Sicherheit im Internet und E-Mail

Im Internet und in der E-Mail gibt es Gefahren, die allen bestens bekannt sind. Trotzdem hat es viele Anwender/Innen, die nicht recht wissen, wie sie damit umgehen sollen, die sich nicht gross darum kümmern, falsche Informationen haben, das technische Wissen fehlt usw. und irgendwann einen nicht mehr richtig funktionierenden Computer haben.
Bekanntlich sind das Internet und die E-Mail zwei verschiedene Dinge. Die Gefahren und deren Auswirkungen sind die gleichen, so dass ich in diesem Artikel in grossen Teilen keinen Unterschied zwischen Internet und E-Mail mache. Die Software ist auch auf den Schutz beider Dienste ausgelegt. Meine Ausführungen richten sich an all jene Personen, die etwas unsicher sind. Profis unter Euch können sich das Lesen ersparen.
Der erste Computervirus wurde vor etwa 20 Jahren programmiert. Heute sind es zwischen 60'000 und 100'000. Allein im dritten Quartal 2003 tauchten insgesamt 823 neue Viren auf.

Mit welchen Gefahren müssen wir nun rechnen? Nachfolgend eine Aufstellung von Begriffen, die alle kennen, aber nicht alle wissen, um was es sich dabei handelt:

Virus

Ein Virus ist ein kleines Programm, das dazu geschrieben wurde, die Funktionsweise eines Rechners zu ändern. Es installiert sich ohne die Erlaubnis oder Kenntnis des Benutzers. Es gibt 5 bekannte Virentypen: Programmviren, System- oder Bootviren, Masterbootviren, Hybridviren und Makroviren.
Viele Viren sind dazu programmiert, dem Computer zu schaden. Sie beschädigen Programme, löschen Dateien oder formatieren die Festplatte neu. Andere Virentypen richten keine eigentlichen Schäden am Computer und Programmen an, sondern geben ihre Anwesenheit durch Text, Bild oder Ton bekannt. Auch diese "ungefährlichen" Viren können Benutzern Probleme bereiten. Sie gebrauchen Speicher, der von legitimen Programmen verwendet wird. Deswegen verursachen sie oft ein fehlerhaftes Verhalten und können zu Systemabstürzen führen. Einige davon enthalten Programmierfehler, welche ebenfalls Systemabstürze und Datenverluste hervorrufen. Informationen zu Viren und Würmer finden Sie unter: www.tu-berlin.de/www/software/antivirus.shtml und www.sophos.de/virusinfo

Wurm

Ein Wurm ist ein Programm, das sich selbstständig von Computer zu Computer verbreitet. Die Absicht der Würmer ist, so viele Computer wie möglich zu befallen. Sie wählen die gespeicherten E-Mailadressen an, was eine rasend schnelle Verbreitung garantiert. Man denke an Konzerne, bei denen jeder Arbeitnehmer dutzende, ev. hunderte E-Mailadressen gespeichert hat. Jeder sendet dann den Anderen sinnlose E-Mails zu, was zu einem Kollaps des ganzen Firmennetzes führen kann. Etliche Würmer haben einen Virus integriert, welcher auf den befallenen Rechnern seinen Schaden anrichten kann oder Backdoors einrichtet (siehe Firewall). Viele Würmer werden für Angriffe auf grosse Firmen programmiert. Informationen zu Würmer finden Sie bei den Virus-Links.

Trojaner

Trojanische Pferde sind Betrüger. Es handelt sich um Dateien, die sich als nützliche Programme ausgeben, in Wahrheit aber schädlich sind. Trojaner enthalten einen schädlichen Code, der, wenn er ausgelöst wird, Datenverlust und, noch schlimmer, Datendiebstahl zur Folge haben kann. Es werden z.B. Passwörter für Onlinebanking mitgeschrieben und per E-Mail an den Absender des Trojaners gesendet. Besonders aggressive Formen richten Backdoors ein (siehe Firewall), über welche der Trojaner-Absender auf ihr System zugreifen und aus der Ferne übernehmen kann. So kann er sämtliche Daten ihres Computers einsehen und das ihm passende auf seinen PC übermitteln. Und SIE merken davon nichts. Viele Infos gibt es bei: www.trojaner-info.de
Hier zwei kostenlose Programme in deutscher Sprache zum Aufspüren und entfernen von Trojanern: das sind TrojanCheck: www.trojancheck.de und ANTS: www.ants-online.de

Hoax

Hoax sind Scherzviren. Es sind Nachrichten, die meist über die E-Mail versendet werden und Kettenbriefen gleichkommen. Darin wird z.B. auf neue Viren oder ähnliches hingewiesen, man soll die Nachricht an alle Freunde, Bekannte usw. weiterleiten. Als Quelle wird oft eine namhafte Firma erwähnt. Dadurch werden die Netze unnötig belastet und unter unerfahrenen Benutzern Angst geschürt. Infos bei: www.hoax-info.de

Dialer

Dialer gehören nicht in die hier beschriebene Kategorie, denn sie richten weder Schaden am Computer an noch versenden sie sich selbstständig weiter. Es handelt sich dabei um Programme, die Sie auf gebührenpflichtige Internetseiten umleiten. Bekanntlich sind es die 09xx Nummern. Es gibt zwei Typen von Dialern. Einerseits die offen angekündigten, zum andern jene, die sich heimlich einschleichen und ohne Ihr Wissen arbeiten. Wer benützt nun solche Dialer? Stellen Sie sich vor, Sie möchten von einem bekannten Fotograf Fotos herunterladen. Dieser Fotograf will seine Bilder aber nicht gratis anbieten, sondern will Geld dafür. Er macht Sie darauf aufmerksam. Wenn Sie einverstanden sind, wird die bestehende Verbindung auf eine andere, kostenpflichtige Nummer umgeleitet. Nicht seriöse Anbieter leiten Sie ohne Nachfrage auf solche Nummern um. Sie stellen das erst fest, wenn Sie die Telefonrechnung erhalten. Dieses Vorgehen wird oft von Anbietern von Sexseiten gewählt. Aber nicht nur, immer mehr dubiose Geschäftemacher wollen schnell abkassieren. So werden E-Mails versandt, um vor Viren zu warnen. Natürlich wird gleich eine Webseite erwähnt, wo ein Programm oder Patch heruntergeladen werden kann, welche die Viren auf Ihrem PC suchen und entfernen. Was nicht gesagt wird ist, dass Ihre Telefonleitung auf eine gebührenpflichtige Nummer (Dialer) umgeleitet wird. Eine weitere Methode ist, beim Herunterladen von Dateien aus dem Internet dem Anwender ein Programm anzubieten. Das mit der Begründung, das Herunterladen sei nur mit diesem Programm möglich. Was Ihnen nicht mitgeteilt wird ist, dass es sich dabei um einen Dialer handelt. In der Regel braucht es nie ein zusätzliches Programm, um Daten herunterzuladen. Auch da gibt es Ausnahmen, z.B. bei Microsoft. Aber bei bekannten Firmen werden Sie (hoffentlich) nicht betrogen. Fallen Sie nicht auf Reklame von Anti-Dialer-Software herein, die Sie einfach so über die E-Mail erhalten. Es könnte sein, dass Sie auch da betrogen werden.

