Bundesamt
für Sicherheit in der
Informationstechnik

Leitfaden „IT-Forensik“

Version 1.0.1 (März 2011)

Die Bedeutung der Zeit

Zeitquellen

Die Grundlage für die Zeit in IT-Systemen ist häufig eine Echtzeituhr (engl. Real Time Clock – RTC). Diese ist üblicherweise mit einer Batterie ausgestattet, welche auch im ausgeschalteten Zustand die Zeit weiterzählt (siehe dazu auch [Bun06]). Aus dieser wird durch das Betriebssystem eine Systemzeit unter Hinzunahme weiterer Korrekturfaktoren, wie z. B. Zeitzoneninformation, erzeugt. Diese Systemzeit ist nun die Grundlage für die in Kapitel und in Kapitel detailliert beschriebenen Zeiten, welche durch das Betriebssystem erfasst und vom Dateisystem eines Computers für Verzeichnisse und Dateien mitgeführt werden. Jedoch ist die RTC nicht die einzige Zeitquelle. Viele Betriebssysteme in einem Netzwerk bieten zusätzlich die Möglichkeit, über das Netzwerk die Zeit zu synchronisieren. Dies geschieht üblicherweise über das auf Basis des Network-Time-Protokolls (NTP)[15].

Zeitlinien

Einen sehr wichtigen Einfluss auf Untersuchungen im Rahmen der IT-Forensik hat die von Computersystemen bzw. im Netzwerk mitgeführte Zeit. Ein der wichtigsten Tätigkeiten des Forensikers, insbesondere im Abschnitt der Datenanalyse (siehe Kapitel), ist die Korrelation von Ereignissen anhand des Zeitpunkts, zu dem sie stattfanden. Dabei wird eine Zeitlinie (engl. timeline) erzeugt. Eine wichtige Ausgangsvorraussetzung für die Korrelation, insbesondere wenn Daten aus unterschiedlichen IT-Systemen innerhalb eines Netzwerks in einen zeitlichen Zusammenhang gebracht werden müssen, ist daher eine vertrauenswürdige Zeitbasis.

RTC und Systemzeit erfassen und validieren!

Eine bedeutsame Forderung ist es, sämtliche Zeitquellen in einem IT-System zu von allen Einzelkomponenten zu erfassen. Die RTC eines IBM-kompatiblen PCs lässt sich häufig direkt im BIOS[16] auslesen. Auf windows-basierten Systemen kann die Uhrzeit mittels des Kommandos *time* und das Datum mit *date* in der Kommandozeilenumgebung abgefragt werden. Auf linux-basierten Systemen liefert der Befehl *date* sowohl das Datum als auch die Uhrzeit.

Achtung!

Da die Veränderung der Systemzeit selbst, z. B. zum Verwischen von Spuren, ein nachzuweisender Vorfall sein (siehe dazu auch Kapitel) kann, müssen sowohl die hardwarebasierte Zeit aus der RTC als auch die Systemzeit erfasst werden und mit einer aus einer unabhängigen Zeitquelle verglichen werden.

Einige Betriebssysteme (u. a. Linux) erlauben es, die Systemzeit völlig unterschiedlich zur RTC Zeit zu setzen. Schon allein deshalb ist eine Erfassung beider Zeiten (RTC und Systemzeit) erforderlich. Bei Microsoft Windows-basierten Systemen hingegen bewirkt eine Änderung der Systemzeit auch eine Änderung der RTC-Zeit. Beide Betriebssystem-Familien verlangen jedoch nach Administrator-Rechten zur Änderung der Zeit.

Zeitstempel

Der Aufbau und die Interpretation der Systemzeit sind stark vom eingesetzten Betriebssystem abhängig. Beispielhaft sollen nachfolgend ausgewählte typische Datumsformate kurz vorgestellt werden (siehe dazu auch [Fle08]).

