Sicherheit und kompromittierte Systeme – was tun?

Einmal angenommen man hat eben kein automatisches Windows Update verwendet, und auch die Patches nicht manuell installiert. Man ist der Meinung, dies sei überflüssig und das SP2 sowie die laufend angebotenen Sicherheitspatches stellt Microsoft nur zur Verfügung, um sein eigenes Betriebssystem zu sabotieren. Ist also überflüssig…
Jetzt hat es einen erwischt. Egal, warum.
Man wurde gehackt: Was nun ?
In diesem Fall gibt es eigentlich nur schlechte Nachrichten: Praktisch nichts hilft, um das System wieder sauber zu bekommen!
Das sagt wikipedia dazu: http://oschad.de/wiki/index.php/Kompromittierung
Zunächst einmal ist es so, das man ein System, in das bereits eingedrungen wurde, nicht durch einen Patch säubern kann. Der Patch (oder Windows-Update) beseitigt nur die Verwundbarkeit. Ist aber ein Hacker (oder dessen Tool) erst einmal im System gewesen wird er fast immer sichergestellt haben, das er auf verschiedene Arten erneut ins System gelangen kann.
Um das gleich und deutlich zu sagen: *Du bist keinesfalls so wichtig, das ein Hacker sich die Mühe machte, gezielt Dein System zu hacken!*
Nein, das erledigen vollautomatisch die im Internet kursierenden Schadprogramme.
Es werden immer mehr Webserver mittels SQL-Injection so manipuliert, dass sie den Exploit-Code an anfragende Rechner ausliefern.
Somit kann ein Windows-System allein durch den Besuch einer Webseite infiziert werden.
Ein zusätzlicher Klick ist nicht einmal nötig…
Man bekommt das System auch nicht sauber indem man die Backdoors entfernt die der Hacker hinterlassen hat. Und zwar deshalb, weil man nicht weiß, wie viele Türen der Hacker tatsächlich für sich hinterlassen hat. Die Tatsache das man keine weiteren Türen mehr finden kann bedeutet dabei gar nichts: Nur weil man nichts mehr findet heißt das nicht, das nicht noch weitere Türen im System ist. Das System kann sogar so stark kompromittiert sein, das es schlicht nicht möglich ist einige Türen aufzuspüren.
Nutzer tendieren meist dazu, die Kompromittierung durch eigene Reparaturarbeiten zu beheben. Weil sie die Neuinstallation scheuen.
Dies ist jedoch meist nicht von Vorteil, da der Angreifer volle Kontrolle über das System hatte. Dies ermöglichte es dem Angreifer unter Umständen auch Schadprogramme zu installieren, die Virenscanner oder andere Werkzeuge nicht erkennen.
Auch Tools zum entfernen von Würmern sind nicht wirklich hilfreich. Microsoft und andere Hersteller haben solche Tools veröffentlich - und damit wird man die von einem bekannten Wurm hinterlassenen Türen sicherlich los: Was aber ist mit den anderen Einlässen die der Hacker nach der Übernahme des Systems noch eingebaut hat - die aber eben nicht von diesen Tools entfernt werden?
Auch Anti-Virus Programme nützen nichts. Man kann einem kompromittiertem System schlicht und ergreifend nicht trauen: Angenommen der Antivirenscanner untersucht das System nach bestimmten Kriterien - was hält den Hacker davon ab für diesen Fall Tools platziert zu haben, die das System und den Virenscanner belügen? Nichts!
Es gibt inzwischen eine ganze Reihe von Schadprogrammen, die als Erstes den anwesenden AntiVir- Programmen versichern, das man schon immer gut befreundet war. Neinein, sagt das Schadprogramm – neinnein, ich bin kein Schadprogramm, ich bin ein guter Freund! Geh mal schlafen, Du dummes Anti- Tool!
Was vergessen? Ach ja, die paar bits, die Desktopfirewall schlafen zu schicken, ja, die hab ich auch noch. Ja, und neuerdings werden sogar Prozesse mißbraucht, die jedes Tool und sogar MS selbst als vertrauenswürdig einstuft – wie z.B. das Microsoft- Update!
Und sie lassen sich oft sogar recht leicht erkennen und löschen.
Aber nicht ohne in verschiedenen dll- Dateien ein kleines Fürzchen hinterlasse zu haben, das auch nicht im mindesten stinkt. Aber sehr geduldig auf seine Aktivierung wartet. Durch oben genannte Exploids zum Beispiel.

