Inhaltsverzeichnis

1. Einleitung

Das Internet hat neben zahlreichen positiven Aspekten, wie z.B. einer Fülle von Informationen, auch seine Schattenseiten.
Diese Hausarbeit widmet sich eben diesen Schattenseiten, stellt sie nacheinander vor und erläutert sie mit praktischen Beispielen. Zum Schluss werden zudem Abwehrmechanismen aufgezeigt und erklärt, die einem helfen, diese Probleme zu unterdrücken, abzuwehren oder zu beseitigen.

2. Spam

2.1 Begriffsklärung

Der Begriff stammt aus einem Sketch von Monty Python, einer Truppe britischer Komödianten. In diesem Sketch wird versucht, ein Menü zu bestellen, welches kein Spam (eine bekannte Marke von Dosenfleisch) beinhaltet, was offenbar schier unmöglich ist. Hieraus leitete sich dann der Begriff für unerwünschte Werbung ab.
Man teilt Spam-eMails in zwei Kategorien ein. Zum einen ist das UBE (unsolicited bulk eMail; unerwünschte eMails), die das Postfach des eMail-Accounts regelrecht überfluten und den Empfänger nötigen, viel Zeit in die Beseitigung dieser elektronischen Post zu investieren. Die andere Variante nennt man UCE (unsolicited commercial eMail; unerwünschte Werbe-eMail) und enthält Werbung, meist marktschreierischer Natur und aus dem pornografischen Bereich.
Ein anderes Ärgernis sind so genannte Pop-Up-Fenster, also sich selbsttätig öffnende Fenster in Internetbrowsern, die in fast allen Fällen ebenfalls Werbung beinhalten.

2.2 Spambelästigung durch eMails

Mittlerweile ein alltägliches Ritual – man ruft seine eMails ab und darf erstmal 5 bis 20 eMails mit lästiger Werbung aussortieren und löschen. Die Texte sind nahezu alle gleich, angepriesen wird alles Mögliche, von Penisverlängerung über Viagra bis hin zu Sexkontakten einfach alles, was man gemeinhin als unseriös bezeichnen kann und durchaus für peinliche Momente sorgen kann, wenn einem die falsche Person beim abrufen der eMails über die Schulter guckt. Natürlich werden diese Spam-Mails nicht zielgruppenorientiert verschickt, sondern wahllos an jeden, dessen eMail-Adresse halt in diesem Spam-Verteiler gelandet ist.

Als praktisches Beispiel hier einmal eine UCE-Mail, die am 13.03.2005 im Postfach des Autors lag:

> "Hi!
>
> We have a new product that we offer to you, C_I_A_L_I_S soft tabs,
>
> Cialis Soft Tabs is the new impotence treatment drug that everyone is talking about. Soft Tabs acts up to 36 hours, compare this to only two or three hours of Viagra action! The active ingredient is Tadalafil, same as in brand Cialis.
>
> Simply dissolve half a pill under your tongue, 10 min before sex, for the best erections you've ever had!
>
> Soft Tabs also have less sidebacks (you can drive or mix alcohol drinks with them)."

Hier wird also ein Mittel gegen Impotenz angeboten. Versprochen werden einem die tollsten Sachen, aber entspricht das auch der Realität? Dies darf wohl mit relativer Sicherheit angezweifelt werden, denn Garantie etc. gibt es natürlich keine, von rechtlicher Absicherung mal ganz zu schweigen, sitzen die Anbieter doch meistens im Ausland.
Man sieht auch, dass die eMails völlig unpersönlich sind. Keine Namensnennung, keine ausführliche Begrüßung, was noch stärker erkennen lässt, dass diese eMails reiner Spam sind.
Zudem sind Spam-Mails ein nicht unerheblicher Schaden. Im Jahre 2002 belief sich dieser Schaden auf ungefähr 2,5 Milliarden Euro.
Die meisten eMail-Anbieter, z.B. GMX oder Hotmail, arbeiten schon länger an sogenannten Filtersystemen, die die Spam-Mails gar nicht erst bis zu den Endkunden gelangen lassen sollen.
Doch auch die Versender des Spams schlafen nicht. Gab' es erst Spam in der dt. Sprache (damit die Filtersystem, die z.B. bei englischen Begriffen in der Betreffzeile der eMail anschlagen, somit überlistet werden), so steht oftmals unverständliches Kauderwelsch in der Betreffzeile, um die Filtersysteme auszuschalten.
Man kann aber selbst einiges tun, um erst gar nicht in solchen Spamverteilern zu landen. So sollte man nie seine eMail-Adresse in Gästebüchern oder Internetforen hinterlassen, da diese bevorzugt von Indexierungsprogrammen, Spiders genannt, besucht werden und somit die eMail-Adresse ebenfalls gespeichert und weitergegeben werden kann.

