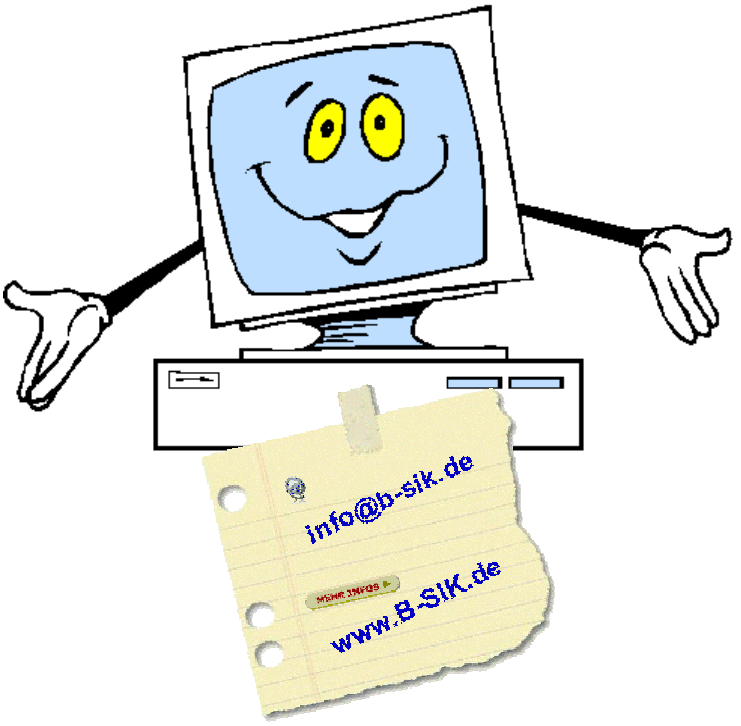
EDV-Kurs

Internetbedrohungen



B-SIK

In der Hand der Trojaner

(ddp)

13.05.2009 Viren, Trojaner, Würmer - das Internet ist für jeden Computer eine Gefahr. Selbst eine Firewall und ein Virenscanner bieten keinen hundertprozentigen Schutz. Doch was tun, wenn das Kind in den Brunnen gefallen ist? Wenn ein Trojaner im Hintergrund alles dokumentiert, was der Nutzer gerade tut, und dabei Passwörter und andere geheime Daten ausspioniert?

Oft merke der Nutzer zunächst gar nichts davon, dass sein Rechner infiziert ist und ein Trojaner im Hintergrund fleißig Schädlinge nachlädt, warnt Daniel Bachfeld von der Computerzeitschrift "c´t". Früher wurden die befallenen PCs meist langsamer: Die Malware, die im Hintergrund ihr Unwesen trieb, bremste den Rechner aus. Doch die Rechenleistung eines modernen Computers ist so hoch, dass zusätzliche Programme kaum noch ins Gewicht fallen. Zudem arbeiten Schädlinge sehr unauffällig, um einer Entdeckung so lange wie irgend möglich zu entgehen.

Stutzig sollte man auf jeden Fall werden, wenn sich wichtige Programme plötzlich nicht mehr auf den neuesten Stand bringen lassen und sich beispielsweise der Virenscanner gegen ein Update sträubt. Der Wurm Conficker etwa sperrt den Zugang zur Homepage des Virenscanners, der damit für den User nutzlos wird.

Besonders gefährlich wird es, wenn ein Trojaner den Rechner befallen hat und Schadprogramme nachlädt, bis der PC komplett ferngesteuert werden kann. Dann wird der Computer zum "Zombie". Nun kommt es ganz darauf an, was die Kundschaft wünscht. Soll der befallene Rechner Spam verschicken, Passwörter auslesen oder Malware weiterverbreiten? Laut Bachfeld gibt es inzwischen eine regelrechte Untergrundwirtschaft im virtuellen Netz. Kreditkartennummern oder Bankdaten, der Versand von Spam - alles hat seinen festgesetzten Preis.