Bei den Dialern wird oft gleich eine Einwahlgebühr verlangt, und das bis zu 900 Euro! Danach kostet jede Minute weiteres, durch Sie hart verdientes Geld.

Fragen Sie bei Ihrem Telefonanbieter nach, ob die 09xx Nummern für Ihren Anschluss gesperrt werden können. Dadurch lösen sich etliche Probleme.

Glücklich sind die, die sich über das TV-Kabel ins Internet einwählen. Da haben Dialer keine Chance, eine Verbindung ist nicht möglich.

Nützliche Informationen finden Sie auf den Internetseiten: www.dialerschutz.de und www.bakom.ch/de/service/tc/0900/index.html und www.dialerhilfe.de und www.dialerundrecht.de

Wenn Sie nicht sicher sind, ob auf Ihrem Computer ein Dialer installiert ist, gibt es Software, die nach solchen Programmen suchen, Ihre Einwahl-Verbindung überwachen und Dialer entfernen. Was welches Programm kann, müssen Sie selber nachsehen. Die Software sollte gratis sein.

Yaw, erhältlich bei: www.yaw.at 0190-Warner, 0190-Alarm und Dialer-Control, alle erhältlich bei: www.winload.de

Spyware

Auch die Spyware richtet keinen eigentlichen Schaden am Computer an. Oft sind es Gratisprogramme, die Sie selber installiert haben, z.B. ein Grafikprogramm, einen CD-Player usw. Das Programm zeichnet Ihre Interessen und Vorlieben beim Surfen im Internet auf, überprüft ob Sie kostenpflichtige Software legal installiert haben usw. Die gesammelten Daten leiten die Programme dem Anbieter weiter. Dadurch lassen sich Kundenprofile erstellen. Sie erhalten dann über die E-Mail unerwünschte Reklame. Natürlich hat nicht jeder Anbieter solcher Programme die gleichen Interessen, dadurch sind die Aufzeichnungen verschieden. (Weiterer Hinweis unter Firewall). Häufig werden diese Informationen weiterverkauft. Natürlich spioniert Sie längst nicht jedes Gratisprogramm (Freeware) aus. Hören Sie sich bei Kollegen/Bekannten um, ob diese das Programm kennen. Nützlich sind auch Hinweise über die Software im Internet, Tests bei Zeitschriften usw.

Es gibt Software, zum Teil auch gratis, die auf Ihrem PC nach bereits installierten Spyware-Programmen suchen.

Bekannt ist Ad-Aware, gratis erhältlich bei: www.lavasoft.de

Vorsicht! Wenn Sie auf Ihrem Computer eine Spyware gefunden haben und dann löschen, wird wahrscheinlich auch das Trägerprogramm, also das eigentliche Programm, nicht mehr funktionieren.

Hacker

Hacker versuchen, in Netzwerke von Firmen, Organisationen usw. einzudringen, um mögliche Schwachstellen zu finden. Sie wollen auf den Systemen keine Schäden anrichten. Grundsätzlich melden sie die Schwachstellen den betroffenen Netzwerkbetreibern.

Cracker

Cracker gehen in etwa gleich vor wie Hacker, jedoch mit dem Ziel, Systeme ausser Betrieb zu setzen oder zu beschädigen. Sie machen auch keine Meldungen an die Betreiber. Cracker versuchen, den Kopierschutz von Programmen zu entfernen oder die Schlüssel (Key) aufzulösen, so dass das illegale installieren und kopieren von Programmen möglich wird.

Hacker und Cracker können Ihren ungeschützten Computer als Zwischenstation missbrauchen, um in Ihr oder andere Systeme einzudringen, Mailbomben zu versenden usw. So verschleiern sie ihre Identität. Und Sie merken von dem allem nichts.
Viele Informationen über Sicherheit erhalten Sie bei: www.Sicherheitsaspekte.de

