Daten- und Internetsicherheit 02

Viren und Malware

Was sind Viren und Malware?

Seit Ende der Achtziger Jahre gelten die so genannten Computerviren in der breiten Öffentlichkeit als Hauptgefahr für den PC-Nutzer. Aber was sind diese so genannten Viren eigentlich, was machen sie und wo kommen sie her?

Computerviren sind eine Untergruppe von Computerprogramme, die als Malware [ˈmælwɛə] (Kofferwort aus engl. malicious, „bösartig“ und Software) bezeichnet werden, diese führen vom Benutzer unerwünschte und ggf. schädliche Funktionen aus. Da ein Benutzer im Allgemeinen keine schädlichen Programme duldet, sind die Schadfunktionen gewöhnlich getarnt oder die Software läuft gänzlich unbemerkt im Hintergrund. Malware bezeichnet keine fehlerhafte Software, auch wenn diese Schaden anrichten kann.

Das „IT-Sicherheitshandbuch“ des BSI (Bundesamt für Sicherheit in der Informationstechnik), teilt die möglichen Schäden in drei grundlegende Punkte auf:

- **Verlust der Verfügbarkeit.** Verfügbarkeit ist definiert als Bereitstellung der Funktionen eines Systems innerhalb einer vorgegebenen Zeit.
- **Verlust der Integrität.** Integrität ist definiert als Unversehrtheit, Korrektheit, Widerspruchsfreiheit und Vollständigkeit der Information und schließt ein, daß diese Information nur von den dazu Befugten in zulässiger Weise modifiziert werden kann.
- **Verlust der Vertraulichkeit.** Vertraulichkeit ist gegeben, wenn die Information nur den dazu Befugten zugänglich ist und weder unbefugt gewonnen noch ungewollt offenbart wird.

Ergeben sich aus der Ausführung der Funktionen eines Computerprogrammes vorsätzliche ein oder mehrere dieser Schäden an Daten und System, so handelt es sich bei dem Programm offensichtlich um eine Malware.

Malware wird unterschieden in folgende Typen:

- **Computerviren** sind die älteste Art der Malware, sie verbreiten sich, indem sie Kopien von sich selbst in Programme, Dokumente oder Datenträger schreiben. Ein teilweise defektes Virus nennt man „Intended Virus“. Dieses bewirkt meist nur eine „Erstinfektion“ einer Datei, ist jedoch nicht fähig sich weiter zu reproduzieren.
- Ein **Computerwurm** ähnelt einem Computervirus, verbreitet sich aber direkt über Netzwerke wie das Internet und versucht, in andere Computer einzudringen.
- Ein **Trojanisches Pferd** (kurz: Trojaner) ist eine Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogrammes mit einem versteckt arbeitenden, bösartigen Teil, oft Spyware oder eine Backdoor. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.
- Eine **Backdoor** ist eine verbreitete Schadfunktion welche üblicherweise durch Viren, Würmer oder Trojanische Pferde eingebracht und installiert wird. Es ermöglicht Dritten einen unbefugten Zugang („Hintertür“) zum Computer, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft genutzt um den kompromittierten Computer als Spamverteiler oder für Denial-of-Service-Angriffe zu missbrauchen.

Die meisten Risiken im heimischen Umfeld können bereits durch einfache und kostengünstige Maßnahmen drastisch reduziert werden.

Verfügbarkeit

Spyware

Als Spyware (Kunstwort aus spy, dem englischen Wort für Spion, und -ware als Endung von Software, also Programmen für den Computer; zu deutsch etwa Schnüffelprogramm oder -software) wird üblicherweise Software bezeichnet, die persönliche Daten eines PC-Benutzers ohne dessen Wissen oder Zustimmung an den Hersteller der Software (Call Home) oder an Dritte sendet oder dazu genutzt wird, dem Benutzer direkt Produkte anzubieten.

Meist dienen Spywareprogramme dazu, das Surfverhalten im Internet zu analysieren. Die gewonnenen Daten werden kommerziell genutzt durch das Einblenden gezielter Werbebanner oder Pop-ups, die an die möglichen Interessen des Internetbenutzers angepasst sind. Die Unternehmen, die Spyware nutzen, erhoffen sich eine Steigerung der Wirksamkeit ihrer Werbemethoden. Um mögliche juristische Probleme zu vermeiden, kennzeichnen viele Anti-Spyware-Programme die ermittelten Softwarekomponenten als möglicherweise unerwünschte Software (potentially unwanted software (PUS)).

Spyware wird meist für Unternehmen programmiert. Mitunter werden ganze Entwicklungsabteilungen damit beauftragt. Sie hat daher häufig ein sehr hohes technisches Niveau. Beispielsweise schützt sich Spyware gegen Löschung dadurch, dass mehrere Prozesse gleichzeitig laufen, die bei Beendigung sofort einen neuen Prozess starten und sich selbst kopieren. Auf der Festplatte entziehen sie dem Administrator die Schreib- und damit die Löschberechtigung.

Ein weiteres Problem entsteht dadurch, dass Spyware zusätzliche Sicherheitslöcher in einem System erzeugen kann, die dann sicherheitsrelevante Software-Updates verhindern. Diese Verfahren machen es selbst technisch versierten Benutzern extrem schwer, sich der Spyware zu entledigen. Antivirensoftware-Hersteller haben Lösungen gegen Spyware entwickelt.

Bei kostenlosen Downloadversionen von Programmen sollten deren AGB (Allgemeine Geschäftsbedingungen) genau beachtet werden, da viele Spywarehersteller aus rechtlichen Gründen dazu übergegangen sind, die Zustimmung des Benutzers über ihre AGB zu erwirken.

Phishing und Pharming

Phishing werden Versuche genannt, über gefälschte WWW-Adressen Daten eines Internet-Benutzers zu erlangen. Der Begriff ist ein englisches Wortspiel, das sich an fishing („Angeln“, „Fischen“) nach Passwörtern anlehnt. Eine Weiterentwicklung des klassischen Phishings, welches meist nur in kleinem Stil betrieben wird ist das sogenannte Pharming. Der Begriff Pharming rührt von dem Umstand, daß hier von den Betrügern große Server-Farmen unterhalten werden, auf denen gefälschte Webseiten abgelegt sind. Im Folgenden werden beide Betrugsversuche nur noch Phishing genannt. Beim Phishing handelt es sich um kriminelle Handlungen, die Techniken des Social Engineering verwenden. Phisher geben sich als vertrauenswürdige Personen aus und versuchen, durch gefälschte elektronische Nachrichten an sensible 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.

