http://www.nickles.de/static_cache/538329249.html

Re: Super-Schädling entdeckt
Von: xafford Am: 16.01.2008

Ähm... mal ganz frech gefragt... wisst ihr eigentlich selbst noch was ihr da für einen Blödsinn schreibt? Nur weil die vielen Linux-Server im Netz nicht von Viren und Trojanern befallen sind den Umkehrschluss zu wagen es läge an der "tollen Philosophie" von Linux ist so ziemlich das dämlichste, was ich seit langem gelesen habe. Sorry, das soll keine Beleidigung sein, aber so kommt es bei mir zumindest an.

Ich arbeite schon seit Jahren mit Linux, allerdings nur als Server und den Betrieb eines Systems als Server mit dem Alltag eines Desktopsystems für teilweise ahnungslose User zu vergleichen ist wirklich daneben. Allein schon wenn man nur 10 Sekunden überlegt, wie Viren und Trojaner im Normalfall auf ein System gelangen sollte euch vor Augen führen, dass ein Server hier per sé einer wesentlich geringeren Gefährdung unterworfen ist als ein Arbeitsplatzrechner. Es ist ja nun auch nicht gerade so, dass es massig verseuchte Windows-Server im Netz gäbe. Was es allerdings häufig gibt sind gehackte Webserver und die zumeist unter Linux, weil mal wieder ein Admin vergessen hat einen Apache oder sein SSH zu patchen, einen veralteten Kernel mit einem ungepatchten Exploit einsetzt oder sonstige Versäumnisse begangen hat.

Zudem sind Sever im Allgemeinen besser administriert als ein Desktopsystem, es laufen weniger Dienst darauf und als wichtigeter Punkt: Es sitzt kein dämlicher User davor, der auf jeden Scheiß klickt, der ihm unter den Mauszeiger kommt!

So, und was war nun die tolle Philosophie, die Linux vor Angriffen schützt? Die Benutzerverwaltung existiert unter Windows auch, nur wird sie leider (gerade auf Desktops) einfach ignoriert... Zudem gibt es wirklich unzählige Root-Exploits, die jegliche noch so tolle "Philosophie" genauso zunichte machen, wie dies unter Windows geht. Warum sollte es für einen Angreifer schwieriger sein ein Linux-System mit vorhandenem und ungepatchtem Root-Exploit zu übernehmen, als ein ungepatchtes Windows-System zu übernehmen? Auf die Erklärung wäre ich wirklich einmal gespannt...

Also bitte... schmeißt nicht Server-Systeme mit Desktop-Systemen zusammen in der Argumentation... das ist absolut unzutreffend und unseriös wenn es um die Diskussion über Viren und Trojaner geht, bei brauchen einen dämlichen Anwender, der sie auf´s System holt... und by the way... ich habe noch nie gehört, dass eine Philosophie ein System vor Infektionen geschützt hätte... in der Regel tun dies sehr gute Administratoren, die ihr Handwerk verstehen und um die Schwachstellen der von ihnen eingesetzten Systeme wissen... und die haben ALLE Systeme... ein Windows 2003 Server (der nebenbei eines der Systeme mit den wenigsten entdeckten Schwachstellen ist) genau so, wie ein Linux, ein Unix oder ein BSD... von den unzähligen Diensten und Programmen ganz zu schweigen.

Re: Super-Schädling entdeckt
Von: Data Junkey Am: 17.01.2008

Whoow. Ich habe schon einige Posts vom Xafford gelesen, Alle bisher mit größter Bewunderung und höchsten Respekt.
Aber soo habe ich ihn noch nie erlebt ..
Scheint sich diesmal also um ein "ernztzunehmendes" Problem zu handeln...
Wenn ich euch richtig verstanden habe, war meine Frage an "the_mic" (Data Junkey Am: 16.01.2008, 23:47) garnicht so unbegründet. .., die darauf hin zielt:
Was nutzt dem normalen Desktop-Anwender ein "unverwundbares" OS, wenn die Programme welche er benötigt / benutzt Infos preisgibt, die dem User schaden können.

