Bedrohungen im Internet und mögliche Schutzmaßnahmen

Autor_Thomas Burgard Dipl.-Ing. (FH)

Durch die sozialen Netzwerke und Cloud-Computing wird sich das Internet auch in Zukunft weiter rasant verändern und noch mehr Nutzer für sich gewinnen. Gleichermaßen nehmen aber auch die Bedrohungen aus dem Internet zu. Dieser Artikel gibt einen Überblick über die Gefahren und mögliche Schutzmaßnahmen im Internet.

_Der Branchenverband „Bitkom" hat 2013 eine Top 10-Liste der größten Gefahren im Internet und eine kurze Beschreibung entsprechender Gegenmaßnahmen veröffentlicht hat. Auf Platz 1 steht das unbemerkte Herunterladen von schädlicher Software durch „Drive-by-Downloads". Der Internet-Browser ist hierbei und auch bei anderen Bedrohungsszenarien das Hilfsmittel, um Attacken und das Verbreiten von Schadsoftware zu ermöglichen.

_Drive-by-Downloads von Schadsoftware

Der Internetnutzer besucht eine manipulierte Website und lädt sich unbemerkt schädliche Software auf den eigenen Computer. Hierbei werden Sicherheitslücken von Internet-Browsern oder Browser-Add-ons bzw. Browser-Plugins ausgenutzt. Drive-by-Downloads gelten inzwischen als wichtigster Verbreitungsweg für Computerviren und haben damit sogar die E-Mail verdrängt.

Schutzmaßnahmen

Neueste Versionen der Internet-Browser und Browser-Plugins installieren und verwenden. Dazu gehören auch die Installation der aktuellen Java-, Flash- und Adobe-Reader-Software.

_Trojaner und Würmer

Trojaner sind Computerprogramme, die als normale Anwendung getarnt und im Hintergrund ohne Kenntnis des Nutzers eine andere (schädliche) Funktion durchführt. Ein trojanisches Pferd zählt zur Familie unerwünschter bzw. schädlicher Programme, der sogenannten „Malware".
Computerwürmer sind Computerprogramme oder auch Skripte, die sich ohne Kenntnis des Nutzers im Hintergrund selbst vervielfältigen, nachdem sie einmal gestartet wurden. Sie verbreiten sich im Gegensatz zu Computerviren ohne fremde Dateien. Meist verbreiten sich Würmer über Computernetzwerke und Wechselmedien wie z. B. USB-Sticks.
Trojaner und Würmer sind bereits lange im Einsatz und gehören eindeutig zu den Klassikern unter den Schadprogrammen. Vor allem die Gefährlichkeit von Trojanern steigt wieder, da Cyberkriminelle zunehmend soziale Netzwerke und mobile Plattformen als Verbreitungsweg nutzen. Die Schadsoftware wird völlig unbemerkt in Rechnersysteme eingeschleust und verrichtet dann ihr schädliches Werk. Es werden z. B. eingegebene Passwörter abgefangen und übertragen.
Malware sind Computerprogramme, die dem Zweck dienen, für den Benutzer unerwünschte bzw. schädliche Funktionen auszuführen. Der Begriff Malware fungiert hier als Oberbegriff und umfasst jegliche Computerviren. Als Virenschutz bezeichnet man somit allgemein den Schutz vor Schadprogrammen.

Schutzmaßnahmen

Einen guten, aber keinen absoluten Schutz bieten die jeweils aktuellsten Antivirenprogramme. Es sollte keine Software aus unsicheren oder unbekannten Quellen installiert werden.

_Attacken auf Datenbanken und Websites

Diese Art von Attacken auf Datenbanken werden mittels „SQL-Injection" (dt. SQL-Einschleusung) durchgeführt. Hierbei werden Sicherheitslücken in SQL-Datenbanken ausgenutzt, um eigene Datenbankbefehle in die Datenbank einzuschleusen. Das Ziel ist es, Daten auszuspähen, um die Kontrolle über das Serversystem zu bekommen und so Schaden anzurichten.

Attacken auf Websites werden mittels „Cross Site Scripting" (oft Angriffe auf Websites von Onlinedienst-Anbietern) durchgeführt. Möglich ist aber auch das Auslesen von Log-in-Daten.

Schutzmaßnahmen
Deaktivieren von Javascript und Flash im Internet-Browser. Des Weiteren müssen die Betreiber von Websites die Seiten sehr sorgfältig programmieren und überwachen.

_Viren-Baukästen

Viren-Baukästen, sogenannte „Exploit Kits", sind Computerprogramme, mit denen die Entwicklung von Schadprogrammen sehr gut unterstützt wird und Cyberangriffe automatisiert werden können. Die Programme können Drive-by-Downloads initiieren und nutzen eine Vielzahl weiterer Verbreitungswege, um Computer zu infizieren. Typisch für Viren-Baukästen ist ihre sehr einfache Handhabung, sodass auch Laien die Viren-Baukästen leicht verwenden können.

_Botnetze

Als Botnetz wird ein infiziertes Computernetzwerk bezeichnet, das im Internet verknüpft wird und von einem „Botmaster" gesteuert wird. Aus einem erstellten Botnetz können dann sehr einfach Spam- und Phishing-Mails versendet oder Webserver mit massenhaft versendeten Anfrage-Nachrichten lahmgelegt werden. Außerdem können in einem Botnetz Passwörter und Dateien bzw. Daten gestohlen werden. Das größte bislang entdeckte Botnetz umfasste rund 30 Millionen einzelne Rechner.

Schutzmaßnahmen
Immer aktuelle Versionen von Virenscanner-Software installieren und Firewalls verwenden. Die Webseite www.botfrei.de überprüft, ob der eigene Rechner Teil eines Botnetzes (Zombie) ist und reinigt ihn bei Bedarf.

_Denial of Service Attacken

Denial of Service bedeutet „Verweigerung eines Dienstes". Mit diesen Attacken versuchen Cyberkriminelle Webserver lahmzulegen, damit diese von Nutzern nicht mehr aufgerufen werden können. Erreicht wird das, indem massenhaft Anfrage-Nachrichten an den Webserver gesendet werden, sodass dieser dann durch die steigende Last zusammenbricht. Neben erpresserischen Absichten wird diese Form des Angriffs auch häufig bei Protestaktionen eingesetzt. Die Angriffe können von einem einzelnen Computer oder von vielen ausgeführt werden, zum Beispiel aus einem Botnetz.

Schutzmaßnahmen
Die Abwehr solcher Attacken muss vom Server-Administrator gewährleistet werden, jedoch ist eine Abwehr sehr schwierig, denn die Aufgabe eines Webservers ist ja gerade, Anfragen entgegenzunehmen.

_Phishing

Mit Phishing wird versucht, durch Versenden von E-Mail-Links auf gefälschte Webseiten zu lenken (z. B. gefälschte Bankseiten), um an Kontozugangsdaten, PIN und Transaktionsnummern (TAN) zu gelangen, die auf den gefälschten Seiten von ahnungslosen Nutzern eingegeben werden. Inzwischen senden Kriminelle per E-Mail meist einen Trojaner, der die Daten heimlich ausspäht und überträgt. Angriffsziele sind neben Banken auch Bezahldienste, Online-Händler, Paketdienste oder soziale Netzwerke.

Schutzmaßnahmen
Schutz bietet ein gesundes Misstrauen. Außerdem werden Banken und andere Unternehmen ihre Kunden niemals per E-Mail bitten, vertrauliche Daten auf einer Website einzutragen.

_Datenklau und Datenverluste

Mittels gezielter Hackerangriffe werden Daten und Informationen (z. B. Nutzerdaten, Passwörter etc.) von Servern, die im Internet erreichbar sind, gestohlen und missbraucht. Neben den persönlichen Angaben ist vor allem der Verlust von Kreditkartendaten kritisch.

© Derter

Zudem können sich Hacker mit den gewonnenen Informationen auch bei anderen Diensten mit falscher Identität einloggen. Hauptgründe für Datenverluste sind Hacker-Angriffe und eingeschleuste Schadsoftware. Daneben spielen auch physische Angriffe und das sogenannte Social Engineering eine Rolle. Kriminelle versuchen mit dieser Methode, Zugangsdaten von Unternehmensmitarbeitern zu bekommen (erfragen).

Schutzmaßnahmen
Mit sensiblen Daten prinzipiell äußerst vorsichtig umgehen und niemals anderen (Kunden, Lieferanten, Geschäftspartnern, Fremden usw.) mitteilen.

_Rogueware/Scareware

Diese Art von Computerviren bedienen sich der Mittel Täuschung und Angst. Dem Nutzer wird z. B. eine Infektion seines Computersystems mitgeteilt, die erst gegen Bezahlung behoben wird. Verbreitet sind Schadprogramme, die Logos von Bundespolizei, Landeskriminalämtern oder Institutionen wie der GEMA verwenden. Der Virus legt das Computersystem lahm. Die Sperrung erfolge aufgrund einer illegalen Handlung und werde erst gegen Zahlung einer Strafe wieder aufgehoben.

Schutzmaßnahmen
Auf solche Erpressungsversuche sollte sich kein Nutzer einlassen. Außerdem sollten Antivirenprogramme und Firewall stets auf dem neuesten Stand sein.

_Spam

Spam ist das einzige Cybercrime-Phänomen, das momentan immer weniger wird, jedoch sind immer noch ca. 90 % aller E-Mails Spam. Einer der Gründe des Rückgangs ist die Ausschaltung einiger Botnetze in den letzten Jahren. Auch deutlich besser geworden sind die Spamfilter der E-Mail-Provider.

Schutzmaßnahmen
Es sollten keine Mails unbekannter Herkunft geöffnet werden und bei Nachrichten von bekannten Online-Diensten sehr genau hinschauen.

_Allgemeine Schutzmaßnahmen

Der wohl wichtigste Schutz ist Kompetenz im Bereich IT und Vorsicht. Es liegt klar auf der Hand, dass Unkenntnis 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._

_Kontakt

digital dentistry

Thomas Burgard
Dipl.-Ing. (FH)
Softwareentwicklung
& Webdesign
Bavariastraße 18b
80336 München
Tel.: 089 540707-10
info@burgardsoft.de

www.burgardsoft.de
burgardsoft.blogspot.com
twitter.com/burgardsoft

Infos zum Autor