Sicherheit im Internet

Einführung

In letzter Zeit wird immer öfter über Attacken von Hackern und dem Datenklau im Internet in der einschlägigen Presse berichtet. In der Realität sieht es zwar nicht so extrem aus, wie vereinzelt berichtet wird. Eigentlich sind Angriffe auf Privatpersonen unwahrscheinlich. Jedoch bleibt immer ein Restrisiko.

Viren

Die am häufigsten vorkommende Angriffsform auf Computer sind Viren. Diese Angriffsform ist auch für Privatpersonen beachtenswert. Viren verbreiten sich heutzutage ungehindert über das Internet. Die häufigsten Ansteckungsformen sind verseuchte Downloaddateien und Mailwürmer. Durch einen Virenscanner und ein gesundes Misstrauen kann man sich recht gut gegen Viren schützen. Den Virenscanner sollte man stets aktuell halten und bei E-Mail verdächtige E-Mails nicht gleich pauschal öffnen. Gute Virenscanner haben auch Mailfilter, die z.B. durch H.A.W.K. eine Technologie von McAfee VirusScan ab Version 6.02 verdächtige Aktionen erkennen können. Die Investition in einen guten und aktuellen Virenscanner lohnt sich allemal.
Neben den Mailviren geht auch von Trojanern eine akute Gefahr aus. Diese Viren können eingebaut in Programme wichtige Daten ausspionieren oder Passwörter aufzeichnen. Wenn diese Daten bei der nächsten Onlinesession an den Virenautor versendet werden, so brauchen man sich bei der nächsten Providerauflistung nicht über Onlineverbindungen die nicht einem selbst kommen wundern.

Dialer

Diese verabscheuenswürdigen Programme kann man fast zu den Viren zählen. Diese Angriffsform gewinnt immer weiter an Bedeutung. Dialer installieren sich als neue Standart-Internetverbindung oder manipulieren die bestehenden. Die Einwahl wird über eine 0190-Nummer geleitet, an denen die Autoren Geld verdienen. So kann man schnell unbewusst viel Geld "versurfen". Mit der nächsten Telefonrechnung kommt dann der Hammer. So kann dort bei exzessivem Onlinekonsum schon mal ein Betrag von 500 € stehen. Wenn man keinen Einzelverbindungsnachwei s eingestellt hat, weiss man noch nicht einmal warum.
Solche Dialer kann man sich als Downloaddatei einfangen. So wird suggeriert man würde z.B. einen Film herunterladen, und man lädt jedoch nur den Dialer herunter. Man merkt in solchen Fällen an der Dateigröße, dass es sich um einen Dialer und nicht um einen Film handelt. Kein Film ist gerade mal 50 - 100 KB groß. Auch hat der Dialer die Endung .exe. In solchen Fällen sollte man vorsichtig sein und die Datei nicht ausführen. Auch sollte man in regelmäßigen, möglichst kurzen Abständen die Nummern seiner Wählverbinden überprüfen (ACHTUNG! Einige normale Internetprovider-Einwählnummer haben manchmal auch 019 als Bestandteil. In den Unterlagen vorher nachsehen wie die richtige Einwahlnummer heißt).
Sollte man in der misslichen Lage sein einem solchen Dialer auf den Leim gegangen zu sein sollte man bei der Telekom die Telefonrechnung anzweifeln, Einzelverbindungsnachweis veranlassen und mit dem Einzelverbindungsnachweis und dem unveränderten Computer zur Polizei gehen und dort eine Anzeige wegen Computerbetrugs machen. Wichtig ist, dass man den Dialer, wenn man die teure Telefonrechnung hat, nicht löscht und den Betreiber, trotz allen Ärgers nicht vorwarnt.
Mit Tools wie 0190Warner könnt ihr euch wirksam gegen Dialer schützen
An alle die DSL haben und jetzt Angst haben, da sie eine Flatrate haben, den sei ge-

sagt, dass ausgerechnet sie sich keine Sorgen machen brauchen, da das DSL-System keine Wählverbindungen zulässt und somit der Dialer keinen Schaden anrichten kann.

Ausspionieren durch Portscans

Für Privatpersonen erst an dritter Stelle steht das wirkliche Einbrechen in den Computer. Dies geschieht absolut unbemerkt. Wenn sich der Computer im Internet befindet, befindet er sich in einem Netzwerk. Das dazu gehörige Protokoll verwendet verschiedene Ports. Aber nicht alle Port werden zum Surfen benötigt, so dass diese zwar offen für außen sind, aber nicht genutzt werden. An dieser Stelle setzten Hacker an. Mit sogenannten Portscannern suchen sie nach offenen, unbenutzten Ports am Computer. Diese können für das Ausspionieren, manipulieren und beschädigen des Computers verwendet werden.

