenn Sie Dateien aus dem Internet auf Ihren Rechner laden. Diese Verbreitungsweise macht inzwischen rund 95 % der Infektionen aus. In jeder ausführbaren Datei, wie zum Beispiel *.exe oder *.com, kann sich ein Virus verstecken. Auch Textdokumente vom Typ *.doc oder Tabellen vom Typ *.xls können virenverseucht sein.

4.1.2 Würmer

Die Infektion mit Viren des Typs Wurm erfolgt oftmals über E-Mail. Startet man eine angehängte Datei, wird der Virus aktiviert und verbreitet sich anschließend selbst weiter. Durch Sicherheitslücken in einigen E-Mail-Programmen können sich die Würmer besonders schnell verbreiten. Bei Outlook und Outlook Express von Microsoft ist es sogar möglich, die verseuchten E-Mails ohne Wissen des Benutzers an Personen aus dem Adressbuch zu versenden. Weil die Empfänger den Absender der E-Mail kennen, geraten sie in Versuchung, den Anhang zu öffnen und der Wurm pflanzt sich fort.
Im Gegensatz zu Viren und Trojanischen Pferden infizieren Würmer jedoch keinen fremden Code, um sich fortzupflanzen. Sie sind auf die selbstständige Verbreitung in Netzwerken ausgerichtet und stehlen lediglich Rechenzeit. Dadurch können sie aber innerhalb kürzester Zeit Hunderte PCs infizieren und diese lahm legen.

4.1.3 Trojanische Pferde

Das ursprüngliche Trojanische Pferd bestand aus Holz und war eine Kriegslist der Griechen gegen die Trojaner. Der Legende nach versteckten sich ein paar Griechen im Bau des Pferdes. Sie gelangten so nachts nach Troja, weil die Trojaner das Pferd in die Stadt holten, um es der Göttin Athene zu schenken – jedoch ohne die Gefahr im Innern des Pferdes zu ahnen. Einmal in Troja angekommen, eroberten Griechen alsbald die Stadt.
Die Computerversion des Trojanischen Pferdes funktioniert nach dem selben Prinzip. Ein scheinbar nützliches Programm hat ein anderes sozusagen im Bauch, das dann unbemerkt eindringt und sich auf dem PC installiert. So können beispielsweise Passwörter und andere vertrauliche Daten ausgespäht, verändert, gelöscht oder bei der nächsten Datenübertragung an den Angreifer verschickt werden. Dieser „Datendiebstahl“ bleibt in der Regel unbemerkt, weil im Gegensatz zum Diebstahl materieller Dinge nichts fehlt. Anders als Computer-Viren können sich Trojanische Pferde jedoch nicht selbständig verbreiten.
Mit der zunehmenden Zahl von Internetnutzern verbreiteten sich auch Trojanische Pferde. Es sind Hunderte von Programmen bekannt, die Zugangsdaten von Anwendern erfassen und über das Internet an den „Interessenten“ verschicken können.

4.1.4 Spyware

Spyware – das sind ungebetene Gäste auf Ihrem PC, die Sie und Ihre Surfgewohnheiten ohne Ihr Wissen ausspionieren. Spyware landet häufig durch Internetseiten auf Ihrer Festplatte, die „Aktive Inhalte“ enthalten. „Aktive Inhalte“ sind nicht sichtbare Funktionen von Webseiten die mit Unterstützung Ihres Browsers (z. B. Internet Explorer) auf Ihrem Rechner ausgeführt werden. Eigentlich sollen sie die besuchten Internetseiten anschaulicher darstellen. Es können aber auch ungewollte Aktionen auf Ihrem Rechner ausgeführt werden, wie beispielsweise das Installieren von unerwünschten Programmen oder das Auslesen von Benutzerdaten.