Im Allgemeinen beginnt eine Phishing-Attacke mit einer persönlich gehaltenen, offiziell anmutenden E-Mail oder einem Massenversand von E-Mails, wobei der Empfänger stets mit "Sehr geehrter Kunde" angesprochen wird anstatt mit dem eigentlichen Namen, welcher normalerweise der Bank bekannt ist. Der Empfänger soll eine betrügerische Website besuchen, die täuschend echt aussieht und unter einem Vorwand zur Eingabe seiner Zugangsdaten auffordert. Meistens wird das Opfer in falscher Sicherheit gewiegt, indem im Text das Problem des Datendiebstahls thematisiert wird und die Ausfüllung des Formulars nötig sei, damit ein „neuartiges Sicherheitskonzept“ wirksam werden kann und zusätzlich mit der Sperrung von Konto oder Kreditkarte bedroht, falls die gewünschten Daten nicht innerhalb weniger Tage übermittelt werden. Folgt er dieser Aufforderung, gelangen seine Zugangsdaten in die Hände der Urheber der Phishing-Attacke. Was dann folgt, soll nur noch nachträgliches Misstrauen des Opfers zerstreuen. Eine kurze Bestätigung oder eine falsche Fehlermeldung. Eine andere Variante bindet ein Formular direkt innerhalb einer HTML-E-Mail ein, das zur Eingabe der vertraulichen Daten auffordert und diese an die Urheber sendet. Auf eine Phishing-Website wird hierbei verzichtet.

Die gefälschten Zielseiten haben meistens gefälschte Namen oder Bezeichnungen, die ähnlich klingen wie die offiziellen Seiten oder Firmen. Die Zielseiten mit dem Webformular haben das gleiche Aussehen wie die Originalseiten. Sie sind also nur sehr schwer als Fälschungen identifizierbar. Besonders schwer zu erkennen ist die Verwendung von Buchstaben aus anderen Alphabeten. So unterscheidet sich z. B. das kyrillische „а“ optisch in keiner Weise vom lateinischen „a“. http://www.beispielbank.example.com/ Falls das „а“ in „bank“ kyrillisch dargestellt wird, ist die Adresse unterschiedlich und somit falsch. Allerdings zeigt die Adresszeile des Browsers keinen offensichtlichen Unterschied zur Original-Bankadresse.

Da die HTML-Darstellung und der Einsatz von Scripten bei den meisten Phishing-E-Mails eingesetzt werden, sollte man bei seinem E-Mail-Programm die HTML-Darstellung sowie Java-Script deaktivieren. Auch sollten eigene E-Mails immer reiner Text versendet werden, damit auch der Empfänger in seinem E-Mail-Programm die HTML-Darstellung deaktivieren und sich so vor Phishing-E-Mails schützen kann.

E-Mail-Programme wie z. B. Mozilla Thunderbird und Browser wie Mozilla Firefox (ab Version 2.0) oder Opera (9.10) warnen vor Phishingseiten. Der Phishingschutz basiert dabei entweder auf einer Blacklist, welche über das Internet aktualisiert wird, oder es werden typische Merkmale von Phishing-E-Mails wie z.B. Links auf IP-Adressen oder Links mit einem anderem Hostnamen als im Linktext überprüft.

Da jedoch Phishing Mails außer der Frage nach Persönlichen Daten keinem eindeutig identifizierbaren Muster folgen, ist der einzig 100% wirksame Schutz ein gesundes Misstrauen gegenüber dem unsicheren Medium E-Mail sowie das aufmerksame Lesen offiziell anmutender E-Mails. Kein seriöses Kreditinstitut verlangt weder von einem Kunden persönliche Daten per E-Mail zu übermitteln noch wird es androhen innerhalb weniger Tage Kreditkarten oder Konten zu sperren. Ebenfalls wird man in einer authentischen Nachricht keine Formulierung wie „ein Form auszufüllen“ oder „TAN einzutasten“ finden. Mangelhafte Grammatik und Orthographie sind zwar kein ausschließliches Merkmal für oder gegen Phishing, aber auf jeden Fall höchst verdächtig.

Trojanische Pferde

Der Name ist vom Trojanischen Pferd der Mythologie abgeleitet, das dem Angreifer den Zugang zu einem geschützten System verschaffte, indem es als etwas Nützliches getarnt den Angegriffenen dazu veranlasste, es selbst in den geschützten Bereich zu bringen. Durch die gebräuchliche Kurzform „Trojaner“ wird die mythologische Herkunft des Begriffes genau genommen verkehrt, da die Griechen die Angreifer waren, welche das Pferd bauten und benutzten, die Trojaner (also die Bewohner Trojas) hingegen die Angegriffenen.

Trojanische Pferde sind Programme, die im Allgemeinen gezielt auf fremden Computern eingeschleust werden und dem Anwender nicht genannte Funktionen ausführen. Sie sind als nützliche Programme getarnt, indem sie beispielsweise den Dateinamen einer nützlichen Datei benutzen, oder neben ihren versteckten Funktionen tatsächlich nützliche Funktionalitäten aufweisen mit denen sie den Andwender ködern.

Viele Trojanische Pferde werden dazu verwendet, um auf dem Computer heimlich ein Schadprogramm zu installieren. Diese Schadprogramme laufen darauf eigenständig auf dem Computer. Das bedeutet, daß sie sich nicht deaktivieren lassen, indem das Trojanerprogramm beendet oder gelöscht wird. Die tatsächliche Funktion der installierten Datei kann beliebiger Art sein. So können u. a. eigenständige Spionageprogramme auf den Rechner gelangen (z. B. Programme, die die Festplatte ausspionieren und gefundene Informationen weiterleiten, sogenannte Sniffer oder Programme, die die gedrückten Tastenfolgen abspeichern und weiterleiten, sogenannte Keylogger). Auch die heimliche Installation eines Backdoorprogramms ist möglich, welches es gestattet, den Computer über ein Netzwerk (z. B. das Internet) fernzusteuern, ohne dass der Anwender dies kontrollieren kann. Weil Trojanische Pferde häufig solche schädlichen Programme installieren, besteht das Missverständnis, dass erst die Funktionen der installierten Programme ein Trojanisches Pferd ausmachen. Trojanische Pferde müssen jedoch nicht notwendigerweise ein Schadprogramm bestimmter Art installieren. Sämtliche Programme, die etwas anderes tun, als dem Anwender angegeben wird, werden als Trojanische Pferde bezeichnet, ungeachtet der Tatsache, ob sie eine Backdoorfuntkionalität beinhalten und fremden Zugriff verschaffen, nur Anwenderdaten sammeln oder Werbung einblenden.

Trojanische Pferde können über jeden Weg auf einen Computer gelangen, mit dem Daten auf den Computer gebracht werden. Insbesondere über Netzwerkverbindungen wie das Internet (z. B. Tauschbörsen, präparierte Webseite, Versand durch E-Mails). Im Unterschied zu einem Computervirus fehlt dem Trojanischen Pferd die Eigenschaft, sich selbständig zu verbreiten. Die Verbreitung des Trojanischen Pferdes erfolgt **durch den Anwender des Computers selbst**. Je nach Bedeutsamkeit des Scheinprogramms steigt die Wahrscheinlichkeit, dass der Anwender das Programm an weitere Anwender weitergibt.

Viele Antivirenprogramme erkennen eine Vielzahl bekannter Trojanischer Pferde. Da es einem Trojanischen Pferd jedoch im Allgemeinen an einer offensichtlichen Schadroutine fehlt (das Antivierenprogramm kann nicht entscheiden, ob das Computerprogramm, welches aus dem Internet heruntergeladen und installiert werden soll nützlich und gewollt oder schädlich ist) können Antivierenprogramme nie einen vollständigen Schutz vor Trojanern bieten.

