Computer Forensik

Lerneinheit 1: Einführung

Prof. Dr. Christoph Karg

Studiengang Informatik
Hochschule Aalen

Wintersemester 2013/2014

Übersicht

Ziel dieser Lerneinheit ist es, eine Einführung in das Gebiet der Computer Forensik zu geben.

Sie gliedert sich in folgende Abschnitte:

- Ziele einer forensischen Ermittlung
- Der Ermittlungsprozess
- Gewinnung von Erkenntnissen
- Korrekter Umgang mit Beweismitteln
- Beweissicherung eines Computers

Die Lerneinheit basiert auf Kapitel 4 des Buchs *Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären* von Alexander Geschonnek

Ziele einer forensischen Ermittlung

- Erkennen der Methode oder der Schwachstelle, die zum Systemeinbruch geführt haben könnte
- Ermittlung des entstandenen Schadens nach einem Systemeinbruch
- Identifikation des Angreifers
- Sicherung der Beweise für weitere juristische Aktionen

Wichtige Anforderungen

Anforderungen:

- Es sollen so viele Informationen wie möglich vom kompromottierten System gesammelt werden
- Der aktuelle Zustand des Systems soll so wenig wie möglich verändert werden

Fragen im Zusammenhang mit einer Ermittlung

- Wie wird der Angriff verifiziert?
- Wie sollten der kompromittierte Rechner und die zugehörige Umgebung gesichert werden?
- Welche Methoden können für die Sammlung von Beweisen verwendet werden?
- In welcher Reihenfolge sollen die Beweisspuren gesammelt werden?
- Wo sucht man nach Anhaltspunkten und wie können sie gefunden werden?
- Wie kann das Unbekannte analysiert werden?

Der Ermittlungsprozess

Offene Fragen:

- Welche Ziele verfolgt ein Ermittlungsprozess?
- Welche Anforderungen werden an den Prozess gestellt?
- Welche Phasen werden durchlaufen?

Zielsetzung

- Die vom Ermittler gewählten Methoden und Hilfsmittel sollten robust und nachvollziehbar sein
- Die eingesetzten Methoden und Hilfsmittel sollten auch vor Gericht Bestand haben
- Ein Dritter, der nicht über den gleichen technischen Sachverstand und Erfahrungsschatz verfügt, muss den durchgeführten Tätigkeiten Glauben schenken können

Anforderungen

- Akzeptanz
  - Die eingesetzten Werkzeuge sollten in der Fachwelt anerkannt sein
  - Belege sind entsprechende Veröffentlichungen auf Konferenzen oder in Fachzeitschriften
  - Neue Verfahren müssen sich zunächst etablieren
- Glaubwürdigkeit
  - Eine Methode muss funktional und robust sein
  - Der Ermittler muss verstehen, wie die Methode funktioniert und in welchem Zusammenhang die Ein- und Ausgaben stehen

Anforderungen (Forts.)

- Wiederholbarkeit
  - Die eingesetzten Hilfsmittel und Methoden müssen von Dritten nachvollziehbar sein
  - Die Wiederholung der Ermittlung muss zu denselben Ergebnissen führen
- Integrität
  - Sichergestellte Spuren dürfen nicht verändert werden
  - Integrität der digitalen Beweise muss gewährleistet sein

Anforderungen (Forts.)

- Ursache und Auswirkungen
  - Die eingesetzten Methoden müssen Ergebnisse liefern, auf Basis derer man logisch nachvollziehbare Verbindungen zwischen Personen, Ereignissen und Beweisspuren herstellen kann
- Dokumentation
  - Angemessene Dokumentation jedes in der Ermittlung durchgeführten Schritts

Incident Response Prozess

1. Vorbereitung der Ermittlung
   - Beschaffung einer Autorisierung der Geschäfts- oder Organisationsleitung
   - Definition des Auftrags und Ziels der Ermittlung
2. Schutz der Beweis- und Betriebsmittel
   - Schutz der Beweismittel vor Modifikation
   - Schutz der Untersuchungsumgebung vor Kontamination Gerichtsverwertbarkeit

Incident Response Prozess (Forts.)

