HELPDESK

Trojaner-Erkennung mit System

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

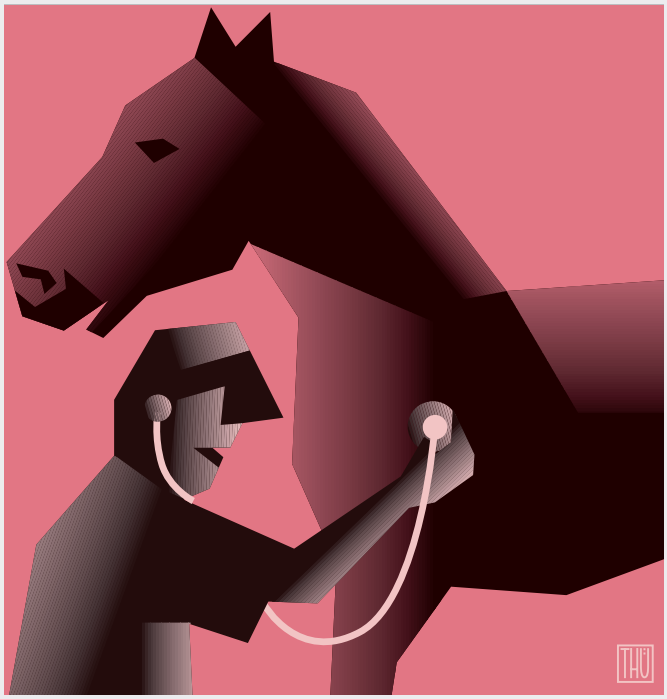

ILLUSTRATION: CW/THÜ

Frage: Wie lassen sich bereits installierte Trojaner entlarven?

Die Erkennung von bereits «installierten» Trojanern ist ein kniffliges Unterfangen, da selbst Anti-Trojaner-Tools keine 100-prozentige Erkennung bei infizierten Systemen garantieren. «Intelligente» Trojaner tarnen sich mittels Rootkits, um der Erkennung vorzubeugen. Wenn das infizierte System (noch) nicht mit der Aussenwelt kommuniziert, fällt auch die Erkennungsmöglichkeit durch Auswertung des Netzwerkverkehrs weg.

Portscanner überprüfen, welche IP-Adressen erreichbar und welche Dienste auf den Zielsystemen in Betrieb sind. Zwei Netzwerkprotokolle, welche in IP-basierten Netzwerken zum Einsatz kommen, sind besonders interessant – das verbindungsorientierte Transmission Control Protocol (TCP) und das verbindungslose User Datagram Protocol (UDP). Insgesamt gibt es je 65 536 Ports (inklusive Port 0) für TCP und UDP. Ein Port kann zwei Stati haben: offen (ein Dienst lauscht auf diesem Port) oder geschlossen (kein Dienst lauscht auf diesem Port).

Die für einen Portscan benötigte Zeitdauer hängt von verschiedenen Faktoren ab: zur Verfügung stehende Bandbreite des Netzwerks, Anzahl zu scannender Ports, Antwortzeit/Auslastung der Systeme und allfällige Existenz von filternden Netzwerkkomponenten wie Firewalls. Falls keine filternde Komponente zwischen Tester und getesteter Komponente liegt, sind TCP- im Vergleich mit UDP-Portscans wesentlich schneller, weil das Zielsystem umgehend zurückmeldet, in welchem Zustand sich der gerade abgefragte Port befindet. Manche Scantypen verdanken ihren Namen den gesetzten Packet-Flags (SYN, ACK, FIN, RST, PSH oder URG). Der SYN-Scan, auch als Halfopen-Scan bezeichnet, ist eine gängige Portscanmethode. Dabei wartet das scannende System nur die Antwort (SYN/ACK bei offenem Port, RST bei geschlossenem Port, keine Antwort: gefilterte Kommunikation) des gescannten Systems ab, ohne den darauf folgenden Protokollschritt (Paket mit Flag ACK senden) abzuarbeiten.

> «Der Zeitaufwand verleitet dazu, auf umfassende UPD-Portscans zu verzichten.»

Manche Denial-of-Service- und Remote-Administration-Trojaner sind so genannte «Schläfer», sie nutzen die Port-Knocking-Technik, indem sie auf das von der Steuerkomponente erwartete Aktivierungssignal in Form eines oder mehrerer an bestimmte Ports gesendete Pakete mit bestimmten gesetzten Flags warten und erst dann die DoS-Attacke ausführen oder für Kommandos empfänglich sind. Diese Taktik erschwert die frühzeitige Erkennung mittels Connect- (Abarbeitung des gesamten Handshake-Protokolls) oder SYN-Scans. Ein ACK-Scan könnte aber zum Ziel führen.

UDP regelt die Koordination des Datenverkehrs nicht selbständig. Falls bei UDP-Portscans keine ICMP (Internet Control Message Protocol)-Messages über nicht erreichbare Systeme oder Ports informieren, müssen die Timeouts abgewartet werden, was bei einem Portscan über den gesamten Portrange Stunden dauern kann. Dieser Zeitaufwand in Kombination mit den unpräzisen Rückmeldungen bezüglich Portstati verleitet dazu, auf umfassende UPD-Portscans zu verzichten. Dies kann fatale Folgen haben, wenn Malware-Autoren diese Geisteshaltung ihrer potenziellen Opfer ausnutzen und ihre Malware so konzipieren, dass sie primär das UDP-Protokoll nutzt.

Falls möglich sollte der gesamte TCP- und UDP-Portrange gescannt werden, da Malware oft Portnummern über 10 000 nutzt. Für TCP-Portscans ist der Open-Source-Portscanner Nmap erste Wahl, weist aber im UDP-Bereich Schwächen auf. Unicornscan eignet sich ausgezeichnet für UDP-Portscans. Portbelegungslisten helfen bei der Zuordnung von Ports und zugehörigen Diensten. ■

Umfangreiche Portbelegungsliste finden Sie unter:

www.computerworld.ch
Webcode: 0540391

Der Autor
Christoph Baumgartner ist Consultant und OPST bei Oneconsult, Thalwil, www.oneconsult.com.

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch