

Zusammenfassung

Dieses Dokument behandelt Trojanische Pferde. Trojanischen Pferde haben den Zweck, ein Gerät wie beispielsweise einen Computer oder einen Server ohne das Wissen der Anwender zu infizieren, um einen permanenten, nicht autorisierten Zugang zum betreffenden Gerät zu erstellen und aufrecht zu erhalten.

Von Trojanischen Pferden kann jeder (Privatpersonen, kleine und mittelständische Unternehmen, grossen Verwaltungen etc.) betroffen sein, der Informationen per e-Mail, oder per Datenträger austauscht sowie Software, Dokumente und jegliche andere Art von Dateien aus dem Internet herunter lädt.

Inhalt

- 1 Was ist ein Trojanisches Pferd? →
- 2 Wie funktionieren Trojanische Pferde? →
- 3 Wer ist betroffen? →
- 4 Warum sollte man sich schützen? →
- 5 Vorbeugende Massnahmen →



1 Was ist ein Trojanisches Pferd?

Das Trojanische Pferd ist aus der griechischen Mythologie bekannt. Homer beschreibt in der Ilias, wie die Griechen in die Stadt Troja eingedrungen sind. Die Griechen wussten, dass sie ihr Ziel durch eine Belagerung von Troja nicht erreichen würden, da die Stadt zu gut geschützt war. Deshalb entschieden Sie sich, ein riesiges Holzpferd zu bauen und es als Geschenk und Zeichen des Friedens vor die Tore Trojas zu stellen.

Das trojanische Volk würdigte diese Geste und nahm das Pferd mit in die Stadt. In der Nacht stiegen einige griechische Soldaten aus ihrem Versteck im Bauch des Holzpferds und öffneten die Stadtpforten Trojas. So ermöglichten sie der griechischen Armee, die draussen vor der Stadt gewartet hatte, Troja einzunehmen.

Ein Trojanisches Pferd ist ein Softwareprogramm oder ein Teil eines Softwareprogramms, auch Maschinencode oder ausführbarer Code genannt, das den Anschein eines harmlosen Programms erweckt, in Wirklichkeit jedoch ähnlich wie ein Virus den Zweck

hat, ein Gerät wie beispielsweise ein Computer oder ein Server ohne Wissen der Anwender zu infizieren.

Im Gegensatz zu einem Virus oder einem Wurm reproduziert sich ein Trojanisches Pferd nicht. Es breitet sich auch nicht selber aus. Es kann jedoch in bestimmten Fällen eine ebenso zerstörerische Wirkung wie ein Virus oder ein Wurm haben.

2 Wer ist betroffen?

Von Trojanern kann jede Person betroffen sein, die Informationen per E-Mail sowie per Datenträger austauscht (Disketten, CD-ROMs, Memory Sticks etc.) oder Software, Dokumente sowie jegliche andere Art von Dateien aus dem Internet herunter lädt.

3 Wie funktionieren Trojanische Pferde?

Die Mehrheit der Trojanischen Pferde - auch Trojaner genannt - wird über Dateien oder Softwareprogramme mit Dateierweiterungen des Typs .EXE, .BIN, .COM, .ZIP und ähnliche verbreitet.

Beispiel einer Intrusionsattacke : das Trojanische Pferd tritt als Virenentfernungsprogramm auf, jedoch in Wahrheit infiziert es die Maschine, einen Computer oder Server, mit Viren.

Im Allgemeinen dient ein Trojanisches Pferd dazu, einen permanenten, unbefugten Zugang zu einem Gerät zu errichten und aufrecht zu erhalten. Die Anzahl der existierenden Trojaner ist ebenso beeindruckend wie die Vielzahl der Aktionen, die sie ermöglichen. Einige ermöglichen einfach den Zugriff auf die Dateien des infizierten Geräts, andere ermöglichen eine umfassende Interaktion mit dem infizierten Rechner über das Internet oder ein lokales Netzwerk.

Trojanische Pferde

Einige ermöglichen einfach den Zugriff auf die Dateien des infizierten Geräts, andere ermöglichen eine umfassende Interaktion mit dem infizierten Rechner über das Internet oder ein lokales Netzwerk.

Trojanische Pferde sind normalerweise in sechs Klassen eingeteilt: "remote access", Datenüberträger, Zerstörer, "denial of service", "proxy" oder "ftp" (File Transfer Protocol).

Beispiel:

Dieser Trojaner öffnet einen bestimmten Netzwerk-Port, der es dem Eindringling ermöglicht, das infizierte Gerät aus der Ferne zu kontrollieren. Ein Netzwerk-Port ist eine "virtuelle Tür" zu einem Dienst eines an ein Netzwerk angeschlossenen Rechners.

Durch diese "Tür" kommen und gehen die im Netzwerk ausgetauschten Informationen. Die bekanntesten Beispiele für Trojanische Pferde des Typs "Geheimtür" sind: «Subseven», «Backorifice» et «Netbus».



4

Warum sollte man sich schützen?

Trojanische Pferde stellen eine beträchtliche Bedrohung für alle Anwender von EDV-Systemen dar.

Sie können zu erheblichen Verlusten führen:

Direkte finanzielle Verluste

- Zerstörung kritischer Daten
- Ausserbetriebsetzung Ihres gesamten EDV-Systems
- ...

Ansehensverlust

- Verbreitung streng vertraulicher Informationen
- ...

Zeit Verluste

- Beseitigung von Trojanischen Pferden aus dem System
- Schliessen der durch die Trojanischen Pferde geöffneten Geheimtüren
- Aufwand für die Wiederherstellung der zerstörten Daten
- ...

5

Vorbeugende Massnahmen

Anbei vorbeugende Massnahmen, um sich gegen ein Trojanisches Pferd zu schützen:

- ➔ Verwenden Sie ein Antivirenprogramm mit Firewall auf Ihrem Rechner. Achten Sie darauf, dass sich die Software regelmässig selbst aktualisiert, um den Rechner vor neu entwickelten Trojanischen Pferden zu schützen.
- ➔ Öffnen Sie keine e-Mails, Softwareprogramme oder jegliche andere Dateien, deren Betreff oder Inhalt Ihnen ungewöhnlich oder verdächtig vorkommt.

- ➔ Um Ihr System nach einem erfolgreichen Angriff wiederherzustellen:
 - setzen Sie individuelle Zugangskontrollmechanismen ein,
 - führen Sie eine regelmässige Sicherung Ihrer Daten durch,
 - schützen Sie Ihre Maschinen auch physisch,
 - halten Sie sich über die neuesten Gefahren auf dem Laufenden.