Nun ja, dann kommen die Klügsten aller User, "reinigen" den PC. Und lassen zum Beweis, daß er sauber ist, ein schlafendes Anti- Tool drüber laufen.
Es gibt sogar Händler und Fachleute", die damit Geld verdienen.
Oder besser gesagt: von der *Heiligen Scheu* der User *vor einer Neuninstallation* profitieren.

Mich erinnert die "Löschung" von deutlich sichtbaren Schädlingen an einen alten Witz:
Es gehen zwei Menschen zum Arzt. Der eine klagt über Durchfall, der andere über zu hohe Erregbarkeit. Der Arzt verwechselt die Medikamente…
Ihm fällt das später auf und er fragt nach einiger Zeit den Durchfall- Erkrankten, wie es ihm gehe. Nun, sagt der, ich sch…ß mir zwar immer noch in die Hosen – aber es regt mich nicht mehr auf….

Auch eine erneute Installation des Betriebssystems ***über*** die vorhandene Installation (Reparaturinstallation) bringt nichts. Der Hacker kann –und wird- auch hier Tools platziert haben die den Installer über die vorliegende Installation belügen. Der wiederum wird deshalb kompromittierte Teile des Systems nicht mit den Originalen überschreiben - die Neuauflage des Systems wäre dann genauso kompromittiert wie die vorige Variante. Völlig abgesehen davon: Der Hacker kann natürlich auch in Programmen die nicht zum Betriebssystem gehören Backdoors eingebaut haben - und die werden beim überspielen des vorhandenen Systems natürlich nicht ausgetauscht.
Man vertraut auch besser keinen Daten eines kompromittierten Systems: Die können natürlich ebenfalls gefälscht sein. Das gilt im Besonderen für die Event-Logs die man mit der Ereignisanzeige betrachten kann: Hier kann der Hacker eintragen was immer er will - oder aber er hat sogar ein Programm platziert das Dir einfach anzeigt was immer der Hacker will, nur eben NICHT den Inhalt des Event-Logs.
Der einzige verlässliche Weg ein einmal kompromittiertes System wieder vertrauenswürdig zu machen ist der: Platte(n) formatieren und neu installieren. Klingt hart, ist aber unumgänglich: Nach dem formatieren muss zunächst das System (von einem nicht kompromittierten Medium) und dann alle Anwendungen neu installiert werden. Daran geht einfach kein Weg vorbei.
Danach wäre es dann sicherlich eine gute Idee, Windows Update einzuschalten und auch die Firewall zu aktivieren.
Immer wieder höre ich die Meinung "Auf meinem PC ist nichts, was einen Hacker interessieren könnte - bei mir lohnt es sich nicht!"
Ja - das stimmt. Private Daten sind nicht sonderlich gefragt. (Passworte, Keys und dergleichen werden aber sicher nicht verschmäht, sondern maschinell ausgefiltert und ausgewertet—denk ich mal)
Noch einmal:
Der Hacker hat sich Deinen PC auch nicht gezielt ausgesucht, weil Du im seine Freundin ausgespannt hast! Und er will auch nicht die Daten Deines schwindsüchtigen Girokontos ausspähen. Obwohl – ein paar TAN sind sicher immer willkommen!
Nein – Du bist nur das Opfer eines "Rundumschlages" geworden. Um Deinen PC zu mißbrauchen! Und das betrifft Dich schon – auch wenn Du garnichts davon bemerkst und der Meinung bist, Du seiest viel zu klug und durch Dein überragendes Wissen sowieso sicher.
Und man muß dazu nicht unbedingt Sex- Seiten anklicken.
(***Weil natürlich keiner, auch nicht einer der Leser jemals auch nur auf den Gedanken käme, sich Porno anzugucken [äkssss!] nennen wir das scheinheilig "Schmuddelseiten", ja?***)
Nein - den Sasser bekam ich schon mal, als ich mit einem neu installierten System nur auf Billys Updates ging. (Das war allerdings vor dem SP2)
Aber weiter - was ist mit Bandbreite und Festplattenspeicher?
Wenn Dein Rechner als Spam- Relay dient, dann bist Du es, den der Provider abklemmt.
Wenn dann auf Deinem Rechner Warez, MP3s und Kinderpornos oder die Links dazu gespeichert werden, dann bist du derjenige, der Besuch vom LKA bekommt. Auch wenn Du garnichts davon weißt. (Es sind in D schon einige solcher Rechner beschlagnahmt worden…)
Ganz abgesehen von Deinen Freunden, die sicher sehr erfreut sind, wenn sie von Dir versendete, verseuchte Mails erhalten - von denen Du garnichts bemerkst.