Wenn z.B. jemand meinen eBay-Account (Zugangsdaten abfischt) ist es ein relativ schwacher Trost, wenn am nächsten Tag mein Linux immernoch läuft, weil das Kind trotzdem in den Brunnen gefallen ist. ..
Die Frage bleibt also, soweit ich das als DAU verstanden habe, wie kann sich ein normaler Verbraucher schützen? ...
Anzumerken sei noch:
Wenn ich Windows boote, gebt es genau 2-Möglichkeiten. Entweder ich will Multimedia oder Spiele machen, dann schalte ich grundsätzlich das Internet aus. Oder, ich will ins Netz, dann läuft als erstes Kaspersky IS7, und erst nach Update geht irgendwas oder jemand online. ..
Unter Ubuntu, ... kein Kaspersky, kein Schutz. .. ??.. Wir hatten gerade hier auf Nickles schon einige Diskussionen zum Thema Schutz; allerdings zu 99% auf das OS-Windows bezogen. ..
Weil ich gerade 2-Fachleute an der Leitung hängen habe, meine Frage?
1-PC, 1-Router, ein Standard-User, (der noch absoluter Linux-Anfänger ist) kann / sollte / muss was machen, um mit z.B. Ubuntu zumindest den Online-Verkehr (eBanking, eMail, PaxPal, eBay, Foren, etc.) so sicher wie möglich zu handeln?
Denn, genau zu diesem Zweck, fahre ich jetzt Zweigleisig, und nehme in Kauf, für gewisse Sachen Windows zu bemühen, weil mir einfach die fachliche Kompetenz und die nötige budgedierung fehlt, alles über ein OS zu organisieren.

Herzlichen Dank für eure Antworten, Thomas

Re: Super-Schädling entdeckt
Von: xafford Am: 17.01.2008
Hallo Data Junkey,

Aber soo habe ich ihn noch nie erlebt ..
Scheint sich diesmal also um ein "ernztzunehmendes" Problem zu handeln...

sorry für das unfreundliche Posting... kommt leider auch mal vor, aber gerade diese ewigen Themen, die mit mehr Mytifizierung als mit sachlicher Argumentation geführt werden (und zwar aus allen Lagern) geht mir ziemlich auf den Senkel, so dass ich sie normalerweise nur noch ignoriere. Das habe ich in dem Fall nicht getan, weil hier User beteiligt sind, die ich eigentlich sehr schätze. Nun mag man mir vorwerfen, dass ich es mit sachlicher Diskussion auch nicht so ernst genommen hätte in dem Post und... ja das stimmt. Deswegen will ich nochmal versuchen es sachlicher zu formulieren und auch auf deine Frage einzugehen, so weit es mir möglich ist.

Erst einmal vorweg und nochmal sachlicher formuliert:

Die Sicherheit und die Gefährdung im Betrieb eines Servers ist in keinster Weise mit der eines Desktop-Betriebssystems zu vergleichen. Die Gefährdungspunkte eines Servers beschränken sich auf Würmer und gezielte Hacks. Hier wiederum muss man unterscheiden zwischen Würmern und Hacks, die das Grundsystem angreifen (hierzu zähle ich mal freier Weise den Netzwerkstack und Kerndienste), die Serverdienste (wie z.B. den Webserver, DNS-Server, Datenbankserver) angreifen oder Anwendungen auf dem Server angreifen (z.B. Scripte im Rahmen des Webservers).

Würmer, die das eigentliche Betriebssystem angreifen waren bisher eher selten, dann aber mit massiver Verbreitung und gab es schon sowohl für Windows, als auch für Linux oder Unix. Würmer, die Serveranwendungen angreifen waren schon häufiger, der IIS5 war hier z.B. leider kein Ruhmesblatt, aber auch Apache hat es schon betroffen. Inwiefern man dies jedoch in eine Grundsatzdebatte über das zugrundeliegende Betriebssystem einfließen lassen will dürfte maßgeblich davon abhängen, wie schnell einem sachliche Argumente ausgehen, was ebenso für Würmer auf Anwendungen (z.B. verbreitete CMS-Systeme) angeht.