Man sollte jedoch nicht hysterisch werden, es ist unwahrscheinlich, dass ein Hacker ein Interesse haben wird, gerade dich als normalen Benutzer auszuspionieren. Was solltest du auch für "geheime" Daten auf deinem Rechner haben. Die Gefahr besteht trotzdem. Um sicher zu sein, sollte man eine Firewall nutzen, die den Verkehr der Ports kontrolliert und unbenutzte versteckt. Eine gute Firewall, wie ZoneAlarm, kontrolliert nicht nur den Verkehr aus dem Internet zum Computer, sondern auch anders herum. Man muss jedem Programm erst vorher erlauben, dass es mit dem Internet kommunizieren darf. Auf diese Weise kann man sich zusätzlich vor Trojanern schützen, die ihre Daten über das Internet an den Autor senden wollen. Sollte sie dies unerlaubterweise tun wollen, schlägt die Firewall Alarm und blockiert den Internetverkehr.

Firewalls zeichnen die IP-Adressen der Angreifer auf. Vor allem ZoneAlarm ist beim abblocken von "Angriffen" manchmal etwas übereifrig. So werden auch ganz harmlose Abfragen von Cookiedaten als Angriff gewertet (wenn bei IE 6 Cookies durch die Einstellung Datenschutz/Hoch eingeschränkt wurden). Sollte jedoch wirklich mehrmals die gleiche IP auftauchen, sollte man die über WHOIS Identität überprüfen, so erhält man eine Info, welchen Provider der Benutzer verwendet. Sollten diese Angriffe anhalten (ACHTUNG! Filesharing-Tools verwenden spezielle Ports! Hier besteht keine Gefahr), solltest du den Provider über die Angriffe informieren. Es kann jedoch auch leider sein, dass dann ein Unschuldiger belangt wird. Gute Hacker bedienen sich eines Tricks und surfen unter fremder IP-Adresse.

Freigaben für jedermann zu lesen

Es hört sich schrecklich an, aber wenn Sie was im Netzwerk freigegeben haben, kann man es auch im Internet lesen. Findige Hacker nutzen das NetBIOS-Protokoll um auf die Freigaben zuzugreifen. Aus Kompatibilität zu älteren Windows-Versionen wird auch heute noch das NetBIOS-Protokoll automatisch aktiviert.

Der Zugriff ist erschreckend einfach: Mit dem von Windows mitgelieferten DOS-Tool nbtstat werden die Freigaben aufgelistet, und schon kann man mit dem Windows-Explorer ganz einfach darauf zugreifen.

Entweder man löst die Aktivierung des NetBIOS-Protokolls oder man sperrt die Ports in der Firewall.

Will man die Aktivierung lösen, so muss man in die ***Netzwerkeigenschaften***, wählt dort ***Eigenschaften*** macht einen ***Rechtsklick auf "Verbindungs ins Internet"*** wählt wieder ***Eigenschaften***, geht aufs ***Internetprotokoll(TCP/IP)*** wählt die ***Eigenschaften*** aus, geht auf ***Allgemein*** und dort auf ***Erweitert***, springt zum Reiter ***WINS***, sucht dort ***NetBIOS-Einstellungen*** und wählt ***NetBIOS über TCP/IP deaktivieren***.

In der Firewall muss man die Ports 135-139 für UDP und TCP schließen.

Lovesan und Sasser Sicherheitslücke immer noch offen

Lovesan oder MSBaster hat uns alle erschreckt, da schafft es doch tatsächlich ein Virus OHNE dass man was macht uns zu infizieren. Nach einem Patch von Microsoft fühlen wir uns wieder sicher. Dann kommt Sasser und nutzt eine ähnliche Sicherheitslücke.
Das präkäre ist, dass Sasser und Lovesan beide eine Sicherheitslücke im RPC-Dienst nutzen. Einen Dienst, der von den wenigsten genutzt wird.
Damit nicht der nächste Wurm eine weitere Sicherheitslücke im RPC nutzen kann wollen wir mal prophylaktisch dessen Ports in der Firewall sperren. Die Ports 135, 139, 445 und 593 sind für UDP und TCP zu sperren. Natürlich kann man danach den Remote-Desktop von WindowsXP nicht mehr nutzen, aber es genügt einfach die Ports wieder für die Dauer des Einsatzes des RPCs zu öffnen.