Phishing

Anwender müssen sich verstärkt mit Wachsamkeit gegen so genannte Phishing-Attacken wappnen. Das Wort setzt sich aus "Password fishing" zusammen. Es beschreibt Betrugsversuche, die darauf abzielen, Zugangsdaten, Bankdaten, Identitätsdaten und Ähnliches zu erhalten. Als deutscher Ausdruck kommt "Identitätsdiebstahl" in Frage. Das Phishing ist momentan eine der gefährlichsten Bedrohungen im Internet.
Dabei werden arglose Anwender/Innen mit allerlei Tricks per E-Mail auf gefälschte Internetseiten gelockt und zur Eingabe von Passwörtern usw. aufgefordert. Die Betrüger bilden gesamte Browserfenster mit Webseiten, auch Seiten mit geschlossenem Sicherheitsschloss, nach. Rein optisch sind die gefälschten Seiten nicht vom Original zu unterscheiden. Dieses Problem betrifft alle Browser, ist also nicht von Ihrer verwendeten Software abhängig.
Gemäss Angaben von antiphishing.org wurden bereits Zugangseiten eines bekannten Auktionshauses und Treuhandservices gefälscht. Die Experten des Sicherheitsunternehmens Sophos haben im Internet frei verfügbare Software gefunden, die für das Erstellen von gefälschten Webseiten nötig sind. Es wird in Zukunft vermutlich auch von "Amateuren" versucht werden, arglose Anwender/Innen zu betrügen.
Um auf diese Täuschungsmanöver nicht hereinzufallen, gilt:
Seiten, die Benutzerdaten verlangen, zum Beispiel Internetbanking und Auktionen, sollten immer direkt durch die Eingabe der Adresse im Browser (Internet Explorer, Mozilla usw.) angesteuert werden. Sehr wichtig: Solche Seiten niemals über Links, die in E-Mails enthalten sind, ansteuern. Seriöse Banken, Auktionen usw. werden nie über E-Mail Passwörter usw. anfordern. Es ist auch nicht üblich, dass Sie Mails erhalten, in denen Ihnen mitgeteilt wird, dass Ihr Konto usw. nicht mehr gültig ist und über den im Mail enthaltenen Link erneuert werden muss. Es ist möglich, dass sie Mails von Banken, Auktionen usw. erhalten, in denen Links zu neuen Geschäftsbedingungen oder Ähnlichem führen. Um diese Seiten anzusehen, schreiben Sie die Adressen auf und geben diese im Browser ein. Dabei können Sie gleich prüfen, ob die Adresse mit dem Original übereinstimmt, zum Beispiel: www.meineBank.com
In diesem Artikel wird auch an anderen Stellen auf dieses Problem eingegangen.

Schutz vor Bösewichten

Wie schützen Sie sich nun vor diesen Bösewichten, die mit Ihnen und Ihrem Computer nichts Gutes vorhaben und Schaden anrichten wollen?
Zuerst stellen Sie die Software ihres Computers so ein, dass Sie bereits eine kleine Sicherheit haben.

Windows XP ohne ServicePack 2

Im Windows XP hat es eine interne Firewall. Aktivieren Sie die, so muss ein Eindringling bereits eine erste Hürde nehmen. Und so aktivieren Sie die Firewall im Windows XP:

- *Start,* - *Systemsteuerung,* - *Netzwerk- und Internetverbindungen,* - *Netzwerkverbindungen*
(Hinweis: Wenn Kategorie Netzwerk- und Internetverbindungen nicht angezeigt, klick oben links im Fenster auf: - *Zur Kategorieansicht wechseln*.)
Klick auf - *DFÜ* oder - *LAN oder Hochgeschwindigkeitsinternet* auf Symbol, um die Verbindung auszuwählen, die Sie schützen möchten.
Klick links im Aufgabenbereich unter - *Netzwerkaufgaben* auf - *Einstellungen dieser Verbindung ändern*. (Sie können auch mit der rechten Maustaste auf die Verbindung klicken, die Sie schützen möchten, und dann auf *Eigenschaften* klicken.)
Klick auf Registerkarte - *Erweitert* unter - *Internetverbindungsfirewall*
Aktivieren vom Feld neben "Diesen Computer und das Netzwerk schützen, indem das Zugreifen auf diesen Computer vom Internet eingeschränkt oder verhindert wird".
Abschliessen mit - *OK*
Bei dieser Firewall handelt es sich um einen reinen Port-Blocker. Besuchen Sie die Internetseiten von Microsoft Firewall und Updates: www.microsoft.com/germany/ms/security/windowsxp.mspx

Windows XP mit Service Pack 2

Wenn Sie das Service Pack 2 installiert haben, erscheint beim Neustart das Fenster mit dem „Sicherheitscenter“. Dabei haben Sie drei Möglichkeiten zu Einstellungen. Sie sehen rechts im Center jeweils, ob die Aktionen ein- oder ausgeschaltet sind, in roter Schrift „inaktiv“, grüner Schrift „aktiv“ oder gelber Schrift „nicht überwacht“. Mit einem Mausklick auf diese Fenster öffnen oder schliessen Sie den

Textteil. Wenn Sie das Sicherheitscenter später einmal öffnen müssen, tun Sie das über „Start – Systemsteuerung – Sicherheitscenter“.
Erstens: Die Firewall. Ganz unten im Fenster haben Sie die Optionen für „Sicherheitseinstellungen verwalten für:“ Sie können dort über „Windows-Firewall“ Einstellungen vornehmen. Wenn Sie eine andere Firewall installiert haben, ist es nicht notwendig, die interne Windows-Firewall zu aktivieren. Sie müssen aber sicherstellen, dass die eigene installierte Firewall aktiv ist.
Zweitens: Automatische Updates. In „automatische Updates“ können Sie die automatischen Updates aktivieren oder deaktivieren. Haben Sie „automatisch“ aktiviert, haben Sie verschiedene Möglichkeiten, die Updates vorzunehmen. Wählen Sie die Option „automatische Updates deaktivieren“, müssen Sie die Updates in regelmässigen Abständen über „Start – Windows Update“ selber herunterladen. Dies ist recht einfach, sucht Windows nach dem Aufbau der Internetverbindung selbständig nach Neuerungen.
Drittens: Virenschutz. **Wichtig: Windows verfügt über keinen eigenen Virenscanner**. Sie müssen also ein Virenprogramm installieren. Windows erkennt einige Virenscanner, so auch den Norton AntiVirus. Dabei wird die Überschrift oberhalb der Sicherheitseinstellungen im Balken von „Virenschutz“ auf „aktiv“ geschaltet.
Öffnen Sie den Textteil mit einem Mausklick auf den Balken. Aktivieren Sie unter „Empfehlungen“ das Kästchen „Ich verfüge über ein Antivirenprogramm, das ich persönlich überwache“. Stellen Sie über die Optionen Ihres Virenscanners sicher, dass das Programm die ein- und ausgehenden Daten überwacht.
Wenn Sie die Firewall und die automatischen Updates deaktiviert haben, erscheint beim Start des PC jeweils eine Warnmeldung. Sie können diese ausschalten. Öffnen Sie das Sicherheitscenter, dann die Option „Ressourcen“ und „Warnungseinstellungen“. Deaktivieren Sie jene Kästchen, für die Sie keine Meldungen wollen. Es liegt dann an Ihnen, an die Sicherheit zu denken.

