Schadprogramme

Gefahren lauern überall – auch im Internet. Wer seine Daten nicht schützt, macht es Feinden einfach, diese bei der Übertragung mitzulesen, zu verändern oder sogar zu löschen. Man hört immer öfter von neuen **Viren** oder **Würmern – Programmen** also, die sich selbständig verbreiten oder über E-Mails versandt werden und Schäden auf Ihrem PC anrichten können. Aber auch von **Trojanischen Pferden** ist oft die Rede. Das sind dann Programme, die vom Nutzer unbemerkt sicherheitskritische Funktionen durchführen, indem sie beispielsweise Passwörter abfangen.
Schädliche Programme für den Computer werden heute nicht mehr vorrangig von Einzeltätern geschrieben, die sich damit in ihrer Clique beweisen wollen. Sie sind schon längst von kriminellen Netzwerken abgelöst worden, die international operieren, arbeitsteilig organisiert sind und es auf das Geld der Internetnutzer abgesehen haben.

Die Familie der IT-Schädlinge

Früher nannte man schädliche Programme aufgrund ihrer Eigenschaften meist "Viren". Heute sprechen Experten generell von "Schadprogrammen" und meinen damit alle bösartigen Programme, die auf von ihnen befallenen Rechnern unerwünschte Funktionen ausführen. Viele dieser Schädlinge sind heute modular aufgebaut und können darum häufig nicht eindeutig einer bestimmten Kategorie - etwa Virus oder Wurm - zugeordnet werden. Inzwischen sind diese Programme zudem so raffiniert, dass sie über das Internet automatisch weitere Funktionen nachladen und sich ständig verändern können.
Viele Exemplare haben eine weitere unangenehme Eigenschaft: Sie versuchen, andere Rechner im Internet ebenfalls zu infizieren. Zu diesem Zweck haben ihre Programmierer viele verschiedene Angriffsmethoden, die z.B. Schwachstellen in gängigen Internetbrowsern oder im Betriebssystem ausnutzen, in ihre Schadprogramme implementiert, die vollautomatisch eine nach der anderen ausprobiert werden. Dieses Vorgehen gleicht einem Einbrecher, der nacheinander Türen und Fenster auf Schwachstellen untersucht, um möglichst schnell und unauffällig ins Haus zu gelangen.

So kommen die Schädlinge auf Ihren Rechner

Ganz zu Beginn des PC-Zeitalters waren austauschbare Datenträger wie Disketten oder CD-ROMs die wichtigsten Verbreitungswege für Schadprogramme. Dann kam das Internet und mit ihm die globale Vernetzung von Computern. Das eröffnete den Tätern neue Kanäle zur Verbreitung von schädlicher Software. Zunächst wurden die Schädlinge bevorzugt per E-Mail versandt: Sie verstecken sich in einem Anhang, der dem Empfänger beispielsweise eine nützliche Information verspricht oder angeblich eine Rechnung enthält. Wer diese Datei anklickt, holt sich den Schädling auf seinen Rechner.
Seit einiger Zeit verfolgen die IT-Kriminellen zusätzlich eine neue Strategie: Sie infizieren Webseiten mit schädlichem Code. Es kann vorkommen, dass seriöse populäre Webseiten von Cyber-Kriminellen gecrackt und mit Schadcode versehen werden, beispielsweise über einen eingeblendeten Werbebanner, der von einem anderen Server geladen wird. Wenn Ihr Rechner Schwachstellen hat, reicht es also aus, eine solche Internetseite zu besuchen, um sich einen Schädling einzufangen. Weil der Nutzer davon nichts bemerkt und auch gar nichts weiter dazu beitragen muss - etwa auf eine Datei klicken -, nennt man diesen Infektionsweg Drive-by-Download (also im "Vorbeifahren").
Das darf jedoch nicht darüber hinwegtäuschen, dass die klassischen Verbreitungsmethoden nach wie vor Verwendung finden. Beispielsweise verbreitete sich der bekannte Conficker-Wurm auch über USB-Sticks.
Auch bei Datei-Downloads aus dem Internet ist Vorsicht geboten: In der Flut von Dateien und Gratis-Programmen im Internet verstecken sich zahlreiche Schädlinge. Besonders Raubkopien und Programme für illegale Zwecke (etwa zum unerlaubten "Knacken" kostenpflichtiger Programme) sind häufig mit bösartigen Funktionen verseucht.