Was ja der eigentliche Sinn dieser Schadprogramme ist!
Nein, Du kluger User, der Du auf SP2 und Patches verzichtest, seit Mai 2008 natürlich SP3 – die, welche das "Zeug von Microsoft" anwenden, das sind die wirklich Klügeren!
Und Verantwortungsbewußteren. Ich für meinen Teil denke, daß ich einen wirklich von Schadprogrammen freien PC habe. Schon bei der Installation berücksichtige, wie ich meinen PC schützen kann. Und wie ich, wenn er nun einmal trotz alledem befallen ist und ich ihn formatieren muß, meine Daten behalte.
Und wie ich ihn am Schnellsten wieder sauber zum Laufen bekomme.
Wie? Mache ich so:
Ich installiere ihn intelligent.

Installationsvorschlag:
http://www.computerhilfen.de/jueki/Installation.pdf

Ich entferne alle Dateien aus dem System, die ich dort nicht benötige und die ich nicht gerne verlieren möchte:

Systemhygiene:
http://www.computerhilfen.de/jueki/systemhygiene.pdf

und das Wichtigste – ich benutze sehr konsequent die Imagetechnologie:

Imageerstellung
http://www.computerhilfen.de/jueki/Image-Erstellung.pdf

Zum Einprägen:

Jeder Versuch, einen Schädling (ein Programm) durch ein Programm sicher zu beseitigen, muss scheitern. Es kann klappen. Muss es aber nicht. Und man kann hinterher nicht sicher wissen, ob es nun geklappt hat oder nicht. Man spielt russisches Roulette.

[Uni Marburg]

Alle die User, die da behaupten, es gäbe neben den gefährlichen Viren, Trojanern und sonstigen Schadprogrammen auch ungefährliche und leicht zu beseitigende, haben zweifellos recht.
Nur konnten diese bisher auch nicht ein einziges Kriterium nennen, mit dem ein beliebiger User dies zweifelsfrei unterscheiden kann!

Hat man eine Datei in Verdacht, dann kann man diese online prüfen lassen, ob sie wirklich gefährlich ist:
http://virusscan.jotti.org/de/
Dort wird eine Aussage getroffen, ob diese Datei als Schädling bekannt ist. Nichts weiter!

Und hier noch ein interessanter Aufsatz der Uni Marburg dazu:
http://www.mathematik.uni-marburg.de/~wetzmj/index.php?viewPage=sec-removal.html
Nichtskönner, stimmts, kluger Reinigungs- Spezialist? Ja, und ganz genau solche Nichtskönner sind auch bei Microsoft beschäftigt:
http://www.microsoft.com/technet/community/columns/secmgmt/sm0504.mspx
- und noch ein interessanter Beitrag:
http://malte-wetz.de.vu/index.php?viewPage=sec-removal.html

Jürgen Kirsten

Dieser Aufsatz ist mehr oder weniger das Resultat einer Zusammenfassung verschiedener Aufsätze, die im Internet veröffentlicht wurden.

Ich habe sie gelesen, verstanden, überarbeitet, zusammengefaßt und mit meinen Gedanken ergänzt.