4.1.5 Pishing

Phishing werden Versuche genannt, über gefälschte WWW-Adressen an Daten eines Internet-Benutzers zu gelangen. Der Begriff ist ein englisches Kunstwort, das sich an fishing („Angeln“, „Fischen“) anlehnt. Häufig wird das h in dem Begriff mit Harvesting erklärt, so dass der Begriff Phishing dann Password harvesting fishing lautet. Typisch ist die Nachahmung des Designs einer vertrauenswürdigen Stelle.
Es handelt sich meist um kriminelle Handlungen, die Techniken des Social Engineering verwenden. Phisher geben sich als vertrauenswürdige Personen aus und versuchen, durch gefälschte elektronische Nachrichten an sensib-

le Daten wie Benutzernamen und Passwörter für Online-Banking oder Kreditkarteninformationen zu gelangen. Phishing-Nachrichten werden meist per E-Mail oder Instant-Messaging versandt und fordern den Empfänger auf, auf einer präparierten Webseite oder am Telefon geheime Zugangsdaten preiszugeben. Versuche, der wachsenden Anzahl an Phishing-Versuchen Herr zu werden, setzen unter anderem auf geänderte Rechtsprechung, Anwendertraining und technische Hilfsmittel.

4.1.6 SPAM

Der Name „Spam“ ist dem Dosenfleisch SPAM (Spiced Porc and Ham) der amerikanischen Firma Hormel Foods entliehen (deutsch: Frühstücksfleisch), den es seit 1937 gibt. Im Internetzeitalter ist er zum Synonym für Massen-E-Mails geworden.
Wie der Schinken zur Massen-E-Mail wurde, darüber gibt es viele Geschichten. Hormel Foods selbst sagt, es beruhe auf einem Sketch der Comedy-Gruppe „Monty Python“. Darin kam der Begriff über 120 mal innerhalb weniger Minuten vor und übertönte jede andere Konversation. Und tatsächlich liegt die Analogie zur Massen-E-Mail damit auf der Hand.
Als Spam, Spamming oder Junk Mail (Müllpost) bezeichnet man im Internet:

» ***Massenversand nichtangeforderter Werbe- E-Mails***
» ***Werbebeiträge in Newsgroups, die nichts mit dem Thema der Newsgroup zu tun haben.***
» ***Kettenbriefe***

4.2 Maßnahmen

An oberster Stelle steht die Installation einer guten Antivirussoftware. Diese muss natürlich auch regelmäßig aktualisiert werden. Das machen die Programme meist selbständig. Moderne Antivirussoftware kann viel mehr als nur Viren erkennen. Sie verhindert das Einnisten von Spyware, kann SPAM und Pishing - Attacken erkennen und schützt den Rechner durch Firewalls.

4.2.1 Antivirensoftware

Ständig aktualisierte Antivirensoftware ist insbesondere auf Windows PCs und Android Smartphones ein absolutes Muss. Windows bietet seit Version 7 eine eigene ins System inkludierte Software an, die das Eindringen und Ausführen von Schadcode verhindern soll, alternativ kann man sich aber auch auf Tools wie **Avira, Kaspersky, Avast** oder **Symantec, etc.** verlassen.

4.2.2 Firewall

Eine Firewall ist eine Netzkomponente(Soft- oder Hardware), die Netz-Zugriffe überwacht und einschränkt. Damit soll die Sicherheit, also der Schutz gegen unbefugte Zugriffe speziell von außen, unterbunden werden. Jeder der mit einer Standleitung im Internet surft sollte unbedingt eine Firewall installiert haben. Sollte Ihre Virenscannersoftware keinen Firewall enthalten, können Sie die Windows Firewall nutzen. Idealerweise sollte aber Ihre Antivirussoftware eine Firewall enthalten.

5. Schutz von Kindern und Jugendlichen

Wenn Minderjährige Zugang zu einem Rechner mit Internet haben, sollten Eltern besondere Vorsichtsmaßnehmen treffen. Denn nicht nur Unterhaltsames und nützliche Informationen warten im WWW auf Ihre Kinder: Gewalt, Pornografie oder extremistische Gruppierungen haben im Netz Hochkonjunktur.