Phishing

Gefährliche Umleitung für Ihre Passwörter
Schlimm genug, dass Spammer Ihre Mailbox zumüllen, andere auf Ihrem PC herumschnüffeln wollen oder Computerschädlinge einem die Lust am Internet verderben. Seit einiger Zeit gibt es eine weitere Plage: Phishing. Das klingt nach fischen gehen – und genauso ist es auch. Das Wort setzt sich aus "Password" und "fishing" zusammen, zu Deutsch "nach Passwörtern angeln". Immer öfter fälschen Phishing-Betrüger E-Mails und Internetseiten und haben damit einen neuen Weg gefunden, um an vertrauliche Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern heran zu kommen – die Nutzer geben ihre Daten einfach freiwillig preis. Als seriöse Bank oder andere Firma getarnt fordern die Betrüger den Empfänger in der E-Mail auf, seine Daten zu aktualisieren. Entweder weil z. B. die Kreditkarte ablaufe, das Passwort erneuert werden müsse, die Zugangsdaten verloren gegangen seien oder aus Sicherheitsgründen Kontoinformationen bestätigt werden müssten. Angreifer spekulieren dabei darauf, dass der Empfänger der massenweise verschickten Nachrichten auch tatsächlich Kunde der vorgegebenen Firmen ist. Der Inhalt der so genannten Phishing-Mails wirkt dabei täuschend echt. Diese E-Mails im HTML-Format zeigen dann einen "offiziellen" Link an, hinter dem sich jedoch tatsächlich ein ganz anderer Link verbirgt. Um diesen Link zu entdecken, muss man den Quelltext der HTML-

Mail lesen. Das funktioniert über einen Klick mit der rechten Maus-Taste im Nachrichtenfeld und der Auswahl des Menüpunktes "Quelltext anzeigen".

Trügerische Links und Webseiten

Der Empfänger wird für die Dateneingabe über einen Link auf eine Internetseite geführt, die z. B. der Banken-Homepage ähnlich sieht. Auf den ersten Blick scheint alles ganz normal, selbst die Eingabeformulare sehen gleich aus. Die Phishing-Betrüger nutzen darüber hinaus entweder Internetadressen, die sich nur geringfügig von denen der renommierten Firmen unterscheiden. Oder aber sie fälschen die Adressleiste des Browsers mit einem JavaScript. Man glaubt also, man sei auf einer seriösen Seite, ist es aber nicht. Wer einer solchen Seite seine EC-Geheimnummer, Passwörter oder andere Daten anvertraut, der beschert dem Angler fette Beute und kann sich selbst jede Menge Ärger einhandeln.
Formal gesehen passiert ein solcher Phishing-Angriff also in zwei Etappen, die manchmal auch einzeln auftreten:

1. Da ist zum einen die E-Mail, die ein Vertrauensverhältnis ausnutzt und entweder auf eine bösartige Internetseite lockt oder Computerschädlinge im Schlepptau hat. Diese Mails sind heute übrigens oft perfekt formuliert, während sie zu Beginn der Phishing-Angriffe zumeist in sehr schlechtem Deutsch verfasst waren. Das lag daran, dass sie oft aus dem fremdsprachigen Ausland stammten und mit automatischen Übersetzungsprogrammen oder von Laien ins Deutsche übertragen wurden.
2. Zum anderen gibt es die Nachahmung von Teilen oder einer gesamten vertrauten Webseite, auch "Spoofing" ("Verschleierung") genannt. Hier geschieht der eigentliche Betrug, indem die Angreifer einen getäuschten Nutzer zur Preisgabe vertraulicher Daten verleiten, die dann missbraucht werden.