---

15 http://www.ntp.org

16 Basic Input Output System, eine hardwarenahe Verwaltungsoberfläche - Achtung, der Zugriff auf das BIOS kann u. U. durch Passwörter geschützt worden sein, dieses muss dann bekannt sein.

MS-DOS Zeitstempel

Bei Verwendung des FAT-Dateisystems (siehe Kapitel) wird immer die lokale Zeit in einem 32bit Wert gespeichert. Da nur fünf Bit für die Speicherung der Sekunden vorgesehen sind, und damit nur max. 32 Sekunden dargestellt werden könnten, entschied man sich, nur die geraden Sekunden zu zählen, so dass der verfügbare Darstellungsraum auf die Sekunden auf diese Weise auf die 60 notwendigen Sekunden ausgebaut wurde. Es wird also niemals FAT-Zeitstempel mit ungerader Sekundenanzahl geben. Die nächsten sechs Bit geben die Minuten an. Darauf folgend, ist in fünf Bits die Stunde angegeben. Das Datum wird dahingehend gespeichert, dass der Tag in fünf Bits, der Monat in vier Bits und das Jahr in sieben Bits gezählt werden. Dabei wird der Null das Jahr 1980 zugeordnet, so dass das maximal darstellbare Jahr in MS-DOS Zeit das Jahr 2107 ist.

Windows 64bit Zeitstempel

Bei der Verwendung des Windows Betriebssystems wird im Dateisystem ein acht Byte (64bit) Zeitstempel mitgeführt (siehe dazu auch [Bun06]). Dabei werden die 100 Nanosekunden-Intervalle seit dem 1. Januar 1601 um 0:00Uhr gezählt. Hier wird also, entgegen des MS-DOS Zeitstempels, keine Teilung in Tage, Stunden usw. vorgenommen. Aus der Zählergröße und der Intervallgröße ergibt sich das maximal erfassbare Datum bis zum Ende des Jahres 59601.

UNIX 32bit Zeitstempel

Ähnlich dem Windows Zeitstempel werden auch beim UNIX Zeitstempel nur Zeiteinheiten ab einem Startzeitpunkt gezählt. Dabei werden jedoch bei UNIX Zeitstempeln die abgelaufenen Sekunden in einem 32bit Wert beginnend ab dem 1. Januar 1970 erfasst. Damit ergibt sich die größte darzustellende Zeit als der 2. September 2030, 19:42 Uhr.

Des Weiteren gibt es noch viele andere potentielle Zeitstempel in einem System. Stellvertretend für weitere Datumsangaben seien hier:

- OLE 2.0 Datum und Uhrzeit (8 Byte, beginnend ab 30.10.1899),
- ANSI SQL Datum und Uhrzeit (8 Byte, beginnend ab 17.11.1858),
- Macintosh HFS+ Datum und Uhrzeit (4 Byte, beginnend ab 1.1.1904),
- Java Datum und Uhrzeit (8 Bytes, beginnend ab 1.1.1970)

genannt.

Die Kenntnis des Zeitstempels allein reicht jedoch zur Zeit-/Datumsfeststellung einer Datei nicht aus, es müssen als Korrekturfaktoren noch die nachfolgend aufgeführten Zeitzonen eingerechnet werden.

Zeitzonen

Prinzipiell sollte bei jeder untersuchten IT-Komponente die RTC/BIOS Zeit erfasst werden. Die im System gültige Zeit hingegen ergibt sich aus dieser Zeit und einer Berechnung anhand der im System eingestellten Zeitzone. Auf windows-basierten Systemen ist die Zeitzone in zentralen der Registrierungs-datenbank (engl. Registry, siehe dazu auch Kapitel und Kapitel) als Schlüssel[17]

17 HKEY_LOCAL_MACHINE/SYSTEM/ControlSet001/Control/TimeZoneInformation (siehe

gespeichert. Auf linux-basierten Systemen ist die Zeitzone in der Datei *timezone* im Verzeichnis /etc gespeichert.