Den einzig wirkungsvollen Schutz vor Trojanischen Pferden bietet der Verzicht auf die Benutzung von Programmen aus unbekannten oder unsicheren Quellen. Als besonders gefährlich einzustufen sind hierbei, wie bei jeder Malware, Anbieter von Programmen bzw. Dienstleistungen am Rande der Legalität.

Antiviren Software

(auch Virenscanner oder Virenschutz genannt, Abkürzung: AV) ist eine Software, die bekannte Computerviren, Computerwürmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.

Arbeitsweisen

Der **Echtzeitscanner** (engl. on-access scanner, real-time protection, background guard u.a.), auch Zugriffsscanner oder residenter Scanner genannt, ist im Hintergrund aktiv und scannt alle Dateien, Programme, den Arbeitsspeicher und evtl. den HTTP- wie den FTP-Verkehr. Um dies zu erreichen, werden so genannte Filtertreiber vom Antivirenprogramm installiert, welche die Schnittstelle zwischen dem Echtzeitscanner und dem Dateisystem bereitstellen. Um die Leistung des Computers nicht zu beeinträchtigen wird im Allgemeinen nur der Schreibvorgang gescannt. Damit werden nur neu ankommende Dateien gescannt und nachdem sie als unbedenklich eingestuft wurden im System zugelassen.

Der alleinige Einsatz eines Echtzeitscanners bietet keinen vollständigen Schutz vor Malware, da die meisten Virenscanner nicht sehr erfolgreich beim Erkennen anderer Arten bösartiger Software als Viren und Würmer sind. Auch sind sie meist nur in der Lage, solche Malware zu erkennen, für die sie Virensignaturen erhalten haben. Befindet sich jedoch eine vom Antivirenprogramm erkannte virulente aber unaktivierte Datei auf dem Computer, die vor dem entsprechenden Update der Virensignatur heruntergeladen wurde, kann sie das System bzw. evtl. das Netzwerk nicht infizieren, wenn sie durch den Benutzer ausgeführt (geöffnet) wird, falls alle Dateien auch beim Öffnen überprüft werden.

Um die Belastung durch den Echtzeitscanner weiter zu verringern, werden oft einige Dateiformate, komprimierte Dateien (Archive) oder Ähnliches nur zum Teil oder gar nicht gescannt. Daher sollte trotz eines Echtzeitschutzes regelmäßig ein manueller Scan durchgeführt werden.

Der **Manuelle Scanner** (engl. on-demand scanner) muß vom Benutzer von Hand gestartet werden (On-Demand). Da der Festplattenscan regelmäßig ausgeführt werden sollte, bieten die meisten Programme hierfür bestimmte Assistenten an, die den Rechner in vorgegebenen Zeitabständen regelmäßig und automatisch durchsuchen.

Als **Online-Virenscanner** werden Antivirusprogramme bezeichnet, die ihren Programmcode und die Viren-Muster über ein Netzwerk (online) laden. Sie arbeiten im Gegensatz zu fest installierten Virenscannern nur im On-Demand-Modus. Das heißt der persistente Schutz durch einen On-Access-Modus ist nicht gewährleistet. Deshalb eignen sich Online-Virenscanner zwar zum Reinigen, nicht aber zum präventiven Schutz eines Systems. Auch besteht die Gefahr, dass ein befallener Rechner über die Verbindung zum Internet ferngesteuert werden kann oder selbst Spam versendet oder andere Rechner angreift, während er für den Scan online ist. Daher sollte man ein potenziell befallenes System nach Möglichkeit umgehend vom Netz trennen und mit einem Offline-Scanner untersuchen. Oft werden Online-Virenscanner auch als sogenannte Second-Opinion-Scanner benutzt, um sich zusätzlich zum installierten Virenscanner eine „zweite Meinung“ zu evtl. Befall einzuholen.

Aufgrund der ständigen Weiterentwicklung von Malware (Viren, Würmer, Trojaner etc.) und der Unvorhersehbarkeit der eingesetzten Schadlogik kann praktisch kein Virenscanner vor allen erdenklichen Viren und Würmern schützen. Virenscanner sollten daher generell nur als Ergänzung zu allgemeinen Vorsichtsmaßnahmen betrachtet bzw. eingesetzt werden. Vorsicht und aufmerksames Handeln sind deshalb für verantwortungsvolle Computernutzer trotz des Einsatzes eines Virenscanners unabdingbar.

Erkennungstechnik

Reaktiv: Bei dieser Art der Erkennung wird ein Schädling erst erkannt, wenn eine entsprechende Signatur seitens des Herstellers der Antivirensoftware zur Verfügung gestellt wurde. Dies ist die klassische Art der Virenerkennung, welche von praktisch jeder Antivirensoftware verwendet wird. Hierbei ist es außerordentlich wichtig regelmäßig, am besten täglich, die aktuellen Virensignaturen zu aktuallisieren.

Proaktiv: Dies bezeichnet die Erkennung von Viren, ohne dass eine entsprechende Signatur zur Verfügung steht. Aufgrund der rapiden Zunahme neuer Malware ist davon auszugehen, dass die Zukunft der Virenerkennung in dieser Technik liegt. Proaktive Verfahren sind etwa die Heuristik oder die SandBox Technologie.

Findet ein Virenscanner eine befallene oder verdächtige Datei auf dem durchsuchten Rechner, fragt er in der Regel den Benutzer nach dem weiteren Vorgehen. Die Optionen sind meist das Löschen der Datei, das Verschieben in die Quarantäne oder, wenn möglich, ein Reparaturversuch.

Bezugsquellen

Mittlerweile sind hervorragende kostenfreie Antiviren Programme für jedes Betriebssystem erhältlich, zum Beispiel das auch auf Deutsch verfügbare AntiVir von Avira (www.free-av.de) für Windows, Linux und Solaris oder Clam AntiVirus des gleichnamigen Herstellers für Mac OS. Da derzeit noch keine Viren existieren die das Mac OS System befallen, gibt es nur diesen einen Virenscanner für dieses System. Der Clam AntiVirus Virenscanner sucht auch nicht nach Mac OS Vieren, sondern nach solchen, die Windows befallen und wird daher nur auf Computern eingesetzt, die als Dateiserver für Windowssysteme fungieren.

Das Deutsche Handbuch für Avira AntiVir kann unter folgender URL heruntergeladen werden

http://www.antivir-pe.com/freet/index.php?id=20&domain=free-av.de

oder einfacher indem man dem auf der oben genannten Seite unter dem Register Download zu findenden Link folgt.

Ver- und Entschlüsselung

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 in eine „unleserliche“, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird. Als entscheidend wichtiger Parameter der Verschlüsselung werden hierbei ein oder auch mehrere Schlüssel verwendet.