Maßnahmen gegen Phishing

Ärger haben auch die Unternehmen, in deren Namen die Betrüger auftreten. Denn sie erleiden oft einen Image-Schaden. Phishing zu bekämpfen ist schwer, da sich die gefälschten von den echten Seiten kaum unterscheiden und somit viele Nutzer sich täuschen lassen. In einigen Ländern haben sich viele Firmen bereits zur Anti-Phishing Working Group zusammengetan. Auf ihrer Internetseite kann man Phishing-Mails melden und nachlesen, welche schon bekannt sind. In Deutschland hat sich eine neue interdisziplinäre Vereinigung aus Wissenschaftlern der Ruhr-Universität Bochum des Phishing-Problems angenommen. Die "Arbeitsgruppe Identitätsmissbrauch im Internet" (A-I3) stellt auf ihrem Online-Portal nicht nur aktuelle Informationen zu Themen der IT-Sicherheit bereit, sondern auch konkrete Hilfestellungen und Tools.
Für Sie als Internetnutzer aber heißt es wieder einmal: Aufpassen! Schauen Sie bei den angeklickten Internet-Adressen besser zweimal hin und überlegen Sie genau, wem Sie welche Daten anvertrauen.
Übrigens: Phishing ist nicht nur auf das Internet beschränkt – Datendiebe machen auch Jagd auf die Nutzer über das Telefon unter Verwendung von Internettelefonen (VoIP). Eine eigene Bezeichnung für diese neue Technik gibt es auch schon: "Vishing" ("Voice Phishing").

Botnetze

Und noch so ein seltsames Wort: Botnetz. Der Begriff "Bot" kommt von robot und heißt so viel wie arbeiten. Im IT-Fachjargon ist mit Bot ein Programm gemeint, das ferngesteuert auf Ihrem PC arbeitet. Von Botnetzen spricht man dann, wenn sehr viele PCs – meist mehrere Tausend, es können aber auch mehrere Millionen sein – per Fernsteuerung zusammengeschlossen und zu bestimmten Aktionen missbraucht werden.
Was das alles mit Ihnen zu tun hat? Ganz einfach: Es könnte sein, dass genau Ihr Computer Teil eines Botnetzes ist und jetzt **ferngesteuert** arbeitet – ohne dass Sie davon etwas mitbekommen. Sie sind an dieser Stelle gefordert: Sorgen Sie mit den entsprechenden Schutzmaßnahmen dafür, dass Fremde keine Möglichkeit bekommen, Ihren Rechner in Beschlag zu nehmen und für Angriffe zu missbrauchen.

Wie wird der Computer infiziert?

Wenn Sie im Internet unterwegs sind oder E-Mail-Anhänge öffnen, dann kann es leicht passieren, dass Sie sich schädliche Programme auf Ihren PC herunterladen – es sei denn, Ihr Rechner ist durch entsprechende Maßnahmen geschützt. Zu diesen Schadprogrammen zählen auch **Bots**, die sich still und heimlich auf Ihren PC schleichen. Viele Bots verhalten sich zunächst ziemlich unauffällig, so dass Sie davon nichts bemerken. Doch der Schein trügt. Denn die Verursacher der Schadprogramme können diese per **Knopfdruck aktivieren**. Dazu schicken Sie entsprechende Kommandos an den befallenden PC. Eine einzige kriminelle Person kann alle Bots zentral in seinem Netzwerk dirigieren und ihnen befehlen, die gleichen Aufgaben auszuführen. Voraussetzung dafür: Der PC muss online sein. Ihr PC scheint nun ganz normal zu arbeiten, während sich gleichzeitig im Hintergrund lauter unerfreuliche Dinge abspielen.
Botnetze werden von Cyber-Kriminellen zu bestimmten Aktionen missbraucht. Das können einerseits DDoS-Angriffe sein, um große Internetseiten lahm zu legen. Andererseits wird über Botnetze aber auch SPAM unerkannt versendet. Darüber hinaus werden Botnetze oft gegen Geld an Dritte weitervermietet. Um es auf den Punkt zu bringen: Hinter Botnetzen steckt verdammt **viel kriminelle Energie** und eindeutig ein böser Wille.
Von den Angreifern ausgenutzt werden vor allem Schwachstellen in den Microsoft-Betriebssystemen. Doch auch Benutzer anderer Betriebssysteme dürfen sich nicht in falscher Sicherheit wiegen. Gekaperte UNIX-Server funktionieren beispielsweise oft als Kernstück eines Botnetzes, d. h. sie steuern die befallenen PCs zentral.