Genauso verhält es sich mit Gewinnspielen oder kostenlosen Produktproben im Internet, die man anfordern kann. Hier ist es wichtig, auf das Kleingedruckte zu achten, damit man sichergehen kann, dass die eigene Adresse nicht weitergegeben wird.
Oder aber, man legt sich eine zweite eMail-Adresse für eben solche Gelegenheiten zu.

2.3 Spambelästigung durch Pop-Up-Fenster im Internetbrowser

Hiermit werden Browserfenster bezeichnet, die sich selbstständig öffnen, um dem User Werbung zu präsentieren. Es gibt sogar sehr aggressive Seiten, die immer wieder neue Pop-Ups laden, wenn man diese schließt, man fühlt sich an die griechische Hydra erinnert – für jedes geschlossene Browserfenster öffnen sich drei neue. Das führt teilweise bis hin zum Absturz des Browsers oder gar des kompletten Rechners.
Abhilfe schafft hier ein so genannter Pop-Up-Blocker wie z.B. der Web Washer (http://www.webwasher.de), der solch nervige Werbung unterbindet. In diversen Browern wie z.B. Opera oder Firefox ist ein solcher Blocker bereits standardmäßig integriert.
Der Internet Explorer ist überhaupt ein Browser, den man am besten durch eins der oben genannten Konkurrenzprodukte ersetzen sollte. Der Hauptgrund liegt hierbei in der Tatsache, dass der Internet Explorer der meistverbreitete Browser und damit Hauptangriffsziel für Betrüger ist.

3. Scam

3.1 Begriffsklärung

Der Begriff Scam kommt aus dem Italienischen und bedeutet „Angriff“. Gemeint sind hiermit betrügerische Geschäftsangebote und sonstige Aktivitäten im Internet.
Der bekanntestes Fall dürfte die so genannte „Nigeria Connection“ sein.

3.2 Nigeria Connection

Bei der Nigeria Connection handelt es sich um eine Organisation von Kriminellen, die mit harmlos und viel versprechend wirkenden eMails ihre Opfer ködern, um so an deren Erspartes zu gelangen.
Nachfolgend ist ein gekürztes Beispiel abgedruckt, welches analysiert und kommentiert wird.

Das Beispiel stammt von der Internetseite www.reversescam.com:

> “DEAR SIR/MADAM,
>
> COMPLIMENTS OF THE SEASON. GRACE, PEACE AND LOVE FROM THIS PART OF THE ATLANTIC TO YOU. I HOPE MY LETTER DOES NOT CAUSE YOU TOO MUCH EMBARRASSMENT AS I WRITE TO YOU IN GOOD FAITH. BASED ON THE CONTACT ADDRESS GIVEN TO ME BY A FRIEND WHO WORKS AT THE NIGERIAN CHAMBER OF COMMERCE ATTACHED TO YOUR EMBASSY IN MY COUNTRY”

Begonnen wird mit einer unheimlich freundlichen Begrüßung und einer Entschuldigung für die Störung. Dies soll den Empfänger der eMail wohl freundlich stimmen. Dann beruft man sich auf eine Quelle, die vertrauenerweckend wirken soll und das Wort „Botschaft“ lässt einen aufhorchen.

> “I REPRESENT MOHAMMED ABACHA,SON OF THE LATE GEN. SANI ABACHA, WHO WAS THE FORMER MILITARY HEAD OF STATE IN NIGERIA. HE DIED IN 1998. SINCE HIS DEATH, THE FAMILY HAS BEEN LOOSING A LOT OF MONEY DUE TO VINDICTIVE GOVERNMENT OFFICIALS WHO ARE BENT ON DEALING WITH THE FAMILY. “

Schnellstmöglich wird ein fremd wirkender Name ins Spiel gebracht, der offenbar in einem fremden Land, eine wichtige Rolle gespielt hat. Dies kann ein reicher Ölscheich, der Präsident eines Staates oder sogar eine Prinzessin sein. Damit soll wohl eine gewisse Seriosität und vor allem Wichtigkeit suggeriert werden.
Was immer gleich ist, ist die Tatsache, dass es um verlorenes Geld geht. Geld wird ebenfalls sehr schnell erwähnt, damit der Leser diese eMail auch hoffentlich nicht direkt löscht.