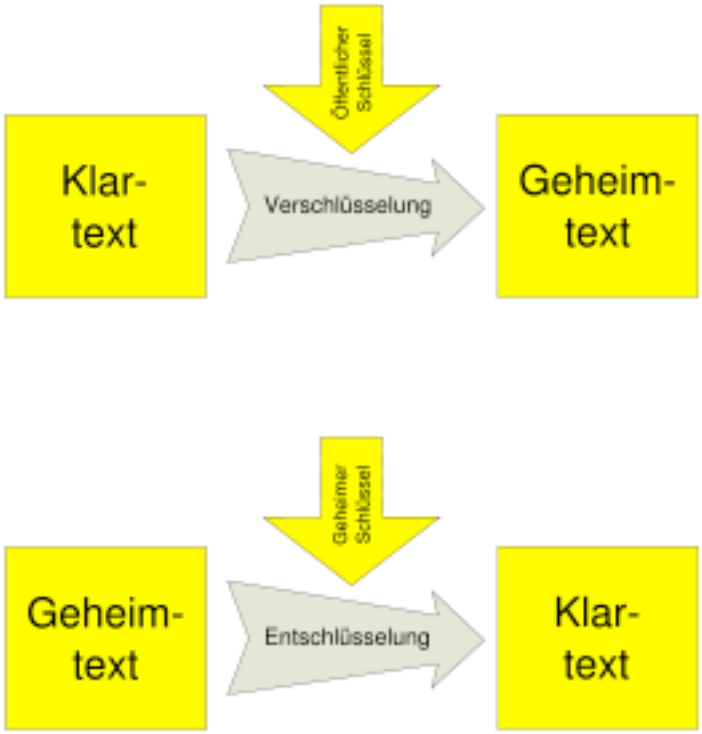
Das wissenschaftliche Forschungsgebiet, das sich mit Verschlüsselungsverfahren und ihrer Geschichte beschäftigt, wird als Kryptografie bezeichnet. Die Kryptografie ist ein Teilgebiet der Kryptologie.

Den umgekehrten Vorgang, also die Verwandlung des Geheimtextes zurück in den Klartext, nennt man Entschlüsselung. Die Algorithmen zur Verschlüsselung und Entschlüsselung müssen nicht identisch sein. Ebensowenig müssen identische Schlüssel für die Verschlüsselung und die Entschlüsselung zum Einsatz kommen.

Sprachlich zu trennen von der Entschlüsselung, also der Tätigkeit des befugten Empfängers einer Geheimnachricht, mithilfe des in seinem Besitz befindlichen (geheimen) Schlüssels, den Geheimtext in einen klar lesbaren Text (Klartext) zurückzuverwandeln, ist der Begriff „Ent-

zifferung“. Als Entzifferung wird die Kunst bezeichnet, dem Geheimtext seine geheime Nachricht zu entringen, ohne im Besitz des Schlüssels zu sein. Dies ist die Tätigkeit eines „Codeknackers“ (engl.: codebreaker). Das Forschungsgebiet, das sich mit der Entzifferung von Geheimtexten befasst, heißt Kryptoanalyse (auch Kryptanalyse) und ist neben der Kryptographie das zweite Teilgebiet der Kryptologie. Die Kryptanalyse dient dabei nicht ausschließlich nur zur unbefugten Entzifferung von geheimen Nachrichten, sondern sie befasst sich auch ganz wesentlich mit der Prüfung der Wirksamkeit und Sicherheit kryptografischer Verfahren.

In der Geschichte wurden vielzählige symetrische Verschlüsselungsverfahren verwendet (siehe Cäsar-Schlüssel, Atbash-Substitution oder Vigenère-Verschlüsselung). Hier wurde der Schlüssel zum ver- und entschlüsseln verwendet. Was den Nachteil hatte, das der nicht nur die verschlüsselte Nachricht, sondern auch der Schlüssel übermittelt werden musste und somit kompromitiert werden konnte.



Heute wird im allgemeinen auf asymetrische Verfahren zurückgegriffen. Bei der asymmetrischen Verschlüsselung besitzt jeder der kommunizierenden Parteien ein Schlüsselpaar, das aus einem geheimen Teil (privater Schlüssel) und einem nicht geheimen Teil (öffentlicher Schlüssel) besteht. Der private Schlüssel ermöglicht es seinem Inhaber z. B., Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentifizieren. Der öffentliche Schlüssel ermöglicht es jedermann, Daten für den Schlüsselinhaber zu verschlüsseln, dessen digitale Signaturen zu prüfen oder ihn zu authentifizieren. Asymmetrische Verschlüsselungssysteme werden daher auch als Public-Key-Verfahren bezeichnet. Im Gegensatz zu einem symmetrischen Verschlüsselungssystemen müssen die Parteien nun keinen gemeinsamen Schlüssel mehr verwenden und es muß kein Schlüssel mehr übertragen werden.

Anwendung

Ver- und Entschlüsselung wird hauptsächlich im Bereich Email eingesetzt. Es gibt für die meisten gängigen Email Programme zusatzsoftware um Emails verschlüsselt zu versenden oder verschlüsselt empfangene Emails zu Entschlüsseln. Die bekannteste freie Applikation ist GPG oder GnuPG (GNU Privacy Guard). Dieser kann zum Beispiel im Mailprogramm Thunderbird integriert werden und per Menüfunktion Nachrichten ver- oder entschlüsseln. GPG ist für Windows, Linux und Mac OS verfügbar und unter der URL http://www.gnupg.org/ erhältlich. Eine ausführliche Anleitung zur Installation von GPG für das Thunderbird Email Programm ist unter http://uckanleitungen.de/thunderbird/gnupg-verschluesselung/ zu finden.

Sichere und unsichere Passwörter

Zu allererst sollte gesagt werden, das es kein 100% sicheres Passwort gibt. Jedes noch so ausgeklügelte Passwort kann mit genügend Zeit und Rechenleistung kompromitiert werden. Jedoch gibt es Passwörter, bei denen dies nur Minuten dauert und andere für die Zeit in Größenordnungen von Jahren bzw Jahrzehnten oder sogar Jahrhunderten investiert werden müsste. Letztere werden als Sicher angesehen, weil davon ausgegangen wird, das zum einen nimand in solchen Größenordnungen Zeit zum herausfinden eines Passwortes investiert und zum anderen Passwörter nach kürzerer Zeit geändert werden.

Passwörter, die einfach kompromitiert werden können entstehen eigentlich immer durch Bequemlichkeit der Benutzer. Menschen neigen dazu, Dinge schneller zu vergessen, die keinen Bezug zu ihrer Lebenswirklichkeit haben. Deshalb verwenden viele den Namen von Ehepartnern, Freund oder Freundin, Kindern, Haustieren, Eltern etc. als Passwort. Auch das Hobby, die Automarke, das Lieblingsessen oder der Titel eines gerade gelesenen Buches müssen zu diesem Zweck herhalten. All diese Passwörter, die in einem Wörterbuch oder einer Namensliste gefunden werden können, sind höchst unsicher. Die Wahl der Sprache spielt dabei nur eine untergeordnete Rolle, obwohl klar sein sollte, dass englische Wörter und Wörter in der Muttersprache des Benutzers (sofern bekannt) eher unsicher sind, als beispielsweise Wörter in Kisuaheli. Dennoch existieren auch für die exotischsten Sprachen elektronische Wörterbücher. Diese Wörterbücher können dazu verwendet werden Passwörter durch ausprobieren der Wörterbucheinträge herauszufinden.