5.1 Schutzprogramme

Es gibt ein breites Angebot an kostenpflichtigen Filtern, die individuelle Schutzeinstellungen erlauben. **Cybersitter** ist ein amerikanisches Programm, das mit englischen Begriffen arbeitet und sich an amerikanischen Wertvorstellungen orientiert. In heimischen Tests hat der Filter zufriedenstellende Urteile bekommen. **Net Nanny** ist ein ähnliches Programm, das zusätzlich die Kontrolle des Surfverhaltens ermöglicht. Außerdem sichert die virtuelle Nanny auch P2P-, FTP und Chat-Verbindungen. Einen zusätzlichen Schutz kann auch eine Kindersuchmaschinen bieten, die Sie im Browser vordefinieren können. Mit diesen Suchmaschinen werden Webseiten durchsucht, die speziell für Kinder und Jugendliche gemacht wurden, von Minderjährigen selbst stammen oder zwar für Erwachsene gemacht wurden, aber thematisch auch für Kinder unter zwölf Jahre interessant sind. Alle guten Kinder-Suchmaschinen verfügen über einen redaktionell erstellten Datenbestand. Besonders empfehlenswert sind etwa die **Blinde Kuh** oder **Trampeltier**.

5.2 Zugangsbeschränkungen

Es gibt spezielle Software die mehr als nur reine Schutzprogramme sind. Damit können Sie nicht nur unerwünschte Inhalte verbieten sondern auch die Zeiten der Nutzung beschränken. So können Sie z.B. pro Woche 5 Stunden erlauben. Sind diese aufgebraucht ist der Internetzugang gesperrt. Oder Sie sperren generell das Internet ab 21:00 Uhr. Denkbar ist fast jedes Szenario. Voraussetzung ist allerdings dass der jeweilige User sich am Rechner anmelden muss.

6. Soziale Netzwerke

In Sozialen Netzwerken präsentieren sich NutzerInnen in einem eigenen Profil mit möglichst vielen persönlichen Angaben, wie z.B. Hobbys, Interessen, Fotos, Videos etc. Wenn zwei InternetnutzerInnen einwilligen, „verlinken" sie ihre Profile. Dadurch entsteht ein Netzwerk von Personen, die miteinander in Kontakt stehen. In Sozialen Netzwerken kann man sich mit anderen austauschen, die ähnliche Interessen haben und nach neuen Kontakten suchen.

6.1 Wie nutze ich Soziale Netzwerke sicher?

Besonders der Schutz der Privatsphäre ist in Sozialen Netzwerken eine Herausforderung. Einerseits will man sich selbst präsentieren, um so auch von anderen TeilnehmerInnen gefunden zu werden, andererseits gilt es zu verhindern, dass persönliche Angaben missbraucht werden. Grundsätzlich gilt: Desto vorsichtiger Sie bei der Angabe von persönlichen Daten und Fotos sind, desto sicherer ist das Social Networking!

Die wichtigsten Sicherheitstipps:

- *Geben Sie keine persönlichen Daten (Adresse, Wohnort, Telefonnummer etc.) bekannt, die es Fremden ermöglichen, Sie auch im „echten" Leben aufzuspüren oder zu belästigen.*
- *Veröffentlichen Sie keine Bilder oder Texte, die Ihnen oder anderen später einmal peinlich sein oder aber zu Ihrem Nachteil verwendet werden könnten. Bedenken Sie, dass auch keine Bilder von Bekannten veröffentlicht werden dürfen, die diese „nachteilig" darstellen. Auch wenn Bilder nur für eine kleinere NutzerInnengruppe freigegeben sind, ist nicht auszuschließen, dass diese irgendwann in falsche Hände gelangen.*
- *Bedenken Sie, dass Soziale Netzwerke von potentiellen Arbeitgebern genutzt werden könnten, um mehr über Ihre Person zu erfahren.*
- *Nutzen Sie die Einstellungsoptionen Ihrer Community für mehr „Privatsphäre", indem Sie z.B. den Zugriff auf Freunde beschränken.*
- *Verwenden Sie sichere Passwörter und halten Sie diese geheim. Gestohlene Log-in-Daten können verwendet werden um Ihr Profil zu verändern oder zu missbrauchen. Nachdem oft diesselben Passwörter auch bei anderen Konten wie z.B. eBay oder Amazon benutzt werden, kann ein gestohlenes Passwort neben Mobbing auch handfeste finanzielle Folgen nach sich ziehen. Verwenden Sie deshalb verschiedene Passwörter für verschiedene Anwendungen und verändern Sie diese auch in regelmäßigen Abständen. Siehe auch: Wie sieht ein sicheres Passwort aus?*
- *Wenn Fremde Sie einladen, Sie als „FreundIn" zu verlinken, nehmen Sie diese Personen genau unter die Lupe, bevor Sie die Einladung annehmen.*
- *In manchen Communities kann es auch vorkommen, dass Schadprogramme verbreitet werden. Seien Sie daher vorsichtig, wenn Sie Programme erhalten. Speichen Sie diese nicht auf Ihrem Computer und verwenden Sie ein regelmäßig aktualisiertes Anti-Virus-Programm.*
- *Werden Sie von NutzerInnen der Community belästigt, so können Sie diese in der Regel sperren lassen. Kontaktieren Sie den Betreiber der Internetseite falls die unerwünschte Kontaktaufnahme nicht aufhört.*

6.2 Netiquette

Unter Netiquette oder Netikette (Kunstwort aus engl. net – Netz und etiquette – Etikette) versteht man das (gute) Benehmen in der virtuellen Kommunikation. Was im Netz als guter Umgang miteinander (noch) akzeptiert wird, ist sehr unterschiedlich und hängt von den Teilnehmern innerhalb des Kommunikationssystems ab. Bezogen auf E-Mail könnte Netiquette bedeuten, dass ein aussagekräftiger Betreff selbstverständlich sein sollte. Ebenso die Einhaltung der Rechtschreibregeln. Eine ordentliche Anrede und ein Gruß am Schluss gehört ebenfalls dazu.

7. Electronic Mail

Die (auch das) E-Mail (kurz Mail; von englisch: „electronic mail“; zu Deutsch: „die elektronische Post“ oder „der elektronische Brief“) bezeichnet eine auf elektronischem Weg in Computernetzwerken übertragene, briefartige Nachricht.

7.1 Aufbau einer E-Mail

Das Format einer E-Mail wird durch Normen festgelegt. Danach bestehen E-Mails nur aus Textzeichen. E-Mails sind intern in zwei Teile geteilt: Den Header mit Kopfzeilen und den Body mit dem eigentlichen Inhalt der Nachricht.

7.2 HTML

HTML-Mails werden teils ungewollt und unbewusst durch die Voreinstellung des E-Mail-Programms, insbesondere von Microsoft-Programmen, versandt, teils bewusst, um Schriftauszeichnungen verwenden zu können, etwa in E-Mail-Newslettern.
HTML-Mails stehen im Ruf, unsicherer als reine Text-Mails zu sein. Da die Vergangenheit gezeigt hat, dass das Rendering von HTML-Mails anfälliger für Sicherheitslücken ist als die Anzeige von Klartext, empfehlen auch heute noch viele EDV-Ratgeber und Softwarehersteller die HTML-Anzeige von E-Mails zumindest im Vorschaufenster des E-Mail-Programms zu deaktivieren, wenn nicht gar ganz auszuschließen.

7.3 Signature – die Unterschrift unter der E-Mail

Eine Unterschrift ist optional, sie ist gegebenenfalls Teil des Bodys. Die am häufigsten zu findende Unterschrift ist die sogenannte Signature, sie gibt nähere Erläuterung zum Absender, zum Beispiel dessen Klarnamen, Arbeitsstelle, persönliche Vorlieben und ähnliches. Sofern diese Unterschrift den Absender angibt, stellt sie eine elektronische Signatur im Sinne des Signaturgesetzes dar. Neben oder alternativ zu dieser „einfachen“ elektronischen Signatur kann eine E-Mail auch eine digitale Signatur enthalten, die Fälschungen oder Verfälschungen der E-Mail erkennbar macht. Unter bestimmten Voraussetzungen kann eine digitale Signatur rechtlich eine qualifizierte elektronische Signatur darstellen, und dann eine zur manuellen Unterschrift eines Briefes gleichwertige Rechtskraft besitzt.

