Norton Safe Web

Ist diese Site sicher?

Site-Adresse eingeben

Hilfreiche Informationen über Bedrohungen

Die Beschreibungen der verschiedenen Bedrohungen, denen ein Computer ausgesetzt sein kann, sind oft etwas verwirrend. Im Folgenden werden die in unseren Berichten erwähnten Bedrohungen kurz beschrieben. Weitere Informationen zu Sicherheitsbegriffen finden Sie außerdem im Online-Glossar von Symantec Security Response.

Drive-by-Downloads

Ein Drive-by-Download ist Computercode, der einen Software-Bug in einem Webbrowser ausnützt. Er beeinflusst den Browser das zu tun, was der Angreifer möchte, z. B. bösartigen Code ausführen, den Browser zum Absturz bringen oder Daten auf dem Computer lesen. Softwarebugs, die zu Angriffen über den Browser führen, werden auch als Sicherheitslücken bezeichnet.

Phishing-Angriffe

Ein Phishing-Angriff liegt vor, wenn ein Angreifer Websites veröffentlicht oder E-Mails sendet, die vorgeben, von einem vertrauenswürdigen Unternehmen zu stammen. Diese Websites oder E-Mails erfragen von unwissenden Kunden sensible Daten. Weitere Informationen über Phishing finden Sie hier bei Symantec Security Response.

Spyware

Unter Spyware versteht man Softwarepakete, die persönliche oder vertrauliche Daten ausforschen und an Dritte übermitteln.

Viren

Viren bestehen aus bösartigem Code oder Malware und gelangen üblicherweise über E-Mail, Download oder unsichere Websites auf Ihren Computer.

Heuristisch erkannter Virus

Ein heuristisch erkannter Virus wird auf Grund seines bösartigen Verhaltens erkannt. Dazu gehört beispielsweise der Versuch, persönliche Informationen wie Kennwörter oder Kreditkartennummern zu stehlen.

Würmer

Würmer bestehen aus anderem bösartigen Code oder Malware und sind hauptsächlich darauf ausgerichtet, andere Computersysteme mit Sicherheitslücken zu befallen. Sie verbreiten sich in der Regel dadurch, dass sie eine Kopie von sich per E-Mail, Instant Messaging oder ähnlichen Programmen versenden.

Unerwünschte Browseränderungen

Eine unerwünschte Browseränderung liegt vor, wenn eine Website oder ein Programm das Verhalten oder die Einstellungen des Browsers ohne Zustimmung des Benutzers verändert. Dabei wird beispielsweise die Startseite oder Suchseite geändert auf eine Website, auf der sich Werbung oder vom Benutzer unerwünschte Inhalte befinden.

Verdächtige Browseränderungen

Eine verdächtige Browseränderung liegt vor, wenn eine Website versucht, die Liste der vertrauenswürdigen Websites zu verändern. Eine Website kann versuchen, den Webbrowser dazu zu veranlassen, dass er ohne Zustimmung automatisch verdächtige Anwendungen herunterlädt und installiert.

Dialer

Ein Dialer ist ein Softwarepaket, das die Modemkonfiguration so ändert, dass eine Telefonnummer mit hohen Gebühren gewählt oder Bezahlung für den Zugriff auf bestimmte Inhalte verlangt wird. Als Ergebnis eines solchen Angriffs werden dem Besitzer des Telefonanschlusses Gebühren für unautorisierte Dienstleistungen verrechnet.

Trackware

Unter Trackware versteht man Softwarepakete, die die Systemaktivitäten und Benutzergewohnheiten verfolgen und Systeminformationen sammeln und diese Informationen an Dritte übermitteln. Die von solchen Programmen gesammelten Daten sind nicht vertraulich und können keiner Person zugeordnet werden.

Hackingtools

Hacking-Tools sind Programme, die von einem Hacker oder nicht autorisierten Benutzer verwendet werden, um Zugriff auf den Computer zu erlangen oder eine Identifizierung oder Fingerprinting des Computers durchzuführen. Manche Hacking-Tools werden von System- oder Netzwerkadministratoren für legitime Zwecke verwendet, aber Ihre Funktionen können

von nicht autorisierten Benutzern missbraucht werden.

Scherzprogramme

Ein Scherzprogramm ist ein Programm, dass das normale Verhalten des Computers ändert oder stört und den Benutzer dadurch ablenkt oder belästigt. Scherzprogramme werden so programmiert, dass sie Aktionen hervorrufen wie z. B. das willkürliche Öffnen des CD- oder DVD-Laufwerks.

Sicherheitsrisiko

Ein Sicherheitsrisiko ist ein Zustand, in dem der PC schlecht gegen Angriffe geschützt ist. So ein Zustand kann entstehen, wenn ein sonst harmloses Programm einen Fehler enthält, der die Sicherheit Ihres Computers gefährdet. Solche Fehler sind in der Regel unbeabsichtigt. Die Verwendung eines solchen Programms kann die Angriffsgefahr auf Ihren PC erhöhen.

Verdächtige Anwendung

Eine verdächtige Anwendung ist eine Anwendung, deren Verhalten ein potentielles Risiko für den Computer darstellt. Das Verhalten eines solchen Programms wurde überprüft und als unerwünscht oder bösartig eingestuft.

Cybersquatting

Beim Cybersquatting wird der Name einer Website gefälscht, um die Besucher irrezuführen und den wahren Betreiber der Website zu verbergen. Dabei werden vertraute Marken simuliert oder der Besucher auf andere Weise getäuscht. Typosquatting ist eine Variante des Cybersquatting, bei denen Varianten der Schreibweise von Namen ausgenutzt werden.

Schwer deinstallierbar

Solche Programme lassen sich nur schwer deinstallieren. Selbst wenn sie deinstalliert werden, können sie Dateien mit Registrierungsschlüsseln zurücklassen, die dann die Ausführung der Dateien bewirken können.