Ein klein wenig sicherer sind Wörter in denen mit der Groß- und Kleinschreibung variiert wird, obwohl auch dies kein allzu großes Hindernis darstellt. Letztendlich kann auch „reGeNScHirM“ in einer kurzen Zeit entdeckt werden. Ein englisches Wörterbuch enthält etwa 150.000 Wörter, nimmt man Abweichungen in der Groß- und Kleinschreibung hinzu kommt man auf etwa 15 Millionen Wörter. Mit der geeigneten Software reichen hier wenige Sekunden zum Brechen des Passwortes aus. Auch bei der Verwendung Wörterbücher mehrerer Sprachen kommt man nicht über ein paar wenige Stunden zum Brechen eines solchen Passwortes. Bei einer Umfrage im Jahr 2001 unter 1200 britischen Büroangestellten wurde festgestellt, dass fast die Hälfte der Befragten ihren eigenen Namen, den Namen von Haustieren oder von Familienangehörigen als Passwörter verwendet hatten. Andere verwendeten Namen wie „Darth Vader“ oder „Homer Simpson“. 2002 wurde eine Liste mit 10.000 Accounts eines existierenden Servers durch ein Programm zum Brechen von Passwörter analysiert. Bereits nach einer halben Stunde waren 30 Prozent der Passwörter ermittelt.

Beliebte Passwörter sind außerdem Zeichenketten, die Muster wie „qwertz“ oder „12345“ aufweisen und daher besonders leicht zu tippen sind. Trotzdem solche Passwörter in keinem normalen Wörterbuch auftauchen sind sie äußerst unsicher, da sie allgemein bekannt sind und es Wörterbücher eigens für solche Musterketten existieren.

Auch ein Passwort, das aus einer zufälligen Buchstabenkette besteht, jedoch zu kurz ist, ist unsicher. Moderne Computer sind leistungsfähig genug um zum Beispiel 10 Millionen Schlüssel des Verschlüsselungsalgorithmus RC5 pro Sekunde auszuprobieren. RC5 gilt zur Zeit als einer der Sichersten Verschlüsselungsalgorithmen. Stellt man dieser Zahl Passwörter mit einer Länge von 6 Buchstaben (Groß- oder Kleinschreibung) gegenüber, kann man ohne großen Aufwand die benötigte Zeit zum Brechen errechnen:

52 mögliche Zeichen (Buchstaben, Zahlen, Sonderzeichen) hoch 6 Zeichen Länge ergibt etwa 20 Milliarden Kombinationen. Bei 10 Millionen probierten Schlüsseln pro Sekunde kommt man auf 2000 Sekunden was etwas über einer halben Stunde entspricht.

Zusammenfassend sollten Passwörter die folgenden Eigenschaften aufweisen, um ein akzeptables Maß an Sicherheit zu gewährleisten:

- **Passwörter sollten lang sein (mindestens 8 bis 10 Zeichen)**
- **Passwörter sollten Buchstaben/Zahlen/Sonderzeichen-Kombinationen enthalten**
- **Passwörter sollten keinen erkennbaren Sinn ergeben**

Durch die folgenden Verfahren erhält man hinreichend sichere Passwörter, die trotzdem leichter zu merken sind als willkürliche Buchstabenfolgen:

- Verbindung zweier Wörter oder Silben (mit gemischter Groß/Kleinschreibung) durch ein Sonderzeichen
  (z.B. „4zU&hAUse“, „gHE1m#niS“, „zEIt+f0rM“)
- Die Anfangsbuchstaben eines Merksatzes, am besten mit zusätzlichen Sonderzeichen und Zahlen
  (z.B. „mLksP1nm“ für „manche Leute können sich Passwörter einfach nicht merken“)
- Sinnlose Wörter, die aus aussprechbaren Silben bestehen, idealerweise um Sonderzeichen und Zahlen ergänzt
  (z.B. „dOsil?Ar0n“)

Anmerkung: Verwendet **niemals** eines dieser Beispiele als Passwort!

Warum auch das nicht ausreicht...

Eine beliebte Art der Passwort-Verbreitung ist auch die Mehrfachverwendung von Passwörtern für verschiedene Accounts. Ist z.B. dem Betreiber eines Diskussionsforums mein Passwort bekannt, so kann er – genügend kriminelle Energie vorausgesetzt – hoffen, dass ich das gleiche Passwort für meinen Firmenzugang verwende. Passwörter sollten daher immer nur ein einziges Mal verwendet und häufig gewechselt werden.

Und zum guten Schluß, eine alte Weisheit besagt: möchte man sicherstellen, das ein Geheimnis bewahrt wird, so muß man dafür sorgen, das man nur selber für das Bewahren des Geheimnisses verantwortlich ist. Sobald das Geheimnis einer weiteren Person bekannt ist, kann man nicht mehr sicherstellen, sondern nur noch darauf vertrauen, das die andere Person das Geheimnis bewahrt. Daraus ergibt sich, das Passwörter und/oder PIN-Nummern immer nur einer einzigen Person zugänglich sein sollten.

SHTTP, SSL und sicherer Handel im Internet

SHTTP, HTTPS und SSL

SHTTP steht für Secure Hypertext Transfer Protocol. Es wurde 1995 entwickelt um eine verschlüsselte Datenübertragung über das Hypertext Transfer Protocol (HTTP), also den Datenaustausch zwischen Webserver und Browser im World Wide Web zu erlauben. Da nicht alle Webbrowser SHTTP unterstützten, wurde es nur mit dem Status Experimental eingeführt. Und mittlerweile von dem besseren Hypertext Transfer Protocol Secure (HTTPS) abgelößt. HTTPS überträgt die Daten über einen sicheren SSL/TLS-Tunnel zwischen Server und Client. (mehr zu SSH später). SHTTP dagegen verschlüsselt jede einzelne Anfrage, kapselt dabei jedoch nur die Nutzdaten, die Header dagegen nicht.

HTTPS verändert nicht die übertragenen Daten an sich, sondern stellt eine verschlüsselte Datenleitung zwischen Server und Client zur verfügung. Die komunikation zwischen Server und Client geschieht dann identisch zum normalen HTTP Protokoll.

Der Benutzer baut eine HTTPS-Verbindung auf, indem er entweder auf einen Link mit https://..... klickt, oder die URL entsprechend in seinem Browser einträgt. Der Browser baut daraufhin eine Verbindung über Port 443 zum Webserver auf. Der Webserver präsentiert sein Zertifikat, ein elektronisches Dokument welches ihn identifiziert. Diese Zertifikate werden von zentralen und vertrauenswürdigen Servern im Internet angeboten. Zum Beispiel laufen in vielen Universitäten Zertifizierungsserver. Danach erfolgt die nur für den Webserver lesbare Übertragung des Sitzungsschlüssels. Mit dem nun auf beiden Seiten vorhandenen Sitzungsschlüssel kann eine symmetrische Datenverschlüsselung beginnen.