> “CONSEQUENTLY, THE FAMILY HAS ASKED ME TO SEEK FOR A FOREIGN PARTNER WHO CAN WORK WITH US AS TO MOVE OUT THE TOTAL SUM OF US$75,000,000.00 (SEVENTYFIVE MILLION UNITED STATES DOLLARS), PRESENTLY IN THEIR POSSESSION. THE SWISS GOVERNMENT HAS ALREADY FROZEN ALL THE ACCOUNTS OF THE FAMILY IN SWITZERLAND, AND SOME OTHER COUNTRIES WOULD SOON FOLLOW TO DO THE SAME. THIS BID BY SOME GOVERNMENT OFFICIALS TO DEAL WITH THIS FAMILY HAS MADE IT NECESSARY THAT WE SEEK YOUR ASSISITANCE IN RECEIVING THIS MONEY AND IN INVESTING IT ON BEHALF OF THE FAMILY. THIS MUST BE A JOINT VENTURE TRANSACTION AND WE MUST ALL WORK TOGETHER. “

Nun kommt der Empfänger dieser Mail ins Spiel. Erwähnt wird eine astronomisch hohe Summe, in deren Besitz angeblich derjenige ist, der einem schreibt oder es zumindest verwaltet. Um wieder an das Geld zu kommen, welches auf irgendwelchen Schweizer Konten lagert, braucht man eine helfende Hand, die das Geld transferiert.

> “I HAVE PERSONALLY WORKED OUT ALL MODALITIES FOR THE PEACEFUL CONCLUSION OF THIS TRANSACTION. THE TRANSACTION DEFINITELY WOULD BE HANDLED IN PHASES AND THE FIRST PHASE WILL INVOLVE THE MOVING OF US$25,000,000.00. MY CLIENTS ARE WILLING TO GIVE YOU A REASONABLE PERCENTAGE OF THIS MONEY AS SOON AS THE TRANSACTION IS CONCLUDED. “

Hiermit sieht man das Verlockende an dem ganzen Brief – der Empfänger soll eine nicht unerhebliche Beteiligung bekommen, da man ihn für seinen Aufwand entlohnen möchte.

> "PLEASE, THIS TRANSACTION REQUIRES ABSOLUTE CONFIDENTIALITY AND YOU WOULD BE EXPECTED TO TREAT IT AS SUCH UNTIL THE FUNDS ARE MOVED OUT OF THIS COUNTRY TO WHERE YOU INTEND TO RECEIVE THEM.
>
> LET ME KNOW IF YOU ARE INTRERESTED SO I CAN FURNISH YOU WITH MORE DETAILS. HOWEVER, PLEASE, IGNORE THIS LETTER AND RESPECT OUR TRUST IN YOU BY NOT EXPOSING THIS TRANSACTION, EVEN IF YOU ARE NOT INTERESTED."

Unweigerlich kommt auch die Aufforderung zum stillschweigen über die geplante Aktion, denn der Empfänger könnte ja gewarnt werden, dass er Gefahr läuft, einem großen Schwindel aufzulaufen. Auch im Falle einer nicht stattfindenden Kooperation möge man doch bitte keine Informationen weitergeben, denn je weniger die Öffentlichkeit über diese betrügerische Organisation weiß, um so einfacher ist es für sie, andere Personen möglicherweise um ihr Geld zu bringen.
Lässt man sich erst einmal auf eine solche Aktion ein, sieht man sein investiertes Geld nie wieder. In der Regel wird man darum gebeten, einen gewissen benötigten Betrag (mehrere tausend Euro) an ein bestimmtes Konto zu überweisen, um die Transaktion anlaufen zu lassen. Das Geld würde für Gebühren und ähnliches benötigt, aber man würde es ja wiederbekommen.
Die Nigeria Connection ist allerdings nicht nur seit der gestiegenen Popularität des Internets aktiv, sondern hat solche Briefe schon als Fax oder mit der Post verschickt.
Um sich jeglichen Ärger zu ersparen, sollte man eMails solcher Art direkt und ungelesen löschen.

3.3 Gefälschte Passwortabfragen, Betrügereien bei eBay und mit Kreditkarten

Eine weitere, höchst kriminelle Machenschaft sind unter anderem die gefälschten Passwortabfragen, Betrüger, die bei eBay aktiv sind oder Betrug mit Kreditkarten machen.