Internet Explorer
Im Internet Explorer können viele Einstellungen vorgenommen werden. Es handelt sich dabei um das Programm, mit welchem Sie Zugang ins Internet haben. An dieser Stelle alle Einstellungen zu erklären, würde zu weit führen. Ich verweise Sie deshalb an eine Internetseite, wo die Einstellungen auf 10 Seiten sehr gut erklärt werden. Diese Anweisungen können Sie herunterladen und ausdrucken. So müssen Sie nicht online bleiben und können die Einstellungen in Ruhe vornehmen. Achten Sie darauf, dass Sie nicht alles deaktivieren und verbieten, sonst werden Webseiten nicht mehr richtig oder unvollständig dargestellt. Und etwas Vertrauen sollte man auch haben. Link: www.html-discount.de/data/sicherheit.pdf
Wenn Sie einen anderen Browser benützen, z.B. Netscape Navigator, Opera, Mozilla, Pegasus usw. finden sie dort ähnliche Einstellungen.

Machen Sie regelmässig Updates Ihres Betriebssystems und des Internet Explorers oder anderer Browser. Die Hersteller sind bemüht, die erkannten Sicherheitslücken in der Software zu schliessen. Sie bieten die Updates gratis auf ihren Webseiten an. In den Medien wird immer wieder darüber berichtet, wenn Microsoft Sicherheitslücken festgestellt hat. Auf der offiziellen Webseite werden Patches angeboten, um Ihr Windows sicher zu machen.
Jedes Windows hat im Menu Start eine Option, um das Update zu starten. Die Patches werden dann automatisch auf ihr System abgestimmt und nach Ihrer Zustimmung heruntergeladen und installiert.

Fallen Sie nicht auf E-Mails herein, die Sie von einer Ihnen bekannten Softwarefirma erhalten und aufgefordert werden, den angegebenen Link zu wählen, um Updates herunterzuladen. Das ist (vermutlich) eine Falle. Ich kenne keinen Hersteller, der Sicherheits-Updates auf diese Weise anbietet. Verlassen Sie das Mailprogramm und benützen das Internet, um die offizielle Webseite der Firma zu besuchen. Suchen Sie dort nach dem angebotenen Update.

Nun zu der Software, die Sie sich selber besorgen müssen.

Anti-Virenprogramm (Virus-Scanner)
Für „normale“ Anwender gilt: Als absolutes Muss sollte auf Ihrem Computer ein Anti-Virenprogramm installiert sein. Es vergeht wohl kein Tag, ohne dass ein neuer Virus, Wurm oder Varianten davon im Internet und der E-Mail auftauchen. Bösartige Viren können Ihren PC unter Umständen unbrauchbar machen. Das kann teuer werden. Bereits das Entfernen eines weniger schädlichen Virus durch den Fachmann kostet einige bis viele Euro. Und ein Programm kaufen Sie danach sowieso.
In der Regel spricht man nur von Virenprogrammen. Natürlich erkennen diese nebst Viren auch Würmer und Trojaner.

Woher nehmen Sie nun ein solches Programm und was kosten diese?
Beim Händler können Sie etliche solcher Programme kaufen. Die bekanntesten sind der Norton- und McAfee-Antivirus und kosten etwa 40-50 Euro. Von der Qualität her sind sich die beiden Programme

ebenbürtig. Die Installation der Programme sollte auch Anfängern keine Mühe bereiten, man wird dabei bequem geführt. Sie erhalten danach für ein Jahr die Möglichkeit, gratis Updates vorzunehmen. Was nach einem Jahr? Bei Norton ist es so, dass Sie sich registrieren können. Wenn Sie dabei die E-Mail-Adresse angegeben haben, erhalten sie automatisch die Nachricht, dass eine Zahlung fällig wird. Diese ist wesentlich günstiger als der Kauf eines Update beim Händler. Die Zahlung erfolgt übers Internet mit Kreditkarte. Danach haben Sie für ein weiteres Jahr Ruhe. Bezüglich Bezahlung mit Kreditkarte achten Sie auf meine Ausführungen weiter unten.
Im Internet können einige Virenprogramme gratis oder gegen einige Euro heruntergeladen werden. Bei den Gratisprogrammen handelt es sich um Freeware. Ein solches, bekanntes Programme ist: Antivir Personal Edition, erhältlich bei: www.free-av.de
Achten Sie darauf, dass die Verwendung für Privatpersonen auch wirklich gratis ist und Updates erhältlich sind. Das gilt selbstverständlich für alle anderen Programme auch. Ich persönlich habe keine Erfahrung mit dem Programm, gehe aber davon aus, dass auch diese Installation einfach vor sich geht. Bei den Gratisprogrammen erhalten Sie keine schriftlichen Dokumentationen, allenfalls eine Online-Hilfe.
Stellen Sie das Programm so ein, dass es sich schon beim Start des Computers selbst aktiviert. So sind Sie sicher, keine Viren über Dateien, die Sie ab Disketten, CD-Rom usw. öffnen, auf Ihr System zu schleusen. In der Regel wird diese Einstellung bereits bei der Installation vorgenommen, ansonsten stellen Sie es ein.
Alle beschriebenen Programme sind deutsch erhältlich. Selbstverständlich gibt es Norton und McAfee auch in vielen anderen Sprachen. Bei der Freeware muss in der jeweils gewünschten Sprache im Internet nach Alternativen gesucht werden.