Professionelles Hacking

Für Privatpersonen eigentlich gänzlich unwahrscheinlich sind DoS-Attacken. Diese können Internetseiten und Unternehmen schwere Probleme bereiten. Bei DoS (Denial of Service) Attacken werden wahllos Anfragen an den Server gesendet, dieser muss alle diese Anfragen verarbeiten. Wenn man nicht nur einen Computer zur DoS-Attacke verwendet, sondern viele (durch Trojaner auch unbeteiligte), dann summiert sich das Datenaufkommen derart, dass der Server überlastet wird und abstürzt. Folge, das Unternehmen/die Internetseite sind vom Netz. Bei der Internetseite heißt das offline, keiner kann die Seite mehr betrachten, beim Unternehmen kann das bedeuten, das alle User des Servers eine "längere Kaffeepause" haben und möglicherweise die Arbeit des ganzen Tages im Datennirwana versunken ist, da oft die Daten erst Abend auf Datenbänder dauerhaft gespeichert werden. Die Folge sind massive Verdienstausfälle. So kann man Unternehmen nachhaltig schädigen. Je nach dem welchen Server man hackt, kann man auch Menschenleben bedrohen (Ampelkontrollzentrum, Flugkontrolle, usw.)

Sonstige Sicherheit

Wir haben zuvor immer sehr krasse und außergewöhnliche Fälle behandelt, bei denen der Computer oder sonstiges Schaden nimmt. Manchmal reicht es aber schon, dass man durch Postwurfsendungen und Massenmails belästigt wird. Vor allem E-Mail können schlimme Dimensionen annehmen, so kann eine Ehefrau eine E-Mail in der einem sexuelle Angebote gemacht werden falsch verstehen. In solchen Fällen ist auch Sicherheit gefragt, diesmal Sicherheit nicht belästigt zu werden, Sicherheit der Identität.
Wenn man heute im Internet surft wird man fast ununterbrochen mit Werbung berieselt, den Werbern genügt es nicht mehr einfach nur ihre Banner in die Webseiten einzubinden. Um ihre Bandbreite und Reichweite der Werbung abzustimmen, werden per Cookie Informationen über den Benutzer gesammelt und gespeichert, so kann man nicht nur persönlich begrüßt, sondern auch persönlich beworben werden. Befehle in Webseiten können inzwischen dem Browser Benutzerdaten entlocken. Damit lassen sich per E-Mail Werbekampagnen koordinieren. Auch Gewinnspiele sind ein guter Weg um an die Adresse des Surfers zu kommen.
Wenn die Spammails immer vom gleichen Absender stammen, kann man diesen bei Freemailern blockieren. Benutzt man einen POP3-Zugang zu seinem Postfach, dann kann man Filterregeln festlegen, nach denen Mails aussortiert werden. Einen besse-

ren Schutz bieten Anti-Spam-Tools wie AntiSpamWare, die zum einen nur die Betreffzeilen der Mails herunterladen können und man so ohne langes herunterladen einige Mails von vorneherein schon auf dem Server löschen kann. Außerdem lassen sich Absender blockieren, es geht sogar soweit, dass AntiSpamWare den Spamversendern eine Fehlermeldung schickt, wonach es die E-Mail-Adresse nicht gibt. 100%igen Schutz gibt es aber nie!!!
Gegen viele Sachen kann man sich nicht so pauschal wehren. Gegen allzu aufdringliche Banner und Popupfenster kann man sich etwas schützen indem man Tools wie den Webwasher verwendet, der diese Flut an Werbung etwas eindämmt. 100%igen Schutz bietet dieses Programm jedoch nicht. Man sollte um allzu viel Post (Snailmail und E-Mail) zu vermeiden mit seiner Adresse knauserig sein und sie nicht an jeden x-beliebigen weitergeben. Eine gewisses Misstrauen ist notwendig. Gegen Cookies kann man sich wehren indem man beim Internet Explorer (ab Version 6) unter Datenschutz den Regler nach oben verschiebt. Man sollte jedoch beachten, dass es dann sein kann dass einige Seiten nicht mehr funktionieren, die die Cookies nicht zum Ausspionieren verwenden, sondern nur für Nutzerdaten oder Sessiondaten beim Onlineeinkauf. Gegen das Entlocken von Browserinformationen kann man sich schwer schützen, Tools wie Anomizer bieten zwar etwas Schutz, ein gläserner Surfer ist man trotzdem.
Wenn man jedoch ein gutes Verhältnis zur Ehefrau hat, wird sie einem glauben, dass alles nur dumme Werbung ist!!!

Schlussworte

Abschließend muss man nochmals darauf hinweisen, dass die beschriebenen Attacken selten Privatpersonen treffen und auch nicht oft durchgeführt werden. Man sollte sich jedoch trotzdem vorsorglich schützen um brenzlige Situationen zu vermeiden. Ein Virenscanner, eine Firewall, ein gesundes Misstrauen und Verständnis von den Arbeitsweisen der Angreifer helfen einem sich gegen diese Attacken zu schützen. Man sollte jedoch den Surfspass nicht verlieren, sich jedoch bei allem Schutze im Klaren sein, dass es 100%igen Schutz nie gibt. Sei für alles bereit, davor sei jedoch relaxed!