Zertifizierungsstelle

Eine Zertifizierungsstelle (englisch Certificate Authority, kurz CA) ist eine Organisation, die digitale Zertifikate herausgibt. Ein digitales Zertifikat ist gewissermaßen das Cyberspace-äquivalent eines Personalausweises und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie sie mit ihrer eigenen digitalen Unterschrift versieht.

Vorbereiten der CA

1. Generieren eines Schlüsselpaares für die CA
2. Verteilen des CA-Zertifikates auf alle Browser

Vorbereiten des Webservers

3. Generieren eines Schlüsselpaares für den Webserver
4. Zertifizierung des Webservers nach Prüfung durch die CA

Unsymmetrischer Sitzungsaufbau

1. Aufbau der Verbindung https://www.softed.de auf Port 443
2. Übertragen des Webserver-Zertifikats zum Browser
3. Prüfen der Signatur des Zertifikats anhand des von der CA hinterlegten Schlüssels, bei Erfolg ist die Identität des Webservers festgestellt
4. Generieren eines temporären Sitzungsschlüssels
5. Senden des Schlüssels in einer nur für den Webserver lesbaren Art
6. Entschlüsseln des Sitzungsschlüssels

Symmetrischer SSL-Tunnel

7. Symmentrische Ver- und Entschlüsselung beim Client
8. Symmentrische Ver- und Entschlüsselung beim Server

Online Banking

Einen guten Schutz gegen Phishing bietet auch das TAN-Verfahren. Eine Transaktionsnummer (TAN) ist ein Einmalpasswort, das üblicherweise aus sechs Dezimalziffern besteht und vorwiegend im Online-Banking verwendet wird. Als Teilnehmer beim Electronic Banking erhält man, meist per Post, eine Liste von Transaktionsnummern. Bei jedem Buchungsvorgang – der Transaktion – muss eine TAN eingegeben werden. Sie ist eine Ergänzung zur Persönlichen Identifikationsnummer (PIN). Falls die Bank nach Eingabe der korrekten PIN einen Buchungsauftrag mit korrekter TAN erhält, geht sie davon aus, dass der Auftrag vom Kunden abgesendet wurde. Die TAN wird von der Bank als Quasi-Unterschrift interpretiert. Sie verfällt nach einmaligem Gebrauch. Wenn die TAN-Liste zur Neige geht, erhält der Kunde von der Bank eine neue.

Eine modernere und sicherere Möglichkeit, Onlinebankingtransaktionen durchzuführen, besteht darin, das signaturgestütze HBCI-Verfahren (Homebanking Computer Interface) mit Chipkarte und autarkem Chipkartenleser zu nutzen. Diese Variante des Onlinebankings ist darüber hinaus sehr komfortabel, da das Vorhalten einer Liste mit TAN-Nummern entfällt. Belauschen der PIN-Eingabe mit einem Keylogger oder Trojaner ist hier nicht möglich. Da die PIN-Eingabe auf einem vom Computer getrennten Gerät geschieht. Somit gibt es keine elektronische Schnittstelle vom Kartenlesegerät zum Computer und somit zum Internet.

Online Einkaufen

Bevor man in einem Online-Shop einkauft, sollte man genau überprüfen, ob man mit einem seriösen Anbieter in Kontakt steht. Man sollte auf alle Fälle immer die auf jeder guten Website enthaltenen Hintergrundinformationen zum betreffenden Unternehmen und die Allgemeinen Geschäftsbedingungen (AGB) gut durchlesen. Werden in den AGB keine unlauteren oder unfairen Abschnitte gefunden und sind neben den elektronischen Kontaktdaten auch Adresse und Telefonnummern auf der Seite mit angegeben, so kann man davon ausgehen, das man es hier mit einem seriösen Anbieter zu tun hat.

Man sollte darauf achten, dass persönliche Daten nur verschlüsselt übertragen werden! Einer Übertragung von Kontonummern oder Passwörtern im Internet sollte nur zugestimmt werden, wenn der Anbieter die Daten verschlüsselt. Das erkennt man an dem im vorherigen Kapitel besprochenen "https" in der Internetadresse. Oft erscheint auch ein Sicherheitsschloss oder ein Schlüssel als Symbole in der Statusleiste.

Weiterhin sollte sichergestellt werden, das Einwahldaten bei technischen Schäden am PC nicht verloren gehen. Insbesondere Informationen rund um Finanzen sollten nicht nur auf der Festplatte des PC, sondern auch auf anderen Speichermedien und wenn möglich einfach auf einem Blatt Papier gesichert werden. Ebenfalls ist es sinnvoll, Bestellungen bzw. Rechnungen auszudrucken und aufzubewahren.

Verschiedene Zugangsdaten wie Passwörter, PIN und TAN sollten keinesfalls auf dem Rechner abgespeichert werden. Dort könnten sie von Eindringlingen aufgespürt und dann missbräuchlich verwendet werden. Wenn Zugangsdaten auf Papier notiert werden, so sollten diese Informationen an einem sicheren Ort aufbewahrt werden. Zugangsdaten, die aus zwei Elementen bestehen (wie etwa Passwörter und PINs), sollten niemals gemeinsam auf dem gleichen Blatt oder am gleichen Ort aufbewahrt werden.

Beim Surfen im Internet sollte man den Browser generell so eingestellen, dass "aktive Inhalte" wie JavaScript oder ActiveX nicht automatisch ausgeführt werden. Diese können nämlich Sicherheitsprobleme mit sich bringen. Seriöse Onlineshops sollten daher immer auch dann genutzt werden können, wenn die Ausführung solcher aktiver Inhalte nicht gewünscht ist. So sollte etwa die Möglichkeit bestehen, auf Produktpräsentationen mit Java zu verzichten (ein weiteres Indiz für die Seriösität eines Anbieters im Internet).

Prüfen, ob alternative Bestellmöglichkeiten existieren! Ein guter Online-Shop bietet auch die Möglichkeit, Waren telefonisch oder per Fax zu bestellen. So können Sie den Weg über das Internet umgehen, wenn er Ihnen nicht sicher erscheint.

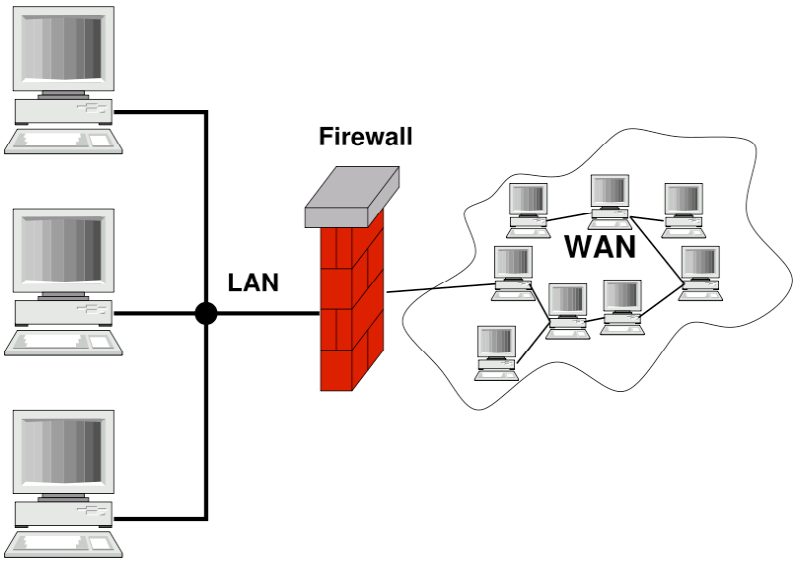
Vorsicht ist geboten wenn E-Mails empfangen werden, in denen zur Aktualisierung der Kundendaten aufgefordert wird. Siehe Kapitel Phishing. Wenn die Website von Geschäftspartnern besucht werden soll, dann gibt man die entsprechende Internetadresse am besten jedes Mal wieder neu ein – dadurch kann man vermeiden, dass Sie von Betrügern auf gefälschte Seiten gelockt werden.