Das Problem der Bot-Netze hat im letzten Jahr massiv zugenommen. Der Grund: Immer mehr Nutzer verfügen über einen Breitband-Internetanschluss. Nicht wenige Computer sind rund um die Uhr ans Internet angeschlossen. Immer günstigere Flatrates machen's möglich.
Und im Gegensatz zu analogen Internetverbindungen fällt bei DSL-Anschlüssen kaum auf, ob der Computer "heimlich Dinge macht", weil die Verbindungsgeschwindigkeit nicht merklich langsamer wird. Studien zufolge werden pro Tag weltweit mehrere Tausend neue Computer gekapert und für **fremde Zwecke missbraucht**. Ein neu ans Internet angeschlossener PC wird bereits nach wenigen Minuten erstmals angegriffen.
Die Folge: Durch Botnetze ist Ihr Rechner nicht **mehr nur Opfer**, sondern er wird gleichzeitig auch zum **Täter**. Er erhält die entsprechenden Befehle und führt diese ohne Ihre Kontrolle aus. Auch Ihre, auf dem PC gespeicherten persönlichen Daten sind nun nicht mehr sicher.
In den Medien taucht für Botnetze übrigens immer öfter der Begriff "Zombie-Rechner" auf, weil der Rechner wie ein Zombie – ein willenloses Werkzeug – zum Leben erweckt wird.

Die Gefahr der Botnetze steigt

Laut einer Studie des IT-Sicherheitsunternehmens Trend Micro liegt Deutschland, bezogen auf die Anzahl der mit Bots infizierten Computer, im Ländervergleich auf Platz 3. Mehr infizierte Rechner gibt es nur in den USA (Platz 2) und China (Platz 1).
Diese Zahlen sind alarmierend. Zu befürchten ist, dass die Anzahl der Botnetze weiter steigt, da Cyber-Kriminelle immer neue Arten von Bots, die intelligenter agieren und so länger unentdeckt bleiben, entwickeln. Auch werden in gängigen Programmen ständig neue Lücken und Methoden gesucht, Computer zu infizieren. Hinter den Betreibern von Botnetzen stehen zudem gut organisierte und professionelle Kriminelle, die sich zunehmend vernetzen und weltweit operieren.
Eine weitere Gefahr stellt die Ausbreitung der Botnetze auf weit verbreitete mobile Geräte, wie zum Beispiel Blackberry, iPhone usw., dar.
Gegenmaßnahmen zeigen jedoch bereits Wirkung: Die verstärkte Kooperation zwischen Providern, CERTs und IT-Sicherheitsexperten auch auf internationaler Ebene trägt dazu bei, dass Botnetze schneller aufgedeckt und zerschlagen werden können. Auch Maßnahmen zur Aufklärung und Sensibilisierung der Privatanwender haben dazu geführt, dass Firewalls immer konsequenter eingesetzt und Updates regelmäßig installiert werden.