Gezielte Hacks auf Server haben da schon wieder eine andere Qualität, denn sie sind individuell und wenig geeignet eine große Zahl an Systemen unter seine Kontrolle zu bringen, was eben dazu führt (wobei wir wieder beim obigen Thema sind), dass es eben keine Millionen gehackter Server im Netz gibt und das unabhängig vom Betriebssystem. Wenn man sich jedoch anschaut, wie flott bei Contests Hacker Demohacks an Webservern durchziehen der wird sich hüten einen Linux-Server als vom Grundkonzept sicherer hinzustellen... die Sicherheit steht und fällt mit der Qualität der Administration und auch hier gilt dies wieder für sämtliche Systeme.

Wenn Du einen Linux-Server von einer Distributions-CD (respektive DVD) installierst dürftest Du, vorsichtig geschätzt, davon ausgehen mindestens 3 schwere Sicherheitslücken auf dem System zu haben, ohne Update hast Du erst einmal ein potentiell unsicheres System (und wieder: das gilt ebenso für alle anderen Systeme). Wie gefährlich diese Lücken sind hängt nun natürlich auch davon ab, wo diese Lücken sind und ob und wie dieser Teil des Systems zum Einsatz kommt. Hier ist jedoch ein Server einer höheren Gefährdung ausgeliefert, als ein Betriebsystem, da auch ein lokaler Exploit aufgrund des Grundprinzips eines Servers oft remote ausgenutzt werden kann (siehe ptrace() und Webserver). Als erstes ist also erst einmal Updaten angesagt, oder Du hoffst einfach darauf, dass dein Server in der großen Zahl der existierenden Server untergeht und deswegen nie individuell angegriffen wird.

Zu diesem Teil will ich nun mal eigenmächtig zusammenfassend sagen: Server werden im Normalfall gezielt und individuell angegriffen und selten automatisiert aufgrund der vielfältigen Systemunterschiede und unterschiedlicher Administration, was schon von Grund auf Massenhacks selten werden lässt.

Nun zu Desktopsystemen: Es gab mal Zeiten (ist schon eine Weile her), wo ein unerfahrender Linux-Nutzer nach einer "out of the box" Linuxinstallation ein offenes Scheunentor sein eigen nannte. Angefangen von einem offenen Relay (Emailserver), über einen offenen Telnetserver, einer an jedes Interface gebundenen Datenbank über Finger-Dienst, Time-Server bis hin zu frei verbindbaren X-Servern konnte man versehentlich fast alles ungewollt mitinstallieren. Da sieht bei Linux die Situation heute wesentlich besser aus. Dennoch hast Du als Anwender auch heute noch die Möglichkeit aus Unkenntnis dein System offen in die Welt zu stellen, wobei Du hier schon eine Menge an mutwilliger Handarbeit leisten musst.

Ähnlich sah es auch bei Windows aus und leider sieht es selbst heute noch so aus, denn Microsoft hat zwar grundsätzlich auch das Handwerkszeug ein Windows dicht zu bekommen, aufgrund von Bequemlichkeit (der des Anwenders) wird es schlicht ignoriert. Zwar wird dies nun versucht in Vista umzukrempeln, dieser Versuch dürfte aber mächtig nach hinten losgegangen sein, allein schon weil er so abrupt unternommen wurde, davon dass er halbherzig ist einmal abgesehen. Allein schon, wenn in Windows das vorhandene Rechtesystem sinnvoll eingesetzt worden wäre seit NT wäre viel an Sicherheitslücken nie akut geworden, denn das Rechtesystem nach Machart Microsofts ist eigentlich viel granularer als das Unix-artige (sprich, es lässt eine viel feinere Rechteabstimmung für Benutzer / Gruppen / Anwendungen zu), was aber natürlich auch viel mehr Fallstricke bietet als dies die Rechtevergabe unter Unix tut. Hinzu kommt natürlich noch, dass es Microsoft für sinnvoll erachtete, dass jeder User an senem Desktop als Administrator arbeiten solle, worauf sich dummerweise auch Software-Entwickler eingeschossen haben und ihre Software hanebüchenerweise so entworfen haben, dass diese dies voraussetzt, dies wäre vergleichbar damit, dass unter Linux jeder als root arbeitet.

