DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Kompromittierung

Was tun bei Kompromittierung des Systems?

Wenn ein System kompromittiert wurde, **ist das System nicht mehr vertrauenswürdig**. Das heißt, dass alle Daten manipuliert sein könnten, das alle Programme manipuliert sein könnten und das alle Informationen, die auf dem System gespeichert waren oder verarbeitet worden sind, an Dritte weitergegeben worden sein könnten.

Wenn man diese Annahmen trifft, müssen zwingend folgende Maßnahmen durchgeführt werden:

- Das betroffene System ist sofort herunterzufahren, man kann sogar über ein hartes Ausschalten nachdenken. Es gibt hier sich widersprechende Ansichten, ich bin der Meinung, dass weitere Datenmanipulationen verhindert werden müssen. Hat man ausreichend Backups im Schrank, reicht aber auch eine Trennung vom Netzwerk.
- Alle sensiblen Informationen wie Passwörter für Betriebssystem, Online-Banking, Datenbanken etc., personenbezogene Daten, Geschäftsgeheimnisse, also alles, was irgendwie vor den Augen Dritter geschützt sein soll, muss als öffentlich bekannt angesehen werden. Dementsprechende Maßnahmen müssen eingeleitet werden.
- Ein Backup des Systems mit all seinen Daten ist zur späteren Analyse zu empfehlen. Falls man über kein Backup seiner Daten verfügt, sollte man dies zur späteren Wiederherstellung seines Systems unbedingt anfertigen. Dies muss aber von einem sauberen System aus geschehen. Dazu kann z.B. ein von einer CD bootbares Betriebssystem benutzt werden wie Knoppix. Soll der Einbruch in das System zur Anzeige gebracht werden, sind gesonderte Schritte einzuleiten. Soll nur ein sauberes System wiederhergestellt werden, so kann mit dem nächsten Schritt weitergemacht werden. Hinweis: Die Analyse eines Virenscanners ist völlig unzureichend, um Aussagen über das System zu machen, kann aber als Hilfsmittel eingesetzt werden, sofern er von einem sauberen System aus betrieben wird.
- Wenn ein sauberes Backup des Systems existiert oder Prüfsummen über das saubere System, können durch Vergleich Manipulationen aufgedeckt werden und der nächste Schritt kann übersprungen werden. Ist dies nicht möglich, so muss das System neu aufgesetzt werden.
- Neuaufsetzen des Systems: Zuerst muss das System vom LAN/Internet getrennt werden. Dann empfiehlt es sich die Festplatte, die das Betriebssystem enthielt, vorher zu formatieren, deren Bootsektor zu überschreiben und anschließend das Betriebssystem neu zu installieren. Wichtig ist, dass nur von garantiert sauberen Installationsmedien die Installation des Betriebssystems vorgenommen werden darf. Es darf nichts mehr verwendet werden, was zuvor auf der Festplatte lagerte (Programme, Treiber, Dateien mit ausführbarem Inhalt). Mit einem Linux wie Knoppix lässt sich beispielsweise prima eine Festplatte komplett leeren, auf der Kommandozeile einfach mal `dd if=/dev/zero of=/dev/hda` eintippen, sofern es sich um eine IDE-Festplatte handelt. Man sollte

aber wissen, was man tut. Hat man mehrere Festplatten eingebaut und erwischt die falsche, wäre das nicht so günstig.

