Viren, Trojaner und andere Gefahren aus dem Internet, und wie schützt man sich?

Da das Medium Internet das gesellschaftliche Leben widerspiegelt, gibt es auch dort gute und böse Nutzer. Letztendlich möchten die bösen Nutzer mit bösartiger Software Geld verdienen. Dieser Artikel gibt einen Einblick in die „Malware" und beschreibt Lösungen für den Schutz.

Einführung

Immer mehr Menschen benötigen das Medium Internet für berufliche Zwecke oder möchten das gigantische Informations- und Produktangebot für private Zwecke nutzen. Persönliche, vertrauliche Informationen und Dokumente werden heute milliardenfach auf Computern gespeichert oder per elektronischer Post (E-Mail) versendet. Geldtransaktionen zwischen Unternehmen oder die private Online-Überweisung mit dem eigenen Girokonto bzw. Kreditkarte sind heute selbstverständlich und werden von immer mehr Menschen getätigt. Soziale Netzwerke *(engl.: social networks)* wie Facebook, Twitter, XING, YouTube und Co. sind besonders beliebt und verzeichnen einen unglaublichen Mitgliederzuwachs. Da die Computer für diese Kommunikationszwecke am weltweiten Internet angeschlossen sein müssen, sind sie Teil des Internets, also des gesamten Netzes. Theoretisch stehen somit alle Ressourcen des Computers allen anderen Nutzern im Internet zur Verfügung. Genau diese Tatsache scheint aber vielen Menschen nicht bewusst zu sein. Die Gefahr besteht nicht nur in der leichtsinnigen Weitergabe bzw. Bekanntmachung von persönlichen und vertraulichen Daten im Internet, sondern eben auch in der Öffnung des am Internet angeschlossenen Computers für bösartige Software, die Hacker oft mit großer Programmierkunst bekannt machen.

Man kann sogar behaupten, dass Hackerangriffe immer raffinierter und dreister in Erscheinung treten. Man kann sich ja leicht vorstellen, dass dann ahnungslose Bürger ganz schnell und oft unbemerkt in die Falle laufen. Die folgenden Kapitel sollen die Begriffe genau erläutern und abgrenzen.

Was bedeutet der Begriff Hacker?

Hacker *(engl.: Computereindringling)* sind meistens junge und talentierte Softwareexperten (und Sicherheitsexperten), die illegal in fremde Computersysteme eindringen. Die Computersysteme können Großrechner von Banken, Militär, öffentliche Einrichtungen, am Arbeitsplatz bzw. zu Hause stehende Computer und mobile Computersysteme (z.B. Smartphones) sein. Die Hacker verfolgen dabei unterschiedliche Ziele und die Beweggründe können ebenfalls sehr unterschiedlich sein (Spionage, kleine Betrügereien, Bereicherung, Selbstbestätigung, in der Hackerszene bekannt werden, oder einfach Unternehmen aus Jux und Tollerei schädigen).

Doch eines sollte jedoch hier gesagt sein: Intelligente Virenprogramme stellen in der Tat eine hohe Kunst der Softwareprogrammierung dar und erfordern viel Knowhow in der Informatik.

Angriffsarten und Verhaltensweisen von bösartiger Software

Prinzipiell gehört die bösartige Software *(engl.: Malicious Software, kurz Malware)* zu der Kategorie Software, die Computersystem oder auch den Menschen Schaden zufügen (bei Menschen natürlich finanziellen Schaden). Das geht sogar so weit, dass Hacker legale Software in der Art missbrauchen, dass damit illegale Software in Computersysteme eingeschleust wird und Schaden anrichten kann. Im Folgenden soll die Malware genauer betrachtet werden.

Malware

Wie bereits oben beschrieben, ist Malware Schadsoftware, die auf eine bestimmte Art und Weise in Computersysteme gelangen. Hierzu zählen Trojaner, klassische Viren (z.B. Dateiviren), Würmer, von Hackern geschriebene Software-Werkzeuge *(engl.: Tools)* und andere Software, die dann auf kleinen Computersystemen, Großrechnern oder ganzen Computer-Netzwerken ihr schädliches Werk verrichten.