7.4 Die E-Mail-Adresse

Eine E-Mail-Adresse ist die Angabe, welche den Empfänger einer E-Mail eindeutig bezeichnet und damit eine Zustellung an diesen Empfänger ermöglicht. Eine E-Mail-Adresse, wie sie für den Transport per SMTP im Internet verwendet wird, besteht aus zwei Teilen: Einem lokalen Teil, im Englischen local-part genannt, und einem globalen Teil, im Englischen domain-part genannt. Beide Teile werden durch das „@“ (At-Zeichen) verbunden. Bei der E-Mail-Adresse info@vhs-goetzis.at ist vhs-goetzis.at der domain-part, info der local-part.

7.5 CC: Carbon Copy, der (Kohlepapier-) Durchschlag

Beim Schreiben einer E-Mail wird dieses Feld verwendet, um Kopien an einen oder mehrere Empfänger zu senden. Mit einem Eintrag in diesem Feld wird gleichzeitig symbolisiert, dass diese E-Mail sich nicht direkt an

diesen Benutzer wendet, sondern lediglich „zur Beachtung“ bzw. „zur Kenntnisnahme“ an ihn versendet wurde. Die Einträge im CC-Feld werden (im Gegensatz zum BCC-Feld) bei allen Empfängern angezeigt und sind somit bekannt.

7.6 BCC: Blind Carbon Copy, die Blindkopie

Das BCC-Feld enthält eine oder mehrere durch Kommas getrennte E-Mail-Adressen, an die eine Kopie der E-Mail gesendet wird, ohne dass dies jedoch für die anderen angegebenen Empfänger sichtbar ist („Blindkopie“). Durch eine Blindkopie sind die Empfänger von Rund-Mails vor der Adressen-Sammlung von bösartigen Diensten wie z. B. Spambots gesichert.

7.7 Dateianhänge

Ein Dateianhang (engl. attachment) ist eine Datei, welche im Body einer E-Mail verschickt wird. Dies wird durch das MIME-Protokoll ermöglicht, welches die Unterteilung des Bodys und die Kodierung der Datei regelt. Dateianhänge können Computerviren beinhalten, daher sollte sorgsam mit ihnen umgegangen werden. Die Größe eines Attachments ist zwar prinzipiell nicht begrenzt, wird aber in der Realität durch Größenbeschränkungen für die gesamte E-Mail sowie für das Postfach des Empfängers limitiert.

8. SMS und MMS

Short Message Service (engl. für „Kurznachrichtendienst“, Abk. SMS) ist ein Telekommunikationsdienst zur Übertragung von Textnachrichten an andere mobile Endgeräte oder an normale E-Mail-Adressen. Er wurde zuerst für den GSM-Mobilfunk entwickelt und ist nun in verschiedenen Ländern auch im Festnetz als Festnetz-SMS verfügbar.

Der Multimedia Messaging Service (MMS) ist als Weiterentwicklung von SMS (Short Message Service) und EMS (Enhanced Message Service) anzusehen und bietet die Möglichkeit, mit einem Mobiltelefon multimediale Nachrichten an andere mobile Endgeräte oder an normale E-Mail-Adressen zu schicken. Als MMS-Postkarte kann seit 2003 auch ein gedrucktes Endprodukt über die Briefpost versendet werden. MMS wird von 3GPP und OMA standardisiert.