Dabei wird als Normzeitzone die Greenwich Mean Time (GMT) Zone benutzt, zu welcher in westlicher Richtung die Stunden addiert (GMT+X) und von welcher in östlicher Richtung die Stunden (GMT-X) abgezogen werden müssen.

Des Weiteren gilt es, eventuelle Sonderzeiten, wie z. B. die Sommerzeit (engl. Daylight Savings Time) zu berücksichtigen, um eine Aussage über die tatsächliche Zeit in einem System und den von ihm erstellten Objekten treffen zu können.

Eine Sonderstellung nimmt die durch das NTP-Protokoll[18] verbreitete Netzwerkzeit ein. Hier wird nur die koordinierte Weltzeit (engl. UTC) ohne jegliche Zeitzoneninformationen übertragen. Die Korrektur der Zeiten an die jeweilige Zeitzone muss also hier durch den Untersuchenden erfolgen. Wie aus den Angaben ersichtlich ist, differiert der Aufbau der Systemzeit sowohl bezüglich des dafür reservierten Speicherplatzes als auch der Interpretation der Daten erheblich. Deshalb muss sowohl das Betriebssystem, das verwendete Dateisystem und evtl. die erzeugende Anwendung des untersuchten Computersystems beachtet werden (siehe dazu auch Kapitel).

Sicherstellung einer zuverlässigen Zeitbasis

Strategische Vorbereitung beachten!

Da die Zeit eine bedeutende Rolle für die IT-Forensik spielt, sollen nun mögliche Strategien zur Sicherstellung einer korrekten Systemzeit vorgestellt werden. Diese sind ein wichtiger Teil der strategischen Vorbereitung und obliegen dem Anlagebetreiber. Hierbei kann eine Skalierung in einen niedrigen, mittleren und hohen Aufwand zur Sicherstellung einer korrekten Systemzeit unterschieden werden.

In der *niedrigsten* Ausbaustufe sollte zumindest eine Synchronisation des Computernetzwerkes mit einem zuverlässigen, netzwerkbasierten Zeitserver[19] unter Verwendung des Network Time Protokolls (NTP) erfolgen. Allerdings kann das Signal durch Vorfälle und bewusste Angriffe verfälscht werden.

In einer *mittleren* Ausbaustufe kann der Systembetreiber ein zusätzliches Empfangsgerät in Form eines DCF-77[20] Empfängers in sein Computernetzwerk integrieren. Derartige Geräte empfangen das offizielle Zeitsignal der in Deutschland gültigen gesetzlichen Zeit, welches über Langwelle deutschlandweit empfangbar ist (siehe dazu auch [Pie04]). Ein DCF-77 Empfänger setzt die Zeitsignale typischerweise in NTP-konforme Pakete um, welche dann als Zeitbasis für alle Computer im Netzwerk eingesetzt werden können. Jedoch sind das genutzte Funksignal und die damit übertragenen Daten nicht gegen eine absichtliche Manipulation geschützt.

In einer *hohen* Ausbaustufe wird deshalb eine Kombination aus DCF-77 und

dazu auch [Bun06])

18 http://tools.ietf.org/html/rfc778

19 empfohlen wird hier ntp1.ptb.de, dieser führt die "gesetzliche Zeit" in Deutschland und hat eine vorgeschriebene Verfügbarkeit von >99,9%

20 http://www.ptb.de/de/org/4/44/pdf/dcf77.pdf

GPS-Empfänger empfohlen. Derartige kombinierte Geräte[21] bestehen sowohl aus einem DCF-77 als auch aus einem GPS Empfänger und besitzen zusätzlich einen hochpräzisen internen Zeitgeber. Ein derartiges Gerät kann Differenzen aus beiden externen Quellen erkennen und den Anlagenbetreiber warnen. Es werden Logdaten in Normalbetrieb und im Fehlerfall geführt, welche vom Gerät über das Netzwerk gesichert und ausgewertet werden können.