- Die Passwörter, die zur Anmeldung an das Betriebssystem verwendet wurden, müssen neu ausgewählt werden, da die alten Passwörter als bekannt angesehen werden müssen.
- Nun sollten alle für das Betriebssystem sicherheitsrelevanten Patches bzw. Updates eingespielt werden. Da das neue System noch Sicherheitslücken hat, müssen die Patches von einem weiteren sauberen System (z.B. wieder mit Knoppix) heruntergeladen werden. Hilfreich ist hier http://winpatches.freewww.info/ und der Microsoft Baseline Security Analyzer, den man auch offline betreiben kann. Anschließend muss das System sicher konfiguriert werden. Für Windows 2000/XP siehe Dienste sicher konfigurieren, grundsätzlich sollten alle überflüssigen Dienste beendet werden, um offene Ports zu schließen. Umfangreiches Wissen über das Thema Sicherheit gibt es im Linkblock der Newsgroups de.comp.security.misc und de.comp.security.firewall. Anzumerken sei, dass man bei Google prima in alten Newsgroup-Postings suchen kann in der Rubrik Groups, bitte erst dort suchen, bevor man fragt und die FAQs bzw. den Linkblock lesen.
- Wenn das Betriebssystem neu installiert wurde, können die benötigten Anwendungen installiert werden. Auch hierbei ist peinlich genau darauf zu achten, dass nur von garantiert sauberen Installationsmedien, die Installation vorgenommen werden darf. Desweiteren gilt auch für Anwendungen, dass Sicherheitslücken mit Patches geschlossen werden müssen. Teilweise bietet die ein oder andere Anwendung automatische Updates an, teilweise muss man auf den Webseiten des Programmierers/Herstellers Ausschau halten. Es ist zu empfehlen bei Google mal die Begriffe "vulnerable", "exploit", "malware" und "spyware" nacheinander zusammen mit dem Software-Namen einzutippen, um einen groben sicherheitstechnischen Überblick über die Software zu erhalten, **bevor** man diese Software installiert.
- Um das System zu komplettieren, müssen nun die Daten (Datenbanken, Bilder, Schriftstücke etc.) aus einem sauberen Backup eingespielt werden. Gibt es kein Backup, das garantiert nicht veränderte Daten enthält, oder Prüfsummen über einen garantiert sauberen Datenbestand, so kann nur mit Einschränkungen mit dem alten Datenbestand weitergearbeitet werden. Lässt sich der Zeitpunkt der Kompromittierung nicht feststellen, so müssen alle Daten als manipuliert angesehen werden.
- Geht man von Manipulationen aus, müssen alle Dateien, die auch ausführbare Inhalte haben können, als schädlich angesehen werden. Eine Aufzählung von Dateitypen mit ausführbarem Inhalt für Windows gibt es hier. Dateien, die wirklich ausschließlich Daten und keinen ausführbaren Code enthalten, müssen, sofern der Inhalt wichtig ist, verifiziert werden, entweder durch Durchsicht oder automatisiert durch geeignete Algorithmen.
- Lassen sich Daten nicht verifizieren und sind trotzdem wichtig, so hat man Pech. Da angenommen werden muss, dass diese Daten manipuliert sind, sind diese ein Fall für die Mülltonne.
- Dateien, die ausführbaren Inhalt haben können, müssen genauer analysiert werden. Dies erfordert unter Umständen einen sehr hohen Aufwand. Wird die Analyse nicht durchgeführt, so kann auch ein Programm zur Ansicht der Daten herangezogen werden, das garantiert keine Inhalte ausführen kann, um die Daten gesondert von den ausführbaren Inhalten speichern zu können. Ist beides nicht möglich, so sind diese Dateien ebenfalls ein Fall für die Mülltonne.

Dies ist eine Liste von Dateiendungen, die Dateien mit ausführbarem Code bezeichnen können. Diese Liste ist mitnichten vollständig, denn die Anzahl der Dateiendungen ist fast unendlich. Da aber grundsätzlich jede Anwendung bei der Verarbeitung von Dateien Fehler machen kann und dadurch auch Code bei speziell präparierten Dateien zur Ausführung gelangen kann, sollte man stets sein System mit allen Anwendungen auf dem aktuellsten Sicherheitsstand bringen. Ein Beispiel für einen Fehler bei der Verarbeitung von Bilddateien gibt es hier.

Desweiteren ist darauf zu achten, dass der Windows-Explorer unter Umständen die Anzeige der Dateiendungen unterdrückt und so z.B. aus dem Dateinamen "Virus.jpg.exe" der Dateiname "Virus.jpg" wird. Dieses Verhalten kann für die meisten Dateitypen in den Ordneroptionen vom Windows-Explorer konfiguriert werden. Die Dateiendungen "pif" und "lnk" sind da etwas hartnäckiger und müssen, um im Windows-Explorer sichtbar zu werden, in der Registry zur Ansicht eingeschaltet werden. Ein Fehler im Windows-Explorer, Windows ZIP-Programm und Winzip lässt außerdem eine Datei der Art "Virus.folder" als Ordnersymbol erscheinen, in einer solchen Datei könnte ein Schadprogramm enthalten sein. Auch hier erkennt man die Dateiendung erst durch entsprechende Konfiguration des Windows-Explorers.

.asf .com .exe .html .js .mde .nws .reg .url .ws
.bas .cpl .folder .inf .jse .msc .pdf .scf .vb .wsc
.bat .crt .hlp .ins .jsp .msi .pif .scr .vbe .wsf
.chm .doc .hta .isp .lnk .msp .pl .sct .vbs .wsh
.cmd .eml .htm .jar .mdb .mst .ppt .shs .vcd .xl*

Da aber grundsätzlich jede Anwendung bei der Verarbeitung von Dateien Fehler machen kann und dadurch auch Code bei speziell präparierten Dateien zur Ausführung gelangen kann, **sollte man stets sein System mit allen Anwendungen auf dem aktuellsten Sicherheitsstand bringen**.

(Quelle: Wiki von Oliver Schad, http://oschad.de)