Wichtig

Nach der Installation muss gleich ein Update des Programms vorgenommen und danach der Computer auf Viren geprüft werden. Um einen guten Schutz zu haben, muss das Virenprogramm alle paar Tage mit einem Update versehen werden. Waren Sie längere Zeit nicht am Computer und wollen dann ins Internet oder die E-Mail, machen Sie zuerst ein Update. Bei diesen Updates werden die Signaturen von neuen Viren heruntergeladen. Dadurch haben Sie Gewähr, dass auch neue Viren erkannt werden.
Beachten Sie aber, dass ganz neue Viren auch von einem aktuellen Update nicht immer erkannt werden. Die Softwarehersteller müssen den Virus ja zuerst kennen, bevor sie Gegenmassnahmen ergreifen können.
Als etwas extreme Vorsichtsmassnahme gilt: Traue niemandem, auch dir nicht !! So schlimm ist es natürlich nicht. Seien Sie aber vorsichtig bei E-Mails, deren Absender Sie nicht kennen oder deren Inhalt Ihnen keinen Sinn macht. Äusserste Vorsicht ist geboten, wenn solche Mails Anhänge haben, also Dateien, die geöffnet werden müssen. Darin verstecken sich die Viren, Würmer und Trojaner.
Beispiele gefällig?
Der Wurm "Sober.C" Es handelt sich dabei um die dritte Variante des Sober. Er kommt nicht über eine Sicherheitslücke auf den Computer, sondern überlistet den Anwender am Computer. Wie ist das möglich? Der Wurm benützt deutschsprachige Betreffzeilen und bedroht zuweilen den Benutzer. So wird zum Beispiel erwähnt, "Sie sind ein Raubkopierer", "Ihre IP wurde geloggt", "Sie tauschen illegal Daten aus", "Ich zeige Sie an", "Umfrage: Rente erst mit 80!" usw. usw. Die Nachrichten sehen zum Teil sehr echt aus. Eine der Nachrichten gibt vor, von der deutschen Polizei zu sein. Im Text steht, gegen den Empfänger sei ein Ermittlungsverfahren wegen illegalem Film- und Musiktausch im Internet eingeleitet worden. Die entsprechenden Akten liegen dem Mail als Dateianhang bei. Wer will sich das schon bieten lassen? Die meisten nicht, andere fühlen sich sicher ertappt! Aber alle öffnen die Datei im Anhang um nachzusehen, was genau Sache ist. Genau das ist der Sinn, der Wurm kopiert sich auf das System und versendet sich selbständig an jene Mailadressen, die gespeichert sind.
Der Wurm "Novarg.A", welcher auch unter anderen Namen bekannt ist, ist ein Mail-Wurm, der als Anhang in einer E-Mail ist, mit der Dateierweiterung .bat, .cmd, .exe, .pif, .scr oder .zip. Wenn ein Computer infiziert wird, richtet der Wurm eine Hintertür (Backdoor) im System ein. Dadurch kann ein Angreifer eine Verbindung zu Ihrem Computer herstellen, um Zugriff auf das angeschlossene Netzwerk zu erhalten. Ausserdem können über die Hintertür beliebige Dateien von Ihrem System gestohlen oder ohne Ihr Wissen installierte Dateien auf Ihrem PC ausgeführt werden.
Etliche Würmer werden programmiert, um sogenannte DoS-Attacken auszuführen. DoS steht nicht für das zu früheren Zeiten benützte DOS, sondern für Denial of Service. Es geht darum, zu einem bestimmten Zeitpunkt von den infizierten Computern aus E-Mails an eine ausgewählte Firma zu versenden. Die Mailserver dieser attackierten Firma sind nicht in der Lage, die grosse Flut der Mails zu bewältigen. Sie versagen ihren Dienst und müssen neu gestartet werden. In grossen Firmen steht natürlich nicht nur ein E-Mailserver, sondern gleich mehrere, was nebst Imageverlust auch erhebliche finanzielle Auswirkungen hat.
Nachdem die Würmer "Novarg" und "Mydoom" im Verkehr waren, schnellte alleine in der Schweiz der Mail-Verkehr um 14% in die Höhe. Der Wurm "Mydoom" hat die Server einer US Softwarefirma lahmgelegt, da sie an einem bestimmten Tag mit Millionen sinnloser E-Mails von infizierten Computern überschüttet wurden.

Ein ähnlicher Angriff auf Microsoft konnte durch das Unternehmen angeblich abgewehrt werden. Solche Würmer sind programmiert, um an einem ganz bestimmten Tag loszuschlagen.
Löschen Sie also dubiose Nachrichten, ohne sie zu lesen und vor allem, ohne die Dateianhänge zu öffnen. Wenn Sie sich nicht sicher sind, nehmen Sie mit dem Absender Kontakt auf.
Ich sende Text wenn möglich nie als Anhang, z.B. als Word-Dokument, sondern schreibe den Text direkt in die Mail.
Viren, Würmer usw. gelangen nicht nur online auf Ihr System, sondern können auf einer Diskette, CD oder in Software sein. Mit einem aktuellen Virenscanner können auch diese Daten durchsucht und die Schädlinge vernichtet, resp. gefunden werden. Wenn Sie eine Datei, einen Ordner oder ganzes Laufwerk überprüfen wollen, klicken Sie diese mit der rechten Maustaste an. Im öffnenden Menu sollte ein Befehl für den Virenscan vorhanden sein. Natürlich können diese Scans auch direkt in der Viren-Software vorgenommen werden.
Viele Infos erhalten Sie bei den beiden Software Hersteller:
www.symantec.com/region/de/avcenter und http://de.mcafee.com/virusInfo/default.asp
Auch bei anderen Herstellern sind Informationen vorhanden.

