DuD
Datenschutz und Datensicherheit

Computer-Forensik

Dirk Fox, Stefan Kelm

Unter Computer-Forensik werden Methoden und Vorgehensweisen zur Gewinnung von Erkenntnissen über beobachtete oder festgestellte Unregelmäßigkeiten oder Vorgänge verstanden. Üblicherweise werden sie bei Verdacht auf Vorliegen einer Straftat oder eines Tatversuchs im Bereich der Computer-Kriminalität angewandt, gelegentlich aber auch zur Klärung von Streitfällen. Zu den Straftatbeständen zählen nicht nur Computer spezifische wie Spionage oder Computerbetrug, sondern auch „klassische“ Straftaten, bei denen der Computer vom Täter nur als Hilfsmittel (z.B. zum Verfassen eines Schreibens) verwendet wurde. Grundsätzlich lassen sich daher drei Klassen von Tatbeständen unterscheiden:

- Vorgänge, bei denen der Computer selbst Ziel des Angriffs war (wie Spionage, Betrug),
- Vorgänge, bei denen der Computer vom Täter als Tatwerkzeug eingesetzt wurde (wie das Eindringen in andere Systeme, Verteilung oder Speicherung strafbarer Inhalte), und
- Vorgänge, bei denen der Computer eher eine zufällige (Neben-) Rolle gespielt hat und nicht erforderlich gewesen wäre (wie das Verfassen eines Drohbriefes, die Buchhaltung einer strafbaren Handlung).

Analyse

Ziele einer forensischen Analyse eines Systems, auf dem ein Angriff vermutet wird, sind

- die Rekonstruktion des Angriffshergangs (Vorgehensweise des Täters, Schwachstelle, die das Eindringen ermöglicht hat)
- die Ermittlung des tatsächlichen Schadens (gelöschte, veränderte oder kopierte Daten, weitergehende Angriffe)
- die idealerweise gerichtsverwertbare Sicherung von Spuren und Beweisen für eine erfolgte Straftat und
- die Identifikation des Täters anhand hinterlassener Spuren.

Die Erreichung dieser Ziele ist im Bereich der Computer-Kriminalität dadurch erschwert, dass

- das Verwischen „digitaler Spuren“ für einen kompetenten Angreifer oft sehr einfach ist (wie das Löschen von erstellten Dateien) und sogar durch Angriffstools unterstützt wird (Löschen oder Verfälschen von Log-Daten);
- den meisten Spuren kein verlässlicher Zeitpunkt zugeordnet werden kann, da entweder kein Zeiteintrag vorliegt (wie bei Resten einer gelöschten Datei) oder die Systemuhr vom Angreifer verstellt worden sein kann; und
- jeder Untersuchungsschritt an einem vorgefundenen System notwendigerweise eine Veränderung am Systemzustand verursacht.

Der erste (und wichtigste) Schritt einer forensischen Analyse ist daher ein umgehendes und möglichst vollständiges „Einfrieren“ des Systemzustands, idealerweise einschließlich flüchtiger Speicherinhalte (RAM). Die anschließende Tiefenanalyse sollte ausschließlich auf einer Kopie des Originalsystems erfolgen, um die Systemveränderungen, die die Analyse unvermeidlich selbst verursacht, jederzeit durch Zurückspielen des Originalzustands rückgängig machen zu können. Die Systemanalyse umfasst in der Regel die folgenden Schritte:

- die Sicherung gefundener Spuren eines erfolgten Angriffs, ggf. eine Beweismittelsicherung,
- die Überprüfung bestehender Zugriffsberechtigungen (in bis zu 80% der Fälle sind Innentäter involviert) und
- die Rekonstruktion gelöschter Daten.

Tools

Sowohl für das Sichern des vorgefundenen Systemzustands als auch für die Durchführung Betriebssystem spezifischer Tiefenanalysen gibt es zahlreiche Tools.[1] Eine vergleichende Untersuchung solcher Tools wurde vom amerikanischen NIST (National Institute of Standards and Technology) im Rahmen des Computer Forensics Tool Testing Projekts (CFTT) durchgeführt.[2] Diese sollten in jedem Fall statt auf dem zu untersuchenden System vorliegenden Systemprogrammen verwendet werden, da letztere modifiziert worden sein können.

Allein der Einsatz von Tools garantiert noch keine erfolgreiche Analyse. Die Kunst besteht darin, weitere Spuren im vom Angreifer genutzten oder „besuchten“ Gesamtsystem zu identifizieren und geeignet mit den Systemdaten abzugleichen oder zu verknüpfen, wie z. B. Logfiles von Firewalls, Routern oder eingesetzten Intrusion Detection Systemen (IDS).

Da einige im Rahmen der forensischen Analyse gewonnenen Erkenntnisse flüchtig und nicht oder nur eingeschränkt reproduzierbar sein können, ist eine umgehende Dokumentation aller Schritte und Beobachtungen von zentraler Bedeutung. Die Analyse sollte zudem nie von einer Person alleine sondern immer mit Zeugen durchgeführt werden.

In vielen Betriebssystemen ist die Zurückgewinnung von vom Täter vermeintlich gelöschter Daten dann erleichtert, wenn dieser sich keiner speziellen Angriffsprogramme bediente, denn in der Regel werden durch eine Löschoperation nicht alle Daten einer Datei von einem Speichermedium gelöscht, sondern lediglich der Eintrag im „Inhaltsverzeichnis“ des Mediums. In diesem Fall ist die Zurückgewinnung der Daten einfach, solange keine neue Datei in den wieder freigegebenen Speicherbereich hineingeschrieben wurde.

Reichen Software-Tools zur Rekonstruktion von Spuren wie z. B. gelöschten Dateien nicht aus, können physikalische Rekonstruktionsversuche weiter helfen. Nachteil: Diese Analysen müssen am Originalmedium erfolgen, da sie z. B. Magnetisierungs-“Reste“ an den „Rändern“ von Speichermedien für die Rekonstruktionsversuche auswerten; diese lassen sich aber mit Software auf einem Standardsystem nicht kopieren.

Das größte Problem in der Praxis ist allerdings, dass eine forensische Analyse in den seltensten Fällen an einem „unangetasteten“ System vorgenommen werden kann: Meist wurden bereits Untersuchungen an dem System durchgeführt, bevor mit einer systematischen Analyse begonnen wird. Oft werden dabei zahlreiche Spuren verwischt oder sogar unwiederbringlich zerstört.

Daher ist eine zentrale Voraussetzung für den Erhalt der durch eine forensische Analyse dokumentierbaren Spuren ein etablierter und eingeübter Notfallplan, der Panikreaktionen bei den Nutzern eines betroffenen Systems vermeidet und eine schnelle und professionelle Reaktion auf einen Anfangsverdacht ermöglicht.

[1] http://www.computer-forensik.org/tools.html
[2] Siehe http://www.cftt.nist.gov