Profiling: Der gläserne Kunde

Wer im Internet surft, hinterlässt Spuren. Durch den Einsatz von Cookies und Data-Mining kann ein genaues Bild darüber gewonnen werden, welche Seiten von welchen Nutzern besucht werden. So können klare Profile von Internetsurfern erstellt werden. Das kann durchaus positive Auswirkungen haben – wenn man etwa nach dem Login auf der Seite eines Webshops schon mit geeigneten Produktangeboten begrüßt wird. Allerdings kann Profiling auch unseriös eingesetzt werden. So verbreitet sich etwa Spyware, also Spionage-Software, die detaillierte Infos über PC-Nutzer erschnüffelt, rasant im Internet..

Firewall

Eine Firewall (von engl. firewall [ˈfaɪəwɔːl] „die Brandwand“) ist eine Netzwerk-Sicherheitskomponente in der Computertechnik. Sie erlaubt oder verbietet Netzwerkzugriffe anhand einer vorher definierten Liste von Regeln. So können zum Beispiel nur bestimmte Programmgruppen (z.B. WWW-Browser oder Email-Cient) erlaubt und alle nicht erwähnten verboten werden. Das Ziel einer Firewall ist, den Datenverkehr zwischen Netzwerksegmenten mit verschiedenen Vertrauens-Stufen abzusichern. Ein typischer Einsatzzweck ist es, den Übergang zwischen einem lokalen Netzwerk (LAN) (hohes Vertrauen) und dem Internet (kein Vertrauen) zu kontrollieren.



Eine Firewall besteht aus Soft- und Hardwarekomponenten. Hardwarekomponenten einer Firewall sind Rechner mit mehreren Netzwerkschnittstellen, Softwarekomponenten sind beispielsweise Paketfilter oder Proxyserver.

Eine einfachere Version ist die so genannte Personal Firewall. Hier wird keine eigenständige Hardware eingesetzt sondern eine Software auf dem jeweiligen zu schützenden Rechner. Diese verhindert ebenfalls anhand eines vorher definierten Regelwerkes das unautorisierte Programme vom Computer aus Zugriff auf das Internet (z.B. Spyware oder Backdoors) oder das unautorisierte dritte aus dem Internet Zugriff auf den Computer erhalten (z. B. Würmer und Vieren).

Personal Firewall

Personal Firewalls bilden oftmals einen Teil der Absicherung privater PCs mit Internetzugang. Am weitesten verbreitet ist derzeit wohl die in Windows integrierte Firewall. Seit Anfang 2006 wird jedoch in diversen Fachzeitschriften darauf hingewiesen, das eine Personal Firewall nur gegen Schädlinge hilft, die sich nicht die Mühe machen, sich zu verstecken. Den Schutz gegen solche Schädlinge sollte jedoch schon der hoffentlich installierte Echtzeit Virenscanner (oder auch Virenschild, siehe Kapitel Antiviren Software) gewährleisten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bemerkt, das regelmäßig aktualisierte Viren- und Spywarescanner und konsequente Datensicherungen wichtiger als einer Personal Firewall sind. Ebenfalls sollten Betriebssystem und Programme nach bekannt werden von Sicherheitslücken schnell mit den nötigen Updates versehen werden.

So steht der sinnvolle Nutzen von Personal Firewalls seit jeher in der Diskussion. Sicherheitslücken werden durch nicht vertrauenswürdige oder fehlerhafte Software verursacht, oder durch deren unsachgemäße Konfiguration. Es ist der falsche Weg, diesem Sicherheitsproblem durch Hinzufügen zusätzlicher Software zu begegnen, die ebenfalls fehlerhaft oder fehlkonfiguriert sein könnte. Personal Firewalls erhöhen die Komplexität des Gesamtsystems und

somit dessen Angriffsfläche. Zusätzlich verringert eine Personal Firewall viele Ressourcen und behindert einen reibungslosen und schnellen Ablauf der Netzverbindungen.

Konfiguration

Die Schutzwirkung, die sich mithilfe einer Personal Firewall erzielen lässt, hängt zu einem hohen Grad von deren sachgemäßen Konfiguration ab. Die Grundeinstellungen eignen sich häufig nicht für den vom Benutzer gewünschten Einsatzzweck. So stellt beispielsweise ein Fernwartungszugang beim Einsatz der Personal Firewall auf einem Einzelplatzrechner mit Internetzugang nur ein unnötiges Risiko dar. Die meisten, aber keineswegs alle Produkte blockieren in den Grundeinstellungen den Zugriff von außen auf die vom Rechner angebotenen Netzwerkdienste. Bei der Tiny Personal Firewall muss diese Paketfilterfunktion erst vom Benutzer aktiviert werden, wenn sie benötigt wird.

Mithilfe der Rechtetrennung des Betriebssystems lässt sich die Schutzwirkung einer Desktop Firewall erhöhen. Wird zum Surfen im Internet ein eingeschränktes Benutzerkonto verwendet, läuft Schadsoftware, die dabei unbeabsichtigt ausgeführt wird, ebenfalls nur mit eingeschränkten Rechten und kann die Konfiguration der Personal Firewall nicht manipulieren.

Sind auf einem Computer mehr als eine Personal Firewall installiert, so ist die Chance hoch, das diese sich gegenseitig behindern, ganz blockieren oder sogar für Systemausfälle sorgen.

Bei der Konfiguration einer Personal Firewall kann nach verschiedenen Grundhaltungen vorgegangen werden: „Erlaubt ist alles, was nicht ausdrücklich verboten ist“ und „Verboten ist alles, was nicht ausdrücklich erlaubt ist“. Letztere Grundhaltung gilt als sicherer, ist aber schwieriger zu konfigurieren.

Für unerfahrene Benutzer wirkt es oft verwirrend, wenn für unbekannte Prozesse nach einer Regel verlangt wird. Manche dieser Prozesse gehören zum Betriebssystem und sind für Internetverbindungen notwendig. Bei der Definition der Regeln nach der zuletzt genannten Grundhaltung werden zunächst so wenige Prozesse wie möglich freigegeben. Funktioniert danach eine Software nicht mehr wie erwartet, so kann das Log nach gesperrten Verbindungen durchsucht werden, um den zu der behinderten Software gehörenden Prozess freizugeben. Bei unbekannten Prozessen empfiehlt es sich, nach weiteren Informationen zu forschen, um zu klären, wozu dieser Prozess gehört.