Spam

Der Name "Spam" ist dem Dosenfleisch SPAM (**S**piced **P**orc and **H**am) der amerikanischen Firma Hormel Foods entliehen (deutsch: Frühstücksfleisch), den es seit 1937 gibt. Im Internetzeitalter ist er zum **Synonym für Massen-E-Mails** geworden.
Wie der Schinken zur Massen-E-Mail wurde, darüber gibt es viele Geschichten. Hormel Foods selbst sagt, es beruhe auf einem Sketch der Comedy-Gruppe "Monty Python". Darin kam der Begriff über 120-mal innerhalb weniger Minuten vor und übertönte jede andere Konversation. Und tatsächlich liegt die Analogie zur Massen-E-Mail damit auf der Hand.
Als Spam, Spamming oder Junk Mail (Müllpost) bezeichnet man im Internet:

- Massenversand nichtangeforderter Werbe- E-Mails
- Werbebeiträge in Newsgroups, die nichts mit dem Thema der Newsgroup zu tun haben.
- Kettenbriefe

Müll und Wurfsendungen in elektronischer Form, die oft kommerzieller Art sind, werden auch **UCE** genannt ("Unsolicited Commercial E-Mails"), was soviel heißt wie "unaufgeforderte Werbe-E-Mails".
Um E-Mails in millionenfacher Menge versenden zu können, benötigen die Spammer Adressen. Diese sind bei Adresshändlern zu bekommen. Oft führen kommerzielle Spammer aber auch Datenbanken mit Millionen von Adressen. Durch das gezielte – mit einem Programm automatisierte – Absuchen von Newsgroups, Homepages oder E-Mailverzeichnissen, aber auch durch Durchprobieren gängiger Adressen (info@… usw.) sind die Adressen schnell erhältlich. Aufgrund der großen Menge spielt es dann auch keine Rolle, wenn viele Adressen ungültig sind. Fast alle Kosten – oder Müllgebühren – müssen Sie als Empfänger und die Provider bezahlen: für die angefallene Downloadzeit und den benötigten Speicherplatz. Der Versand erfolgt meist vollautomatisch über spezielle Programme. Der Spammer muss nur das Programm starten und kann dann einer anderen Tätigkeit nachgehen, während sein Programm Hunderttausende von Leuten belästigt.
Weil Massen-E-Mails für den Spammer relativ kostengünstig sind, lohnt sich das Geschäft bereits, wenn auf fünf Millionen Spams fünf Personen ein Produkt kaufen. Jeder, der solche Spam-Mails erhält, wird merken, dass damit hauptsächlich für Dinge geworben wird, für die es sich nicht lohnt, in andere Werbemittel zu investieren. Entweder ist das beworbene Produkt praktisch wertlos oder aber sogar illegal.
Nach deutschem Recht ist es verboten, Personen unaufgefordert Werbung per E-Mail zuzusenden. Spam ist aber weit mehr als nur ein lästiges Übel: Jedes Jahr entstehen **Kosten in Milliardenhöhe** durch die Übertragungskosten für den Versand, den Zeitverlust für das Lesen, Löschen oder Beantworten dieser elektronischen Belästigungen.
Ärgerlich wird es vor allem dann, wenn Ihre Mailbox zugestopft ist und reguläre Post an Sie aufgrund der Größenbeschränkung Ihrer Mailbox abgewiesen wird. Durch übermäßige Nutzung können Server mitunter sogar abstürzen, was massive Verzögerungen und gravierende Schäden zur Folge hat.