9. Voice over IP

Unter der IP-Telefonie, eine Kurzform für die Internet-Protokoll-Telefonie. auch Internet-Telefonie oder Voice over IP (kurz VoIP) genannt, versteht man das Telefonieren über Computernetzwerke, welche nach Internet-Standards aufgebaut sind. Bei den Gesprächsteilnehmern können sowohl Computer, auf IP-Telefonie spezialisierte Telefonendgeräte, als auch über spezielle Adapter angeschlossene klassische Telefone die Verbindung herstellen. Ist eine Webcam vorhanden können sich die Teilnehmer auch sehen. Der bekannteste Anbieter ist Skype.

10. Instant Messaging

Instant Messaging (kurz IM) (englisch für „sofortige Nachrichtenübermittlung“) oder Nachrichtensofortversand ist eine Kommunikationsmethode, bei der sich zwei oder mehr Teilnehmer per Textnachrichten unterhalten (genannt chatten). Die Teilnehmer müssen dazu mit einem Computerprogramm (genannt Client) über ein Netzwerk wie das Internet direkt oder über einen Server miteinander verbunden sein. Viele Clients unterstützen zusätzlich die Übertragung von Dateien und Audio- und Video-Streams. Benutzer können sich gegenseitig in ihrer Kontaktliste führen und sehen dann an der Präsenzinformation, ob der andere zu einem Gespräch bereit ist. Verbreitete Instant Messaging Programme sind Facebook Chat und Whatsapp auf Smart Phones.

11. Social Networks

Soziale Netzwerke stehen umgangssprachlich für eine Form von Netzgemeinschaften, welche technisch durch Web 2.0 Anwendungen oder Portale beherbergt werden. Im Englischen existiert der präzisere Begriff des social network service. Die deutschen Begriffe „Gemeinschaftsportal“ oder „Online-Kontaktnetzwerk“ sind eher weniger gebräuchlich.

11.1 Typische Funktionen

Die Webportale bieten ihren Nutzern üblicherweise folgende Funktionen an:

- *Persönliches Profil, mit diversen Sichtbarkeitseinstellungen für Mitglieder der Netzgemeinschaft oder generell der Öffentlichkeit des Netzes*
- *Kontaktliste oder Adressbuch, samt Funktionen, mit denen die Verweise auf diese anderen Mitglieder der Netzgemeinschaft (etwa Freunde, Bekannte, Kollegen usw.) verwaltet werden können*
- *Empfang und Versand von Nachrichten an andere Mitglieder (einzeln, an alle usw.)*
- *Empfang und Versand von Benachrichtigungen über diverse Ereignisse (Profiländerungen, eingestellte Bilder, Videos, Kritiken, Anklopfen usw.)*
- *Blogs*

12. Internetforen

Ein Internetforum, auch Diskussionsforum, ist ein virtueller Platz zum Austausch und Archivierung von Gedanken, Meinungen und Erfahrungen. Die Kommunikation findet dabei asynchron, das heißt nicht in Echtzeit, statt. Englische Bezeichnungen dafür sind internet forum und webboard.
Üblicherweise besitzt ein Internetforum ein bestimmtes Thema bzw. ist nach Themen und Unterthemen in einzelne Unterforen unterteilt. Es können Diskussionsbeiträge (Postings) hinterlassen werden, welche die Interessierten lesen und beantworten können. Mehrere Beiträge zum selben Thema werden wie im Usenet zusammenfassend als Thread (Faden) oder Thema (Topic) bezeichnet. Mit dem Eröffnen eines neuen Threads kann ein neues Thema zur Diskussion gestellt werden.
Im Internet besonders beliebt sind Hilfe-Foren, in denen Benutzer Ratschläge zu einem bestimmten Thema erhalten können. So wird eine Hilfestellung angeboten, die bei speziellen Problemen und nur wenigen anderen Informationsquellen die einzige Hilfe sein kann. Hilfreich sind Benutzer-Foren z.B. auch für Hardware- und insbesondere Software-Hersteller, weil diese durch Benutzer- bzw. Anwenderbeiträge schnell und weiträumig über Mängel ihrer Produkte – bei Software über sogenannte Bugs (Programmierfehler) – informiert werden und reagieren können. In einigen Foren werden auch aktuelle Themen aus Politik oder Weltgeschehen diskutiert.