Die Methode mit den gefälschten Passwortabfragen, Phishing genannt, läuft dementsprechend ab, als das man eine eMail erhält, in der man gebeten wird, sein Passwort, z.B. die Zugangsdaten für das Online-Banking, mitzuteilen, da man einen Fehler entdeckt hätte und das überprüft werden sollte.
Mittlerweile geht das Ganze sogar noch einen Schritt weiter. Man wird gebeten, seine Kontodaten zu überprüfen und zwar auf einer in dieser Mail mitgeteilten Seite. Diese klingt so

ähnlich, wie die offizielle Seite der Bank, z.B. http://deutsche-bnk.info (URL nach offenbar erfolgtem Betrug nicht mehr funktional). Hat man dort den Fehler gemacht und tatsächlich seine Daten eingegeben, so hindert die Verbrecher nichts mehr daran, das Konto des Opfers leerzuräumen.
Eine Bank oder ein anderes seriöses Unternehmen wird einen nie nach vertraulichen Daten fragen. Deswegen solche eMails löschen.

Ähnliches ereignet sich bei Betrügereien mit Kreditkarten.
Um Zugang zu diversen, eher unseriösen Angeboten einiger Homepages zu erhalten, muss man erst einmal bezahlen. Meist geht dies nur über eine Kreditkarte. Hat man nun dort seine Nummer hinterlassen, wird in regelmäßigen Abständen Geld vom Konto abgehoben, da man unwissentlich ein so genanntes Abo eingerichtet hat. Kündigen kann man kaum bis gar nicht, da man ja gar keine Informationen behalten hat, wo man seine Daten hinterlassen hat. Die Betrüger rechnen also schon mit der eigenen Unvorsicht.
Andere Betrüger gehen aber auch einen Schritt weiter und fälschen ihre Karte und gehen dann auf ihre Kosten einkaufen. Die Kreditkartennummer nur weitergeben, wenn man sich sicher sein kann, dass man es mit einem seriösen Gegenpart zu tun hat.

Betrügereien bei eBay laufen anders ab. Hier ersteigert man Ware, die man per Vorkasse bezahlen muss, aber nie erhält. Im Jahre 2004 ging ein Fall durch die Presse, in der ein Anbieter erst durch kleine Auktionen ein positives Profil von sich erstellen konnte, indem er als gutes Mitglied von eBay dastand, mit vielen positiven Bewertungen. Danach ging die Betrügerei los. Versteigert wurden allerhand teure Sachen, die auch bezahlt, aber halt nie an die geprellten Käufer ausgeliefert wurden.
Solche Leute bringen die ganze Auktionsplattform in Verruf, verunsichern potenzielle Käufer und schaden so der Allgemeinheit. Nicht besonders hilfreich ist dabei die Firma eBay selbst, die offenbar nur ein geringes Interesse hat, ihren Kunden Service und damit Schutz zu bieten. Auf die Beantwortung von eMails wartet man leider oft vergeblich und auch das Sperren von offensichtlich auffälligen Mitgliedern kann schon mal dauern, was sehr ärgerlich ist.

4. Sonstiges

4.1 Viren

Viren sind kleine Programme, die innerhalb kürzester Zeit einen Computer lahm legen bzw. unbrauchbar machen können. Dabei löschen sie wichtige Systemdateien, so dass das Betriebssystem nicht mehr arbeiten kann. Ein Teil dieser Viren verschickt sich auch selbstständig an alle Personen, die in einem Adressbuch mit ihrer eMail-Adresse vermerkt sind.

Viren kann man sich ganz schnell einfangen, indem man die Anhänge (angebliche Bilder, Textdateien oder Programme) in eMails unbekannter Absender öffnet (oftmals zu erkennen an der Endung .vbs). Daher unter keinen Umständen die Anhänge solcher eMails öffnen. Auch hier empfiehlt es sich, die komplette eMail ungelesen zu vernichten.

Zusätzlich sollte man einen guten Virenscanner installiert haben und diesen regelmäßig aktualisieren, um diesen Computerviren möglichst vorbeugen zu können.

Das bekannteste Beispiel war der Computervirus „Melissa“ des Amerikaners David L. Smith, der über eMails mit der Betreffzeile „I love you“ verschickt wurde und einen Schaden von 80 Mio. Dollar verursacht hat.

