

Security Check 2. Teil: Rootkits, Trojaner & Botnets

Die Fortsetzung des Security Experten Michael Lausch

Ein Einbruch in ein Computersystem kann, auch wenn er sofort entdeckt wird, zu hohen Kosten führen. Wird er nicht entdeckt, geht der entstandene Schaden ins Unermessliche. Vor allem kommerziell orientierte Hacker haben kein Interesse daran, dass ihre Einbrüche schnell entdeckt werden. Je länger der Einbruch unentdeckt bleibt, umso länger hat dieser Hacker die Gelegenheit, mit dem aufgebrochenen System Geld zu verdienen. Wenn diese Einbrüche entdeckt werden, ist die Behebung des Schadens teurer als ein „einfaches“ Austauschen der Homepage gegen andere Inhalte.

Trojaner am Werk

Die Technologien, die für diese Art der Einbrüche benutzt werden, erreichen einen immer höheren Grad an Perfektion. Im Prinzip gibt es zwei auch kombinierbare Möglichkeiten. Die einfachste und am häufigsten angewendete Methode besteht darin, einen Trojaner zu installieren.

Dies kann durch Mithilfe des Benutzers erfolgen (Klicken Sie „Ja“ wenn sie das Programm installieren wollen), oder aber auch völlig unbemerkt durch Sicherheitslücken in anderen Programmen. Der Trojaner ersetzt ein Programm auf dem Rechner und wird daher immer dann ausgeführt, wenn dieses Programm ausgeführt werden sollte. Dabei kann der Trojaner entweder die Funktionalität des ersetzten Programms zusätzlich zu seinen „Hacking Funktionen“ selbst implementieren, oder er startet das ursprüngliche Programm und führt alles andere im Hintergrund aus. Da im Normalfall der Benutzer davon nichts merkt, kann so ein Trojaner lange Zeit unbemerkt auf einem System existieren. Das macht es schwierig Backups zu finden, deren Daten aktuell genug sind, die noch nicht den Trojaner enthalten.

Rootkits im System

Der Nachteil dieses Verfahrens ist, dass es durch den Einsatz von einfachen und billigen Mitteln möglich ist, eine Infektion zu erkennen und das ursprüngliche Programm wieder herzustellen. Um der Entdeckung zu entgehen, werden die Systemprogramme, die zum Aufspüren von solchen Infektionen verwendet werden (im einfachsten Fall ist das unter Windows

der Taskmanager oder unter Unix das „ps“ Kommando), durch eigene Programme ersetzt. Das kann aber auf Seiten des Hackers zu erheblichen Aufwänden führen, und da bei solchen Einbrüchen der kommerzielle Aspekt eine wesentliche Rolle spielt, wird eine andere Möglichkeit gewählt.

Ein so genanntes Rootkit richtet einen Bereich im System ein, der ohne spezielle Vorkehrungen nicht sichtbar ist, Software und Daten sind nicht ohne weiteres aufzuspüren. Ein unrühmliches Beispiel zum Einsatz eines Rootkits ist der Kopierschutz, der von einer Musikfirma zu Schutz von CDs eingesetzt wurde. Die Software dieses Rootkits verhindert, dass CDs kopiert werden können. Das alleine ist ja noch kein Problem, allerdings wurde dabei Software auf den Rechner kopiert, die ein Verzeichnis einrichtet, das von Virenschaltern nicht durchsucht wurde und auch unter Windows nicht zu sehen war. Mit dem verständlichen Ziel, als Kopierschutz nicht wieder entfernt zu werden, konnte diese Installation dann aber von Viren oder Trojanern verwendet werden, um dort Programme oder Daten zu deponieren.

Warum man sich vor Botnets besser schützen sollte

Worin besteht nun der kommerzielle Nutzen von solchen Trojanern? Die mit einem Trojaner infizierten Rechner werden so konfiguriert, dass sie von einer zentralen Stelle aus fernsteuerbar sind. Ein Zusammenschluss von solchen Rechnern, die zentral gesteuert werden, wird „Botnet“ genannt. Das größte Botnet, das bei Nachforschungen gefunden wurde, umfasste 150.000 Rechner. Solche Botnets oder Teile davon werden zur Miete angeboten und zum Beispiel von Spammern verwendet, um Massenmails zu versenden. Da dem Spammer durch die Größe solcher Botnets ein großer Adressraum zur Verfügung steht, sind die klassischen und kosteneffizienten Lösungen gegen Spam, nämlich durch Blocken von IP Adressen nicht möglich. Große, geografisch divergente Adressräume werden sogar zum Ziel von weit gefährlicheren Attacken, die „Distributed Deny of Service“ oder DDOS genannt werden.

Ein Botnet mit 150.000 Rechnern hat eine Bandbreite von mindestens 8 Gigabit/sec. bei der pessimistischen Annahme, dass jeder Rechner nur ein Telefonmodem mit

einer Bandbreite von 56kB/sec zur Verfügung hat. Wenn nun alle Rechner eines Botnets Webanfragen an einen Webserver stellen, oder auch nur irgendwelche IP Pakete schicken, ist jedes Netzwerk hoffnungslos überlastet. Solche DDOS Attacken werden üblicherweise für Erpressungsversuche verwendet, wenn die Bandbreite hoch genug ist, helfen alle Filter in Routern und Appliances nichts mehr. Voraussichtlich sind bei einem solchen Angriff auch die großen Internet Exchange Knoten betroffen.

In Zukunft noch mehr Achtung vor Rootkits

Neue Prozessortechnologien erschweren zunehmend das Auffinden von Rootkits. Die Technologien, die Virtualisierungen unterstützen, eröffnen ganz neue Techniken um Software zu verstecken. Trojaner laufen dann in ihrer eigenen virtuellen Maschine, die einzige Auswirkung ist im Verbrauch von Bandbreite oder CPU zu erkennen. Virenschalter und Rootkit Detektoren werden aus demselben Grund keine Fehler finden.

Jetzt schon Pflicht und nicht nur Kür

Was im privaten Bereich schon zur Plage geworden ist und eine Multimillionen-Dollar-Industrie ernährt (die Hersteller von Rootkit und Spyware Removal Software etwa), muss auch bei der Planung und dem Betrieb von Firmennetzen Beachtung finden. Die Installation von Software, beabsichtigt oder unbeabsichtigt, wird durch Firewalls nicht verhindert. Ebenso wenig die Regulierung von PC Benutzung durch Vorschriften oder Vereinbarungen zwischen Arbeitnehmer und Arbeitgeber. Es ist natürlich ein Aufwand, Software so zu installieren oder zu konfigurieren, dass die Benutzung auch ohne administrative Rechte möglich ist.

Denn die teuersten Firewalls und die sichersten Applikationen werden ausgehebelt, wenn der Angreifer bereits im Firmennetz ist. Gleiches gilt für Angriffe, die koordiniert von tausenden auf mehreren Kontinenten verteilten Rechnern stattfinden. In Security auch innerhalb und nicht nur am Rand des Netzwerkes zu investieren ist deshalb genauso notwendig, wie hunderttausende von Euros für Firewall-Lösungen auszugeben.