Firewall

Wenn Sie vor Angriffen aus dem Internet, sowie Weitergabe von Daten Ihres Computers in das Internet geschützt sein wollen, braucht es eine Firewall. Diese gibt es als Software, ca. 40-50 Euro, zum Teil sogar gratis, oder als Hardware (Geräte), die bis zu zirka 300 Euro kosten. Dadurch können Sie sich vor unerlaubtem Eindringen schützen. Die Gratis-Software gibt bereits guten Schutz. Verlangen Sie aber nicht die Einstellmöglichkeiten von teurer Soft- und Hardware.
Wie arbeitet die Firewall? Ihr Computer hat sogenannte Ports, bei welchen Daten von einem System zum anderen übergeben werden, z.B. Internet. Was denken Sie, wie viele Ports Ihr Computer hat? Es sind genau 65'535. Eine unglaublich grosse Zahl. Diese Ports sind standardmässig offen. Also so, wie wenn Sie ihre Wohnung verlassen, ohne Türen und Fenster zu verschliessen. Die Firewall überwacht nun diese offenen Türen und Fenster. Sie meldet sich mit einem Dialogfenster,
sobald Programme/Dateien versuchen, von Ihrem Computer aus eine Verbindung ins Internet herzustellen, oder aus dem Internet auf Ihr System einzudringen versuchen. Sie haben die Möglichkeit, diesen Datenstrom zu verbieten oder zuzulassen. Überprüfen Sie, welche Programme/Dateien von Ihrem Computer aus Zugang ins Internet, oder von aussen in Ihr System, wollen. Macht das für Sie keinen Sinn, ist Ihnen das Programm oder die Datei unbekannt, verweigern Sie die Verbindung (siehe Spyware). Haben Sie Programme, welche automatisch Updates vornehmen, z.B. Windows, Virenscanner usw., wäre es natürlich Unsinn, nach der Meldung die Verbindung zu verweigern. Sie können der Firewall angeben, dass es sich um eine erlaubte Verbindung handelt, und ein nächstes Mal nicht mehr danach fragen muss.
Eine Erhebung durch die TV Sendung Konsumentenschutz "Kassensturz" ergab, dass zirka 50% aller Computer ohne jeglichen Schutz im Internet sind. Am meisten werden jene PC's angegriffen, die oft online sind. Bedenklich ist, dass es noch jetzt viele Firmen gibt, die keine Schutzmassnahmen haben und ihre Unterlagen wie Gehaltsabrechnungen, Verträge usw. für die Eindringlinge offen darlegen.

Programme

Ich stelle zwei bekannte Programme vor. ZoneAlarm. Es handelt sich um ein englisches Programm. Es gibt eine gratis und eine käufliche Version. Gratis erhältlich bei: www.zonelabs.com
Eventuell wird von ZoneAlarm auch eine deutsche Version angeboten. Sygate Personal Firewall. Davon gibt es deutsche Versionen, sowohl gratis als auch käuflich. Gratis erhältlich bei: www.sygate.de

Bei den Programmen, die Sie vom Internet herunterladen, erhalten Sie in der Regel keine schriftlichen Dokumentationen, allenfalls eine Hilfe im Programm oder eine Online-Hilfe. Da in den Programmen Einstellungen bis zur vollständigen Blockierung des Internetzuganges vorhanden sind, sind Erfahrungen mit Firewalls oder allgemein gute Computerkenntnisse Bedingung. Wenn Sie die nicht haben, überlegen Sie sich, ob der Kauf einer Firewall nicht sinnvoller wäre, da Sie dazu ein Handbuch erhalten. Überprüfen Sie aber, dass eines beiliegt. Eine andere Möglichkeit ist, im Internet nach Bedienungsanleitungen zu suchen, welche für viele Programme vorhanden sind.

Tipp

Wenn Sie nicht sicher sind, welcher Virenscanner und/oder Firewall für Sie optimal sind, fragen Sie bei Freunden, Bekannten und Arbeitskollegen nach. Die haben eventuell Erfahrungen damit und können wertvolle Tipps geben.
Eine weitere gute Quelle sind Computerzeitschriften. Da werden immer wieder Testergebnisse von Programmen vorgestellt und die Programme sogar auf der Heft-CD geliefert. Besonders praktisch bei Gratisprogrammen.

Die angegebenen Preise sind eine Schätzung von mir und können einige Euro daneben liegen. (Fachhändler, Warenhaus, Aktionen usw.)
Fast alle Programme sind nicht nur bei den von mir angegebenen Links erhältlich, sondern auch bei vielen anderen Anbietern von Free- und Shareware.

Zahlungen mit Kreditkarte

Nehmen Sie Zahlungen mit Kreditkarte übers Internet vor, gilt besondere Vorsicht.
Sie können installierte Programme, bei denen die Lizenz nach einem Jahr abgelaufen ist, mit einer Zahlung verlängern. So z.B. bei Virenscannern. Dies ist günstiger, als wenn das Programm neu gekauft wird. Weiter können übers Internet bestellte Waren so bezahlt werden. Wenn Sie sich dazu entschliessen, werden Sie vom Anbieter auf eine sichere (verschlüsselte) Webseite umgeleitet. Sie werden mit einem Dialog darauf hingewiesen. Sobald die sichere Seite geöffnet ist, erscheint im Browser unten rechts ein gelbes Vorhängeschloss. Wenn Sie Ihre Kreditkarten-Nummer eingeben sollen und sind nicht auf einer sicheren Seite, brechen Sie den Vorgang ab. Überprüfen Sie, ob Sie auch wirklich auf der abgesicherten Seite des Anbieters sind. Doppelklicken Sie das Vorhängeschloss. Nach wenigen Sekunden, bei älteren PC's mehrere Sekunden, erscheint ein Zertifikat. Darauf ist die vollständige Adresse der sicheren Seite vorhanden, z.B. meineBank.de. Vergleichen Sie diese Adresse mit jener, welche oben im Browser eingetragen ist. Wenn nur ein Detail nicht stimmt, sind Sie auf eine falsche Seite umgeleitet worden.
Beispiel Zertifikat: meineBank.de
Beispiel Angabe Browser: meineBank.be
Sehen Sie den Unterschied? Wie kann das möglich sein? Ein Hacker ist in das System der Bank eingedrungen und hat die sichere Seite der Bank auf seine eigene Seite umgeleitet. Natürlich wählt der Hacker einen möglichst identischen Namen wie die Bank, nur ein kleines Detail ist anders.
Brechen Sie die Verbindung sofort ab und nehmen mit ihrer Bank usw. Verbindung auf.
Was passiert, wenn Sie den Irrtum nicht feststellen und Ihre Passwörter, Bankkonten, Nummern der Kreditkarten usw. bekannt geben? Mögliche Szenarien können Sie sich sicher selber vorstellen. Geben Sie nie persönliche Daten nur auf eine Aufforderung per E-Mail bekannt. Eine seriöse Firma wird das nie verlangen. Bedenken Sie, dass die abgesicherten Seiten meist nicht die Startseiten sind. Das heisst, dass im Browser nach dem Ländercode (im Beispiel .de) weitere Seiten vorhanden sind, z.B. meineBank.de/Zahlungen.

Passwörter

Viele Anwender schützen Systeme, Daten, Programme usw. mit Passwörtern. Es gibt spezielle Programme, um Passwörter zu knacken. Je leichter das Wort, umso schneller gelingt das. Sie können Ihre Passwörter testen. Eine gute Seite dazu ist:
https://passwortcheck.datenschutz.ch/check.php?lang=de
Auf dieser Webseite sind weitere gute Informationen und Hinweise zu Passwörtern vorhanden. Wenn Sie auf der Seite mit dem Passwortcheck sind, ist diese sicher, wie am Vorhängeschloss ersichtlich ist. Versuchen Sie nun, das Zertifikat aufzurufen. Die Adressen sollten identisch sein.

Betrug bei Auktionen

Bei Internetauktionen wird, wie bei andern Dingen auch, betrogen. Sie ersteigern sich im Internet z.B. eine Videokamera als Schnäppchen. Die Bedingungen sind ja so, dass Sie den Kaufpreis im Voraus bezahlen müssen, erst danach wird die Ware geliefert. Der Verkäufer verlangt, dass Sie das Geld ins Ausland überweisen sollen. Sind Sie da sehr vorsichtig, eventuell erhalten Sie die Ware nie. Das Geld ist auch weg, da es bereits einige Stunden nach der Überweisung abgehoben wird. Trauen Sie den guten Bewertungen des Verkäufers nicht, die können manipuliert werden.
Ein Fall aus meiner täglichen Arbeit: Ein junger Mann sieht in der Auktion ein Laptop und interessiert sich dafür. Er nimmt mit dem Verkäufer über E-Mail Kontakt auf. Die Antwort ist schnell da. In einem regen Mailverkehr einigen sich die beiden darauf, das Geschäft ausserhalb der Auktion zu machen. Auch ein Aufrüsten des Gerätes wird, natürlich gegen Aufpreis, versprochen. Der Kaufpreis, über 1'500 Euro, überweist der Käufer per Western Union nach Spanien! Das Geld wird bereits am nächsten Tag abgehoben, der Laptop erhält der junge Mann aber nie. Auch eine Kontaktaufnahme mit der Mail ist nicht mehr möglich. Was war passiert? Der Betrüger hackte das bestehende Konto eines fremden Benützers der Auktion, stellte sein Angebot ein, gab für 24 Stunden eine falsche E-Mailadresse an und schon war alles gelaufen. Dass der Betrüger gute Bewertungen hatte, ist klar, er war ja auf dem Konto eines Anderen.
Bei anderen Betrügereien wurde ein Internet-Treuhandservice benützt, bei dem das einbezahlte Geld bis zur Lieferung der Ware zurückbehalten werden sollte. Dummerweise war diese Firma durch die Betrüger selbst ins Leben gerufen worden!
Leider werden in solchen Fällen die guten Ideen, Auktionen oder Western Union, durch die Betrüger aufs schändlichste missbraucht. Es gibt auch Treuhandservices, die die Geschäfte wie oben beschrieben seriös

durchführen. Wenn Sie also bei Auktionen mitmachen und grössere Beträge ins Ausland überweisen müssen, wenden Sie sich an einen solchen Service, die paar Euro sind es wert.
Auf den Webs der Auktionen werden viele nützliche Tipps gegeben. Bei eBay unter:
http://forums.ebay.de/thread.jsp?forum=40&thread=237558&modifed=20040205113549
http://pages.ebay.de/help/basics/n-is-ebay-safe.html
http://pages.ebay.de/help/community/index.html

Spam

Was ist Spam? Es handelt sich dabei um unerwünschte Werbung, die Sie in Form von E-Mails erhalten. Sie fragen sich sicher, woher die Firmen Ihre Mailadresse haben. Wenn Sie eine Nachricht versenden, wird auch Ihre Adresse bei der Reise zum Empfänger bei verschiedenen Mailservern bekannt. Sie können das mit einem Brief vergleichen, den Sie versenden. Bei der Annahmestelle kann Ihre Adresse gelesen werden, beim Sortieren, bei der Zielpost und schlussendlich durch den Postboten. Zurück zur Mail. Auf den Servern werden die Adressen für eine bestimmte Zeit gespeichert. Spezielle Programme suchen diese Server nach Adressen ab und liefern diese den Werbern weiter. Es werden auch Webseiten nach Adressen abgesucht. Bei den Werbern werden all diese Adressen gesammelt und für die unerwünschte Werbung verwendet. Es gibt CD-Roms zu kaufen, die mit Mailadressen vollgestopft sind. Und es kommen immer mehr dazu. Viel Werbung wird auch an systematisch ausgewählte Adressen verschickt. Wie geht das? Ist Ihr Name Hans Meier und sind 1961 geboren? Ist Ihre Adresse hans.meier@.....? Oder hans61@....? Das heisst, dass viele Mailadressen aus Vor- und/oder Nachnamen und/oder Geburtsjahr bestehen. Für die Werber ist die Chance also gross, viele Treffer zu haben. Wie können Sie sich gegen diese unerwünschte Werbung schützen? Gute Provider, also die Mailanbieter, filtern Werbung bereits heraus. AOL, ein Anbieter der weltweit tätig ist, löscht angeblich täglich Millionen von Werbemails. Wenn Sie trotzdem mit Müll überhäuft werden, können Sie auf Ihrem Computer Software installieren, die die Werbung herausfiltert. Es fragt sich nun, wie gross die Anzahl Werbung sein muss, damit es Sinn macht, automatische Filter zur Anwendung zu bringen. Ich z.B. erhalte in der Woche zirka 510 unerwünschte Werbungen. Da habe ich noch die Übersicht und kann sie "von Hand" löschen. Wird Ihnen aber pro Woche ein mehrfaches davon zugestellt, können Sie sich die Installation eines Spamfilters in Form eines Programms oder Plug-Ins überlegen. Die Programme sind eigenständige Anwendungen und haben eine eigene Oberfläche, die Plug-Ins integrieren sich in das Mutterprogramm, z. B. Outlook.