4.2 Trojaner bzw. „trojanisches Pferd“

Trojaner sind im Endeffekt eine Weiterentwicklung von Viren. Hierbei wird allerdings nicht primär das Computersystem lahm gelegt, sondern das Programm begibt sich auf die Suche nach Passwörtern und ähnlich vertraulichen Daten, die dann per eMail an den Absender zurückgeschickt werden.

Das Programm selbst versteckt sich in anderen Dateien (z.B. Bildern) und wird aktiv, wenn diese Datei geöffnet wurde (daher der bezeichnende Name).

Auch hier sorgte ein Fall für besondere Furore – es war der 16jährie Aron Spohr, der innerhalb kürzester Zeit die Verschlüsselung des T-Online-Programmes der Telekom entschlüsselte und so die Zugangsdaten mehrerer hundert T-Online-Kunden ausspionieren konnte.

Auch hier helfen die gleichen Ratschläge wie bei Viren, um sich vor diesen Programmen zu schützen.

4.3 Dialer

Dialer sind derzeit mit die gefährlichste Bedrohung des Internets. Dialer sind Programme, die augenblicklich die Internetverbindung beenden und dann ohne das Wissen des Opfers eine neue Verbindung aufbauen, die schon bei kürzestem Verbindungsaufbau hohe Telefonkosten verursachen.
Dialer lauern oftmals hinter Links auf den Seiten unseriöser Anbieter und starten sofort und wiederholt eine Installationsanforderung, bis der Benutzer aus Versehen doch mal auf „ok“ drückt.

4.3 Browserhijacking

„Browserhijacking“ bedeutet, dass ohne Anforderung eine Internetseite aufgerufen wird, zu der man eigentlich gar nicht hin will. Meistens handelt es sich dabei um eine unseriöse Suchmaschine oder um eine Seite, die sofort einen Dialer installieren möchte.
Entweder diese Seiten richten sich als Startseiten im Browser ein und werden bei jedem Programmstart angewählt oder man klickt auf einen Link, der einen auf Seite X bringen soll, aber stattdessen wird man sofort zu Seite Y weitergeleitet.
Hier helfen Programme wie Ad Aware (http://www.lavasoft.com) oder SpyBot (http://beam.to/spybotsd), um dieser Plage Herr zu werden.

5. Zusammenfassung

Wie man sieht, gibt es eine ganze Reihe gefährlicher und vor allem lästiger Sachen im Internet. Gegen einiges (Pop-Ups, Viren) kann man sich sehr leicht und sehr effektiv schützen – manchmal reicht schon der gesunde Menschenverstand.
Wer sich auf eine Organisation wie die „Nigeria Connection“ einlässt, ist es mitunter selber Schuld, wenn er um sein Hab und Gut gebracht wird.
Andere Sachen machen weit größeren Ärger und sind nicht ganz so einfach zu beseitigen (Dialer).
Dennoch ist diese negative Betrachtungsweise des Internets nur ein kleiner Teil des breiten Spektrums, den das neue Medium bietet. So sollte sich niemand davon abhalten lassen, sich mit dem Internet vertraut zu machen, denn genauso wie die kriminellen Elemente, arbeiten viele Leute an immer besseren Abwehrmechanismen.

6. Quellenangaben

6.1 Artikel aus dem Internet

6.1.1 19.10. 2004 : Fakten zum Thema "Phishing"
http://enterprisesecurity.symantec.de/article.cfm?articleid=4705&EID=0

6.1.2 19.12.2004: "eBay"-Betrug
http://www.mdr.de/kripo-live/betrug/1739686.html

6.1.3 Fenner, Kai: Internetfallen.de das ORIGINAL !
http://www.internetfallen.de/

6.1.4 Racine, Roman: Was ist Spam?
http://spam.trash.net/was.shtml

6.1.5 Robben, Matthias 17.09.2003: Spam: Darf es ein wenig mehr sein?
http://www.ecin.de/spotlight/2003/09/17/06220/

6.1.6 Roth, Wolf-Dieter 02.02.2004: Spam, Betrug und Drogen
http://www.heise.de/tp/r4/artikel/16/16665/1.html

6.1.7 Rötzer, Florian 02.05.2002: Gefängnis für den Autor des Melissa-Virus
http://www.heise.de/tp/r4/artikel/12/12451/1.html

6.2 Einträge aus Wikipedia

6.2.1 Wikipedia: Phishing
http://de.wikipedia.org/wiki/Phishing

6.2.2 Wikipedia: Spam (Monty Python)
http://en.wikipedia.org/wiki/Spam_(Monty_Python)