Schutzmaßnahmen

- Verwenden Sie **ein aktuelles Viren-Schutzprogramm**, das auch vor Drive-by-Downloads schützt und auf schon bekannte bösartige Webseiten hinweist. Erkundigen Sie sich dazu am besten beim Hersteller der Schutzsoftware, da einige den Surf-Schutz nur in den kostenpflichtigen Varianten, aber nicht in den freien Versionen zur Verfügung stellen. Installieren Sie unter Windows auch ein Anti-Spyware-Programm.
- Setzen Sie unter Windows eine **Personal Firewall** ein und aktualisieren Sie diese regelmäßig. Sie schützt bei richtiger Konfiguration vor Angriffen aus dem Internet und verhindert zudem bei einer Infektion des PCs mit einem Computerschädling, dass ausspionierte Daten an einen Angreifer übersendet werden können.
- Achten Sie darauf, ob es ***Sicherheitsupdates* für Ihr Betriebssystem und sonstige von Ihnen installierte Software** gibt.
  Damit Schadcode überhaupt ausgeführt werden kann, muss er eine Schwachstelle in Ihrem Browser oder einem anderen Programm finden, die er ausnutzen kann. Spielen Sie daher regelmäßig alle verfügbaren Updates für das Betriebssystem, den Browser selbst und alle anderen Anwendungen (etwa PDF-Reader oder Flash-Player) ein.
- Alle PC-Betriebssysteme bieten die Möglichkeit, sich als Nutzer mit eingeschränkten Rechten oder als Administrator anzumelden. Arbeiten Sie nach Möglichkeit **nicht als Administrator** an Ihrem PC, denn so können Schadprogramme noch mehr Unheil anrichten. Richten Sie für alle Nutzer eines PCs ***unterschiedliche Benutzerkonten*** ein. Vergeben Sie für diese Konten nur die Berechtigungen, die der jeweilige Nutzer für seine Arbeit braucht. So werden auch private Dateien vor dem Zugriff Anderer geschützt. **Speziell beim Surfen sollten Sie nach Möglichkeit immer auf Administratorrechte verzichten**.
- Verwenden Sie einen **Browser mit integrierter Funktion zur Warnung vor als bösartig bekannten Webseiten** und stellen Sie sicher, dass diese Funktion aktiviert ist.
  - In Computerzeitschriften und Online-Medien finden Sie regelmäßig Tests von Browsern, die Ihnen wertvolle Tipps geben können. Entscheiden Sie sich bewusst für einen Browser mit sehr guten Sicherheitseigenschaften. Da die Browser stetig weiterentwickelt werden, überprüfen Sie Ihre Wahl regelmäßig.
  - Beachten Sie unsere Hinweise zur sicheren Konfiguration von Browsern.
- Gehen Sie sorgfältig mit Ihren ***Zugangsdaten*** um. Halten Sie Kennwörter und Benutzernamen sowie Zugangscodes für Dienste (z. B. beim Online-Banking) unter Verschluss. Wechseln Sie Passwörter in regelmäßigen Abständen.
- Seien Sie vorsichtig beim ***Öffnen von E-Mail-Anhängen***. Schadprogramme werden oft über Dateianhänge in E-Mails verbreitet. Im Zweifelsfall fragen Sie vorsichtshalber beim Absender nach, ob der Anhang tatsächlich von ihm stammt.
- Seien Sie vorsichtig bei ***Downloads von Webseiten***. Vergewissern Sie sich vor dem Download von Programmen aus dem Internet, ob die Quelle vertrauenswürdig ist und bringen Sie Ihr Virenschutzprogramm auf den aktuellsten Stand.
- Seien Sie zurückhaltend mit der ***Weitergabe persönlicher Informationen***. Online-Betrüger steigern ihre Erfolgsraten, indem sie individuell auf ihre Opfer zugehen: Zuvor ausspionierte Daten, wie etwa Surfgewohnheiten oder Namen aus dem persönlichen Umfeld, werden dazu verwandt Vertrauen zu erwecken.
- Nutzen Sie Übertragungstechnologien wie Voice over IP (VoIP) oder Wireless LAN (WLAN), dann achten Sie besonders auf eine ***Verschlüsselung Ihrer Kommunikation,*** damit die Übertragung Ihrer Daten nicht von Dritten mitgelesen bzw. Gespräche nicht abgehört werden können.
- Kommt es trotz aller Schutzmaßnahmen zu einer Infektion des PCs mit einem Schädling, können wichtige Daten verloren gehen. Um den Schaden möglichst gering zu halten, sollten Sie regelmäßig ***Sicherungskopien Ihrer Dateien*** auf CD-ROM/DVD oder externen Festplatten erstellen.

Weitere und aktuelle Informationen

Finden Sie unter den Internet-Adressen **www.bsi-fuer-buerger.de** und **www.polizei-beratung.de** (Themen und Tipps → Gefahren im Internet).

Quellennachweis

Alle Texte sind der Web-Site des „Bundesamtes für Sicherheit in der Informationstechnik“ (www.bsi-fuer-buerger.de) entnommen.