Programme

Bei den Programmen empfehle ich Ihnen die Gratis-Software Spampal 1.53 in deutscher Sprache, erhältlich bei www.spampal.de. Es ist mit Plug-Ins erweiterbar und erhöht damit die Trefferquote. Besuchen Sie die Webseite und lesen Sie die Anleitungen gut durch.
Bei den Plug-Ins wird es schwieriger etwas zu empfehlen. Da sie sich in das Mutterprogramm integrieren, ist es wichtig, welches Mailprogramm Sie verwenden. Das Plug-In I hate Spam 4.0 ist sehr gut, kostet aber 20 Euro, erhältlich bei www.sunbelt-software.com. Es lässt sich in Outlook, Outlook Express, Eudora und Incredimail integrieren. Gratis ist Spambayes 008.1, erhältlich bei www.spambayes.sourceforge.net. Es kann aber nicht in Outlook Express integriert werden.
Natürlich werden die Programme und Plug-Ins ständig erweitert und verbessert. Wenn Sie also etwas spezielles suchen, lesen Sie auf den Webseiten der Anbieter nach, was sich neues getan hat.
Viele der Programme und Plug-Ins sind lernfähig. Das heisst, Sie geben dem Programm gewisse Informationen, nach denen die Mails gefiltert werden. So ist es möglich, nach wenigen Tagen oder Wochen einen gut funktionierenden Filter zu haben.
Es gibt einige Länder, die über gesetzliche Verbote unerwünschter Mails nachdenken. Dabei sollen nicht nur die Werber, sondern auch die Hersteller der Produkte zur Rechenschaft gezogen werden können. Vor allem die Firma Microsoft macht sich stark dafür.

Image

Mit spezieller Software ist es möglich, ein genaues Abbild Ihrer Festplatte herzustellen. Diese Abbilder können auf andere Festplatten, DVD's oder CD-Roms gespeichert werden. Sollten Sie aus irgend einem Grund Datenverluste haben, z.B. durch Viren, irrtümliches Löschen oder Formatieren, Plattencrash usw., können Sie den Originalzustand der Festplatte mit dem Image wieder herstellen. Der Vorteil eines Image ist, dass die Festplatte nach dem Zurückspielen bootfähig ist, also das Betriebssystem hochfährt. Es gibt etliche solcher Programme, z.B. Norton Ghost für zirka 40 Euro. Ein Image ist nicht mit einem Back-up zu verwechseln, bei dem Sie nur Daten sichern.
Wenn Sie einen neuen Computer kaufen, alle Programme installiert sind und einwandfrei funktionieren, ist es sinnvoll, ein Image zu erstellen. So haben Sie immer ein sauberes, funktionsfähiges System zur Hand. Bei grösseren Änderungen können Sie sich ein neues Image herstellen.

Selbstverständlich sind solche Images auch bei bereits im Betrieb stehenden Computern zu empfehlen. Es gibt (fast) nichts ärgerliches, als wenn man sich alles von Grund auf neu installieren muss.
Machen Sie regelmässig Sicherungen Ihrer persönlichen Daten. Im privaten Bereich reichen meist 1 oder 2 CD aus.

Bemerkungen

Wenn Sie weitere Informationen zu einzelnen Themen oder Begriffen wollen, suchen Sie über Suchmaschinen im Internet. Auch in den Computerzeitschriften werden immer wieder gute Artikel über Sicherheit veröffentlicht. Zudem liegen den Zeitschriften CD's bei, auf denen sich viele Programme befinden. Oft auch die in diesem Artikel beschriebenen.

Lassen Sie sich den Spass am Internet durch diese Ausführungen nicht nehmen. Wenn Sie nur gelegentlich und für kurze Zeiten im Internet sind, können Sie sich dazu entschliessen, nur ein Anti-Virenprogramm zu installieren. Wenn Sie oft und lange, oder sogar immer online sind, müssen Sie auch eine Firewall haben. Wieso? Wenn Sie z.B. immer online sind, wird die Chance, dass Ihr Computer von einem Hacker/Cracker gefunden wird, recht gross. Ist Ihr System nicht geschützt, kann er Ihren PC missbrauchen. Sie haben in diesem Bericht recht viele Informationen. Die sollten Ihnen zu denken geben und Sie dazu anregen, auch eine Firewall zu installieren. Wenn Sie ein Gratisprogramm nehmen, kostet Sie die Sicherheit gar nichts, ausser einige Minuten Arbeit (vielleicht auch etwas mehr!). Also profitieren Sie davon. Wann gibt es in der heutigen Zeit schon etwas nützliches gratis? Haben Sie ein kleines LAN (Netzwerk) zu Hause? Dann benötigen Sie die Firewall. Aber Vorsicht, nicht alle Gratisprogramme können mit einem LAN umgehen.

Ich habe vor der Veröffentlichung dieses Artikels alle Links überprüft. Es kann sein, dass die eine oder andere Webadresse plötzlich nicht mehr gültig ist. Im Internet hat es über die Sicherheit viele weitere Seiten. Suchen Sie über eine Suchmaschine geeignetes Material.
Ich kann an dieser Stelle die Sicherheit im Internet nicht bis in Details behandeln, was auch nicht die Absicht ist. Es soll eine kleine Übersicht sein. Über Sicherheit haben viele Autoren ganze Bücher gefüllt. Für all jene, die es genau wissen wollen, bleibt nur der Gang in den Bücherladen.

Ich wünsche Euch allen viele viren- und würmerfreie Stunden im Internet und möglichst wenig Werbung in den E-Mails.

Wie bereits mehrmals erwähnt, fragen Sie bei Freunden, Bekannten und Arbeitskollegen usw. nach, wie sie ihre Sicherheit im Internet gelöst haben.
Befolgen Sie die Installationshinweise, Konfigurationen und Programmbefehle der Hersteller genau. Lesen Sie die Lizenzbedingungen der Hersteller durch.
Ich übernehme keinen Support für die in diesem Artikel beschriebene Software. Wenden Sie sich an die Hersteller. Ich übernehme keine Haftung für Schäden an Ihren Daten und Computern, die nach dem Installieren der beschriebenen Software entstehen können.
Ich empfehle Ihnen, von Ihrer Festplatte(n) vor dem Installieren von irgendwelcher Software, ein Image zu erstellen.

Marcel Hadorn
Version 1.2