Hier haben wir einen Punkt, der in der Praxis einem Schadsoftware-Ersteller einen Schritt spart, wenn seine Schadsoftware unter Windows arbeiten soll: Er bekommt idR direkt Zugang zu einem Administrationsaccount. Dies ist jedoch nicht ein grundsätzlichesSystemproblem, sondern ein gemachtes System, Windows würde es genau so ermöglichen eine saubere Account- und Rechtetrennung zu nutzen, inklusive

Schutz von System und Nutzerverzeichnissen, Schutz von Registryteilen, Zugriff auf Treiber und Hardwarekonponenten, Schutz einzelner Protokolle und Schnittstellen etc.

Gehen wir aber jetzt einmal von speziellen Fall einer Schadsoftware aus, die ein Anwender auf dem betreffenden System startet:

Es gibt jetzt zwei Möglichkeiten... der Nutzer hat Administratrenrechte oder nicht... hat er die, so steht ihm in der Regel das System offen wie ein Scheunentor... unabhängig vom zugrunde liegenden System. Hat er keine Administratorenrechte so bleibt der Schadsoftware entweder sich auf den Nutzeraccount zu beschränken, oder sie verschafft sich welche über einen lokalen Exploit, auch dies ist systemunabhängig, dabei muss es nicht einmal ein Kernel-Exploit sein, ein Privilege Escalation Exploit reicht aus. Hat die Software dann erst einmal die Rechte, so kann sie tun oder lassen was sie will.

Wo es nun ein Schadsoftware-Schreiber unter Linux grundsätzlich schwerer hätte eine Schadsoftware zu entwickeln würde mich wirklich einmal interessieren. Meiner Meinung nach beschränkt sich der Sicherheitsvorteil von Linux wirklich hauptsächlich in der erreichbaren Verbreitung einer Schadsoftware, denn selbst innerhalb verscheidener Linux-Installationen ist das eingesetzte System sehr inhomogen was Kernelversionen, Bibliotheksversionen, Dienste und installierte Anwendungen angeht, unter Windows kann man davon ausgehen dass das Prinzip one fits all zutreffend ist, was indirekt der Verbreitungsthese entspricht.

Noch eine Randbemerkung, um die Verbreitungs- und grundsätzlich-höhere-Linuxsicherheitsthese etwas ad absurdum zu führen... Rootkits sind schon ein alter Hut und seit Ewigkeiten bekannt... allerdings ursprünglich unter Unix/Linux... auf Windows kamen Rootkits erst sehr viel später "in Mode".

Was jetzt deinen speziellen Fall angeht:

Du stellst da eine ziemlich allumfassende Frage, die eigentlich eher weniger mit dem Betriebssystem zu tun hat. Du sitzt hinter einem NAT-Router, dein System kann also von Außen nicht direkt angegriffen werden, infolgedessen sind eigentlich systemunabhängige Nutzungsregeln für dich relevant, weniger die Konfiguration des Systems.

Schadsoftware kann nur auf dein System kommen, wenn Du diese auf das System holst, aufgrund fehlender von Außen erreichbarer Dienste kann sie dir nicht "appliziert" werden. Ergo gilt wie immer: Alles aktuell halten, keine aktiven Inhalte von Außen annehmen und öffnen (auch nicht im Browser / NoScript), immer verschlüsselte Verbindungen nutzen wo es möglich ist und darauf achten, wo Du welche persönlichen Informationen hinterlässt.

Jedoch ein oft vernachlässigter Punkt ist der Router und ich denke das wird in Zukunft noch ein böses Problem werden, denn wer den Router kontrolliert kontrolliert meist auch die Daten, bei Unachtsamkeit des Nutzers unter Umständen sogar HTTPS-Verbindungen. Achte darauf, dass die Firmware deines Routers immer aktuell ist, achte darauf, dass das Konfigurationsinterface nicht von Außen (via Internet) erreichbar ist und dass es mit einem guten Passwort gesichert ist. Zudem: Gehe nie auf das Konfigurationsinterface, wenn Du andere Seiten im Browser offen hast.. lösche deine Cookies nachdem Du auf dem Konfigurationsinterface warst oder auch bei anderen wichtigen Seiten. Achte bei sicheren Verbindungen immer darauf, ob das Server-Zertifikat wirklich zu dem Server passt, den Du besuchen wolltest undnicht zufällig zu einem ganz anderen Server gehört....