Haben sich Schadprogramme erst einmal im Computer eingenistet, ist es ziemlich schwierig, sie wieder vollständig herunterzubekommen. Virenscanner erkennen die Malware zwar im laufenden Betrieb, können sie aber so nicht entfernen. Auch im oft empfohlenen abgesicherten Modus ist das eher schwierig. Bachfeld empfiehlt, den Rechner von der bootfähigen CD des Antivirenprogramms hochzufahren. Dann startet Windows nicht und die Schädlinge können sich nicht schützen. Die Hersteller kostenpflichtiger Antivirenprogramme liefern solche CDs im Normalfall mit. Die "c´t"-Redaktion bietet mit Knoppicillin eine eigene Lösung an.

Nachdem der Schädling entfernt wurde, sollte man den Virenscanner das System im normalen Betrieb prüfen lassen. Wenn dann das Antivirenprogramm erneut Alarm schlägt, sind Rückstände der Malware weiterhin auf der Festplatte. Die Gefahr ist dann groß, dass erneut Schädlinge auf den Rechner geladen werden oder der PC weiter ausspioniert wird. Daher hilft im Fall eines ernsthaften Virenbefalls meist nur eins: Der Rechner muss neu aufgesetzt werden.

Wenn man von seiner eigenen E-Mail-Adresse Spam-Mails bekommt, heißt das übrigens noch lange nicht, dass der PC Teil eines sogenannten Botnetzes geworden ist, das Spam verschickt. Die Adresse des Absenders ist nämlich meist gefälscht. Für den Betroffenen ist das sehr ärgerlich, schließlich wird unter seinem Namen Spam verschickt. Doch wirklich tun könne man dagegen leider nichts, sagt Bachfeld. Es sei so gut wie unmöglich, den tatsächlichen Absender ausfindig zu machen.

Eine relativ neue Masche der Cybergangster ist die sogenannte Scareware, die Geschäfte mit der Angst vor Viren und Trojanern macht. Solche Seiten gaukeln einen Sicherheitstest vor, der natürlich negativ ausfällt, und bieten dann eine kostenpflichtige Software an, die angeblich die Probleme behebt. Die Software sei meist völlig funktionslos und der Betroffene habe für nichts und wieder nichts Dutzende Euro ausgegeben, warnt Bachfeld.

Um sich vor Internet-Schädlingen zu schützen, sollte auf jedem internetfähigen PC stets ein aktueller Virenscanner mitlaufen und auch die Firewall muss stets aktiviert bleiben. Sämtliche Programme sollten auf dem aktuellen Stand sein. Das gilt insbesondere für die typischen Einfallstore für Malware wie den Browser, Acrobat Reader, Media Player, Quicktime und Java. Dazu gibt es beispielsweise unter secunia.com und updatestar.com kostenlose Update-Manager im Netz. Und natürlich gilt: Immer die Augen offen halten, denn das Internet ist gefährlich für die Sicherheit des PCs.

Internetbedrohungen

Norton Safe Web

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 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.

Internetbedrohungen

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, das 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.

Internetbedrohungen

Spam

Als Spam oder Junk (engl. für ‚Abfall' oder ‚Plunder') werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden und häufig werbenden Inhalt haben.

Malware

Als Schadprogramm oder Malware (Kofferwort aus engl. malicious, „bösartig" und Software) bezeichnet man Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und ggf. schädliche Funktionen auszuführen.

Trojaner

Als Trojanisches Pferd (engl. Trojan Horse), auch kurz Trojaner genannt, bezeichnet man ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt.

Backdoor

Backdoor (auch Trapdoor oder Hintertür) bezeichnet einen (oft vom Autor eingebauten) Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen.

Adware

Adware ist ein Kofferwort aus engl. advertisement (dt.: „Reklame", „Werbung") und Software. Sie bezeichnet Software, die dem Benutzer zusätzlich zur eigentlichen Funktion Werbung zeigt bzw. weitere Software installiert, welche Werbung anzeigt.

Scareware

Bei Scareware handelt es sich um Software, welche darauf ausgelegt ist, Computerbenutzer zu verunsichern oder zu verängstigen. Der Begriff ist ein engl. Kofferwort aus scare (Schrecken) und Software.

Hijacker

Browser-Hijacker sind kleine Programme, welche die Einstellungen des Browsers manipulieren, um Seitenaufrufe (etwa die Startseite) und Suchanfragen auf bestimmte Webseiten umzuleiten.

Gute Beispiele:

⇨ http://www.www-kurs.de/gefahren.htm