Viren

Sind immer noch die bekanntesten Vertreter von Schadsoftware und werden an Programme (legale Software) oder in einem E-Mail-Anhang angehängt. Hat der Virus den Zielrechner erreicht, aktiviert er sich durch den Programmstart oder das Öffnen des E-Mail-Anhangs und infiziert somit andere Programme auf der Festplatte oder sogar das Betriebssystem des Computers. Im schlimmsten Fall ist jeder Rechner in einem Computer-Netzwerk eines Unternehmens betroffen. Viren kopieren sich selbst und verbreiten sich so auf diese Weise. Damit das auch funktioniert, benötigen die Viren einen sogenannten „Wirt", dessen Code sie manipulieren. Der interne Aufbau eines Computervirus besteht prinzipiell aus drei Modulen: Infektionsroutine, Kopierroutine sowie Statusroutine. Die Statusroutine dient lediglich der Kontrolle und verhindert Mehrfachinfektionen. Im Gegensatz zu Würmern werden von den Viren keine Netzwerkdienste für das Eindringen in fremde Computersysteme verwendet. Der bis heute bekannteste Computervirus war der „ILove You Virus" am 4. Mai 2000. In kürzester Zeit (wenige Stunden) hat er sich mittels Microsoft Outlook-Adressbuch als E-Mail weltweit verbreitet und nach der Aktivierung durch Öffnen des Anhangs großen Schaden angerichtet.

Würmer und E-Mail-Würmer

Im Gegensatz zu den klassischen Computerviren sind Würmer eigenständige Programme, die sich meistens als harmlose Dateien (z.B. Bilddateien) oder Textdokumente tarnen. Für die Verbreitung müssen keine fremde Dateien oder Bootsektoren infiziert werden. Sie werden in den meisten Fällen als E-Mail-Anhang mitgesendet, aber auch mittels anderer Netzwerkdienste wie z.B. Netzwerkprotokolle (der Wurm wird als Datenpaket weitergesendet) zu entfernten Rechnern *(engl.: Remote Computer)* übertragen. Gerade auf den heimischen Computern stellen die Würmer mittlerweile die größte Bedrohung dar.

Bekannte Würmer waren z.B. „MyDoom", „Melissa", „Opasoft" und „Sasser".

Trojaner

Diese Kategorie von Schadprogrammen sind mit Abstand am gefährlichsten. Denn mit ihnen können Hacker ihre bösartige Software in legalen Programmen verstecken. Wird z.B. ein ganz legales Programm von einer Website heruntergeladen und auf dem Computer dann installiert, kopiert oder gestartet, so wird der Trojaner ebenfalls per Huckepack auf den Remote Computer übertragen. Nach Aktivierung (in der Regel selbsttätig) beginnt der Trojaner dann sein bösartiges Werk und kann z.B. als Spionage-Trojaner streng heimliche Dokumente übermitteln oder im schlimmsten Fall kann durch den Trojaner bestimmte Aktionen ferngesteuert werden. Natürlich merkt der ahnungslose Nutzer gar nichts. So können Hacker z.B. an Kontodaten gelangen und Geldbeträge auf ihr eigenes Konto überweisen. Keine Spuren verraten hierbei den Täter.

Bots und Botnetze

Mit Bot- (Bot ist aus dem Wort „Roboter" abgeleitet) bzw. Zombie-Netzen ist es möglich, durch sogenannte „Bot-Programme" (spezialisierte Trojaner) die infizierten Computer (Zombie-Computer) im Zombie-Netzwerk von einem Rechner aus fernzusteuern. Das Bot- bzw. Zombie-Netz dient z.B. als Massenverteiler für Spam-Mails. Mit den Botnetzen können somit in kürzester Zeit Abermillionen Spam-Mails versendet werden. Die Gemeinheit geht sogar so weit, dass die Botnetze an andere Kriminelle vermietet werden können. Die Trojaner steuern die Botnetze und sind Herr über die befallenen Computer.

Eine weitere Möglichkeit, Zombie-Netze einzusetzen, ist das Einschleusen eines sogenannten DDoS-*(engl.: Distributes Denial of Service)* Trojaners in die Computer des Zombie-Netzes. Mittels des DDoS-Trojaners innerhalb des Zombie-Netzes kann so ein entfernter Server regelrecht mit unzähligen Anfragen in Überlast gebracht werden.

Spyware

Mit Spyware *(engl.: Spy = Spion)* werden Programme bezeichnet, mit deren Hilfe das Surfverhalten des Nutzers analysiert (ausspioniert) wird. Somit können den oft ahnungslosen Nutzern ganz gezielt und natürlich vollautomatisch Werbung zugespielt werden. Die Spyware könnte z.B. besuchte Internetseiten so manipulieren, dass der Nutzer gezielt auf bestimmte Online-Shop-Seiten weitergeleitet wird.

Pishing

Als „Pishing" werden Betrugsversuche bezeichnet, mit dem Ziel, an bestimmte Daten (z.B. Zugangsdaten eines Bankkontos) des Nutzers zu gelangen. Als Falle dienen hierbei täuschend echt aussehende Webseiten, auf die der ahnungslose Nutzer hingeführt wird. Der Link einer getarnten Webseite wird meistens innerhalb eines Textes einer täuschend echt aussehenden Unternehmens-E-Mail (Pishing-Mail) platziert. Die E-Mail geht natürlich an tausende Nutzer. Der Nutzer merkt in den meisten Fällen nichts davon, da die Webseiten den originalen Webseiten verblüffend ähnlich sehen. Oft sind es nur winzige Unterscheidungsmerkmale, die eine Pishing-Webseite verraten. Allerdings kann der Link in der E-Mail sehr einfach als falscher Link enttarnt werden. Man braucht lediglich mit der Maus über den Link fahren, um dann die falsche Adresse zu sehen.

