

4.7 Flüchtige Daten sichern: Sofort speichern

Wird man zu einem System gerufen, das im Verdacht steht, gehackt worden zu sein, ist es wichtig, innerhalb kürzester Zeit so viele vitale Informationen wie möglich zu sammeln, ohne dabei überall seine eigenen »Fingerabdrücke« zu hinterlassen. Es handelt sich hierbei um wichtige Statusdaten, die sowohl nach einem Shutdown als auch nach einem harten Ausschalten des Systems nicht mehr verfügbar sind.

Es sei auch an dieser Stelle nochmals darauf hingewiesen, dass man für die Sammlung dieser flüchtigen Informationen unter keinen Umständen die Systembefehle verwenden darf. Der Grund liegt zum einen darin, dass es sich um trojanisierte Programme handeln kann, die entweder bestimmte Informationen verbergen oder auch Schadfunktionen aktivieren können. Die Verwendung der lokalen Kommandos würde deren Zeitstempel des letzten Aufrufs verändern. Aus diesem Grund sollte mit eigenen sicheren und aus vertrauenswürdiger Quelle stammenden Dateien gearbeitet werden.

Keine Systembefehle verwenden!

Die Protokolldateien sollten entweder auf eine Diskette, in einer RAM-Disk oder über das Netz geschrieben werden. Hier eignet sich auch der Einsatz von Skripten oder Batch-Dateien, die die benötigten Informationen sehr schnell sammeln können.

Unabhängig davon, welche der in Abschnitt 7.1.1 und 7.2.1 vorgestellten Tools und Verfahren Sie zum Sammeln der benötigten Daten verwenden, sollten grundsätzlich folgende Informationen gesammelt werden:

- Systemdatum und -uhrzeit (mit Abweichung von einer Referenzzeit)
- Liste der aktiven Prozesse
- Liste der geöffneten Sockets
- Liste der Anwendungen, die auf geöffneten Sockets lauschen
- Liste der User, die gerade angemeldet sind
- Liste der Systeme, die gerade eine Netzverbindung haben oder vor Kurzem eine hatten

Sind diese Daten erfasst, kann man sich auf die Suche nach weiteren verdächtigen Spuren machen.

Grundsätzlich wird gesucht nach

- Timestamps des gehackten Systems,
- trojanisierten Systemprogrammen,
- versteckten Dateien und Verzeichnissen,
- verdächtigen Dateien oder Sockets und
- verdächtigen Prozessen.

Häufig genügt ein einzelner Ansatzpunkt, um die richtige Spur zu finden!

Aktuelle Uhrzeit

Damit alle eingegebenen Befehle einem Startzeitpunkt zugeordnet werden können, sollte unbedingt die lokale Uhrzeit des Systems erfasst werden. Alle Aktionen, die ab diesem Zeitpunkt erfolgen, sollten einwandfrei der Ermittlungstätigkeit zuordenbar sein.

Cache-Inhalt

Der Inhalt von Cache- und Auslagerungsdateien ist für die Analyse von laufenden Programmen oder abgesetzten Befehlen von Interesse. Soweit in einer laufenden Umgebung Zugang zu diesen möglich ist, sollten diese erfasst werden. Der Umfang übersteigt allerdings den Speicherplatz, den eine normale Diskette bietet.

Speicherinhalte

Der Inhalt des Hauptspeichers sollte komplett und auch im Prozesskontext erfasst werden. Für die einfachere Auswertung sollte der einer Prozess-ID zugeordnete Hauptspeicherinhalt jeweils separat erfasst werden. Auch diese Informationen passen nicht auf eine Diskette.

Status der Netzverbindung

Wesentliche Anhaltspunkte über eventuell aktive Hintertürprogramme finden sich auch in der Auflistung der offenen Netzwerkports. Zusätzlich lässt sich auch erkennen, ob Verbindungen gerade aufgebaut oder im Abbauprozess sind. Finden sich z.B. sehr viele Verbindungsaufbauanfragen, ist davon auszugehen, dass dieses System für einen Distributed-Denial-of-Service-Angriff oder einen Portscan verwendet wurde. Einige Betriebssysteme führen eine Statistik über die Anzahl der erfolgreichen oder erfolglosen Verbindungsaufbauversuche. Diese kann mit einem Befehl ausgelesen werden. Weiterhin ist es natürlich von Interesse, welche Applikation bzw. welcher Service den Port geöffnet hat.

Status der laufenden Prozesse

Eine Liste der aktuell laufenden Prozesse sollte gesichert werden. Zusätzlich sollten weitere Informationen (Umgebungsvariablen, Übergabeparameter, geladene Bibliotheken, offene Dateideskriptoren etc.) gespeichert werden.

Inhalt der Speichermedien

Finden sich in dem System Disketten oder Wechselmedien, sollten diese sichergestellt werden.

Beispiele zum Sammeln der gerade erwähnten Informationen können den folgenden Kapiteln 6 und 7 entnommen werden.

Inhalt des Hauptspeichers

In zunehmendem Maße ist es wichtig, auch den Hauptspeicher (RAM) des verdächtigen Systems zu sichern. Hierbei geht es nicht nur darum, den gesamten Speicherinhalt als eine große Datei zu sichern, sondern auch strukturelle Informationen. Hierzu gehören beispielsweise die Informationen welcher Prozess welche Bibliotheken geladen hat bzw. bestimmte Speicherbereiche belegt. Unter gewissen Umständen lassen sich diese Informationen auch im Nachhinein aus einem Hauptspeicherdump herauslesen. Wenn man auf Nummer sicher gehen will, sollten die Daten sowohl strukturiert als auch als Komplettdump sichergestellt werden.

4.8 Speichermedien sichern: forensische Duplikation

Die forensische Duplikation von sichergestellten Speichermedien hat sich quasi zu einem Standardvorgang bei der Ermittlung im Umfeld der Computerkriminalität entwickelt. Ein forensisches Duplikat ist letztendlich lediglich ein Image eines Datenträgers, das bitweise als eine 1:1-Kopie sicher erzeugt wurde. Dabei wird, unabhängig von den logischen Laufwerkszuordnungen, der gesamte physische Datenträgerinhalt übertragen.

Ein Standardverfahren

Grundsätzlich können mehrere Verfahren zum Einsatz kommen, wobei die letztendlich gewählte Variante auch von den lokalen Gegebenheiten am Einsatzort abhängt:

- Die verdächtige Festplatte wird aus dem gehackten System entfernt und dann an das Analysesystem des Ermittlers angeschlossen.
- An das gehackte System wird eine zusätzliche saubere Festplatte des Ermittlers angeschlossen.
- Die kopierten Daten werden über ein (geschütztes) Netzwerk auf das Analysesystem des Ermittlers übertragen.

Um das versehentliche Überschreiben der Festplatte zu verhindern, sollten unbedingt zusätzlich sogenannte Writeblocker angeschlossen werden. Diese Geräte verhindern physisch, dass auf den zu sichernden Datenträger schreibend zugegriffen wird. Der Datenträger kann ganz