Windows Firewall

Die Windows Firewall ist Bestandteil von Windows XP und Vista. Seit Windows XP SP2 ist die Windows Firewall in der Standardkonfiguration bereits aktiviert. Sie verwirft eingehende Verbindungen und fragt beim Start von Programmen, die Server-Dienste anbieten, bei Benutzern, die über Administratorrechte verfügen, nach, ob eingehende Verbindungen zu den von diesen Programmen geöffneten Ports erlaubt werden sollen. Sie kann über das Sicherheitscenter konfiguriert werden. Dort können Ausnahmelisten für bestimmte Ports und Programme erstellt werden.

ZoneAlarm

Von ZoneAlarm gibt es eine für Privatanwender kostenlose und eine kommerzielle Version mit einem größeren Funktionsumfang. ZoneAlarm erlaubt getrennte Sicherheitseinstellungen für das lokale Netz und für das Internet. Der Hersteller gibt die Betriebssysteme Windows 2000 Professional oder Windows XP und einen Pentium III Prozessor mit 450 MHz oder höher als Systemanforderungen an. Der Schwerpunkt des Produkts liegt auf einfacher Installation und Konfiguration. Im Januar 2006 geriet ZoneAlarm in den Verdacht, verschlüsselt Daten an den Hersteller zu versenden. Laut Hersteller wurde dieser angebliche Programmfehler mit der Version 6.1.744 vom 1. März 2006 ausgeräumt.

Norton Personal Firewall

Die Norton Personal Firewall ist bis zur Version 2006 als eigenständiges kommerzielles Produkt und als Bestandteil des Softwarepakets „Norton Internet Security“ erhältlich. Norton Internet Security 2007 benötigt laut Hersteller mindestens einen mit 300 MHz getakteten Prozessor, 256 MB Arbeitsspeicher und 350 MB freien Speicherplatz auf der Festplatte. In entsprechenden Foren im Internet werden immer wieder Stimmen laut, die von übermäßigem Ressourcenverbrauch, Schwierigkeiten bei der Deinstallation und Kompatibilitätsproblemen mit anderen Programmen berichten.

Fazit

Da Personal Firewalls nur sinnvoll Arbeiten, wenn sie sehr genau Konfiguriert sind und auch dann Unmengen von Ressourcen verschlingen. Außerdem Aufgaben übernehmen, die vom Virenscanner und einem regelmäßigen Updaten des Betriebssystems und der installierten Programme gewährleistet werden sollten, kann man getrost auf sie verzichten.

Hoaxes

Ein Hoax (engl., Jux, Scherz, Schabernack; auch Schwindel) bezeichnet eine Falschmeldung, die per E-Mail, Instant Messenger oder auf anderen Wegen (z. B. SMS und MMS) verbreitet wird, von vielen für wahr gehalten und daher an viele Freunde weitergeleitet wird. Das Wort kommt wahrscheinlich aus der Verkürzung von „Hokus” aus „Hokuspokus”.

Der Hoax stammt aus England, wo er seit 1796 nachgewiesen ist. Ein typisches modernes Beispiel ist der Good-Times-Hoax, eine angebliche E-Mail, die beim Öffnen die Festplatte löscht. Die Warnung vor diesem „Virus” verbreitete sich 1994 millionenfach über E-Mail und wurde auch von vielen Zeitungen und Fachinstitutionen veröffentlicht. Die damals vermeintliche Gefahr durch Viren, die sich per E-Mail verbreiten, wurde allerdings erst Jahre später Wirklichkeit.

Große Verbreitung finden zum Beispiel so genannte Charity-Hoaxes „Meine Tochter Natalie hat Hirnkrebs und AOL zahlt uns zur teuren, lebensrettenden Operation 5 Cent für jeden Empfänger dieser E-Mail“ oder Kettenemails, die versprechen das alle Versender dieses oder jenes von Microsoft oder einem anderen großen IT-Unternehmen geschenkt bekommen.

Um Interesse und starke Beteiligung am Weiterleiten zu erreichen, beziehen sich die Texte der E-Mail-Kettenbriefe oft auf aktuelle Geschehnisse und benutzen damit die sog. Lokomotiv-Technik, die auch in der Presse als Aufmerksamkeitserreger gebräuchlich ist. In Zeiten etwa, zu denen Energieversorgungsunternehmen besonders in der öffentlichen Kritik stehen, ergeht eine Ketten-Mail, die zum Abschalten aller Stromverbraucher zu einer bestimmten Zeit eines bestimmten Tages aufruft. Auf dem Zug der Tagesereignisse fahrend wendet sich so ein Aufruf etwa an ökologisch engagierte E-Mail-Benutzer. Oft behauptet der Text eine Organisation, die hinter der Aktion stehe, nennt sie aber nicht namentlich oder erwähnt einen erfundenen Namen.

Solch ein E-Mail-Kettenbrief missbraucht das Engagement der E-Mail-Teilnehmer, um eine mehr oder weniger starke und unnötige Netzlast zu erzeugen. Er ist somit keineswegs unschädlich, denn die Netzkapazität muss finanziert werden, und falls sie nicht ausreichend verfügbar ist, wird der Datenverkehr gebremst.

Im erweiterten Sinn kann ein Hoax auch als Computervirus betrachtet werden, der sich durch Social Engineering fortpflanzt. Insbesondere gab es auch schon Hoaxes mit „Schadroutinen“, die den Benutzer aufforderten, bestimmte Dateien zu löschen, da es sich um Viren handele (beispielsweise SULFNBK.EXE und JDBGMGR.exe (der Teddybärenvirus)). Da es sich

jedoch um eine notwendige Systemdatei unter Windows handelt, schädigt der Benutzer sein eigenes System.

Einen sekundären, jedoch nicht vernachlässigbaren Schaden durch Hoaxes erfährt die Wirtschaft. Wenn in einem größeren Betrieb jeder Mitarbeiter sich mit der Hoaxmail beschäftigen muß, sei es nur mit der Entscheidung, das es sich um einen Hoax handelt und dem anschließenden Löschen dieser, werden einige Minuten seiner Zeit in Anspruch genommen. Bei einer Minute pro Mitarbeiter kommen so in einem Betrieb mit 1000 Mitarbeitern schon über 16 Stunden also zwei Manntage zusammen. Entsprechend mehr Zeit wird in Anspruch genommen, wenn die Mail auch noch gelesen wird.

Bevor man der Versuchung nachgibt eine zum Beispiel eine Viruswarnung oder einen Aufruf zum Boykott von Aral an Bekannte und Freunde weiterzuleiten sollte man vorher einmal die Internetseite der Technischen Universität Berlin besuchen und nachsehen ob es sich bei der entsprechenden Email um einen bekannten Hoax handelt oder nicht.

http://www2.tu-berlin.de/www/software/hoaxlist.shtml

Einige dieser Kettenbriefe sind schon seit mehreren Jahren unterwegs, was bei einigen zeitlich begrenzten Inhalten (in zwei Monaten passiert dies oder das wenn nicht wenigstens soundsoviele Personen diese Email bekommen) doch sehr erstaunlich ist.