Spoofing

Spoofing *(engl.: spoofing = Verschleierung)* ist eine Angriffsart, bei der sich der Angreifer als ein anderer ausgibt, als er tatsächlich ist. Er verschleiert also seine wahre Identität. Es existieren viele unterschiedliche Arten von Spoofing:

- IP-Spoofing: Wird weiter unten ausführlich erklärt.
- DNS-Spoofing (DNS = Domain Name Service): Die Zuordnung zwischen Rechnernamen und der dazugehörigen IP-Adresse werden verfälscht.
- Mail-Spoofing: Bei Mail-Spoofing wird die Absender-Adresse verfälscht.
- ARP-Spoofing (ARP = Adress Resolution Protocol): Der Angreifer leitet Datenpakete in einem Netzwerk um.

Die wohl bekannteste Angriffsart ist das IP-Spoofing. Hierbei werden Datenpakete in Netzwerken so verfälscht, dass die Absenderadresse (IP-Adresse) eine andere als die eigene ist. Die IP-Adresse (IP steht für Internet-Protokoll), die jeder Rechner besitzt, der an einem Netzwerk (z.B. Internet) angeschlossen ist, ist weltweit eindeutig und identifiziert zugleich jeden Rechner. Man kann die IP-Adresse wie eine wahre Absenderadresse eines Briefes ansehen. Der Angreifer kann durch IP-Spoofing natürlich sehr leicht an Informationen bzw. Dokumente gelangen. Der angegriffene Rechner bzw. Nutzer merkt von dem oft nichts.

Wie schützt man sich am besten?

Der wohl wichtigste Schutz ist Kompetenz im Bereich IT und Vorsicht. Es liegt ja klar auf der Hand, dass Unwissenheit und unvorsichtiges Handeln alle Türen für Angreifer öffnen. Ein typisches Beispiel ist das Öffnen von dubiosen E-Mail-Anhängen oder der leichtsinnige Umgang mit Passwörtern.

Ein weiterer Schutz ist auch der richtige Umgang mit wichtigen Daten auf dem Computer. Das bedeutet, dass wichtige Daten immer nochmals gesichert sein sollten und die Verzeichnisse im besten Fall verschlüsselt sind.

Für viele Transaktionen und Zugänge im Internet sind Passwörter gefordert. Der Nutzer sollte unbedingt verschiedene und richtig ausgewählte Passwörter verwenden.

Jeder am Internet angeschlossene Computer sollte ein gescheites Antiviren- und Firewall-Programm installiert haben. Finanzielle Aspekte sollten hier aber keine entscheidende Rolle spielen. Mit billiger Software ist kein richtiger Schutz gewährleistet. Außerdem ist ein regelmäßiges Update der Antivirus-Software unbedingt notwendig.

Auch die Verwendung einer sicheren E-Mail-Software kann die Sicherheit verbessern. Viele Angriffe bedienen sich z.B. der Kontaktdaten von MS-Outlook. Alternative und auch kostenfreie E-Mail-Software gibt es (z.B. Mozilla Thunderbird).

Sichere Internet-Browser spielen ebenfalls eine wichtige Rolle. Durch JavaScript z.B. können Angreifer sehr leicht in das Computersystem eindringen, da JavaScript als Scriptsprache im Browser läuft und auf die Computer-Ressourcen zugreifen kann. Regelmäßige Sicherheitsupdates der Browser-Software sollten unbedingt durchgeführt werden.

Eine weitere Sicherheitsverbesserung besteht darin, dass MS Word-, Excel- und PowerPoint-Dokumente mit einem sogenannten Viewer betrachtet werden können. Makroviren haben dann keine Chance zuzuschlagen.

In sozialen Netzwerken wie z.B. Facebook unbedingt darauf achten, welche Informationen veröffentlicht werden. Vertrauliche Informationen bzw. Daten könnten sonst sehr einfach missbraucht werden. ZT

ZT Adresse

Thomas Burgard Softwareentwicklung & Webdesign
Dipl.-Ing. (FH) Thomas Burgard
Bavariastr. 18b
80336 München
Tel.: 0 89/54 07 07-10
E-Mail: info@burgardsoft.de
www.burgardsoft.de
burgardsoft.blogspot.com
twitter.com/burgardsoft