3. Imaging und Datensammlung
   - ▷ Erstellung von 1 : 1 Kopien von Datenträgern
   - ▷ Sammlung von Daten auf einem laufenden System
4. Untersuchung und Bewertung der gewonnenen Informationen
   - ▷ Untersuchung der Kopien von Datenträgern
   - ▷ Bewertung der Relevanz des Beweismittels
5. Dokumentation
   - ▷ Zusammenfassung der gewonnenen Erkenntnisse
   - ▷ Erläuterung der Schlussfolgerungen

Das S-A-P Modell

- Secure-Phase
  - Erfassung der Daten
  - Rückgriff auf Unterstützung vom Werk- oder Objektschutz
  - Protokollierung der durchgeführten Tätigkeiten
  - Einsatz von Hash-Verfahren und dem Vier-Augen-Prinzip
- Analyse-Phase
  - Analyse der gesammelten Spuren
  - Objektive Bewertung der Ergebnisse
- Present-Phase
  - Aufbereitung der Ergebnisse in verständlicher Form
  - Zielgruppenorientierte Präsentation

Gewinnung von Erkenntnissen

Voraussetzung: Unvoreingenommenheit bei der Analyse eines Sicherheitsproblems

Tätigkeiten:

- Einbruchsanalyse
- Schadensfeststellung
- Analyse der Angriffstools
- Logdatei-Analyse
- Suche nach weiteren Spuren

Einbruchs- und Schadensanalyse

Fragen:

- Wer hatte Zugriff?
- Was hat der Angreifer auf dem System gemacht?
- Wann fand der Vorfall statt?
- Welche weiteren Systeme sind noch betroffen?
- Wie erlangte der Angreifer Zugriff?
- Ist der Angreifer noch aktiv?
- Was konnte der Angreifer auf diesem System einsehen?

Analyse der Tools

Fragen:

- Was wurde vom Angreifer zurückgelassen?
- Welche Tools wurden verwendet?
- Wie wurden die Tools aufgerufen?
- In welcher Programmiersprache wurden die Tools geschrieben?
- Gibt es Querbezüge zu Tools und Dateien, die auf dem System eines Tatverdächtigen gefunden wurden?

Logdatei-Analyse

Fragen:

- Welche Logs wurden protokolliert?
- Was wird durch Protokolldaten enthüllt?

Zu untersuchende Systeme:

- Protokolldaten auf den kompromittierten Systemen
- Protokolldaten der Remote-Access-Systeme
- Protokolldaten der Zutrittskontrollsysteme

Weitere Beweissuche

Fragen:

- Was findet sich auf den Datenträgern?
- Welche Spuren sind durch die verwendeten Applikationen hinterlassen worden?
- Welche Dateien wurden gelöscht?
- Existieren versteckte Dateien?
- Existieren verschlüsselte Dateien?
- Existieren versteckte Partitionen?
- Existieren bekannte Hintertür- oder andere Fernzugriffstools?

Korrekter Umgang mit Beweismitteln

- Grundlage für die erfolgreiche Ermittlung möglicher Tatverdächtiger
- Der Verlust der Beweiskraft von digitalen Spuren durch unsachgemäße Behandlung muss verhindert werden
- Insbesondere bei flüchtigen Informationen (z.B. Inhalt des Hauptspeichers) ist ein besonnenes und koordiniertes Handeln erforderlich
- Besondere Sorgfalt ist bei „Smoking Gun“ Umgebungen geboten, wo der Eindringlich noch aktiv ist oder das System gerade verlassen hat

Juristische Bewertung der Beweissituation

- In Deutschland ist ein Richter grundsätzlich in seiner Beweisführung frei
- Die Gerichtsverwertbarkeit von Beweisen hängt davon ab, unter welchen Umständen diese erhoben wurden
- Beweise werden unterteilt in:
  - Sachbeweise: Gegenstände, Spuren, technische Aufzeichnungen, Logdateien, ...
  - Personalbeweise: Zeugen, Sachverständige
- Die Beweiskraft eines Sachbeweises ist an einen Personalbeweis gebunden
- die Integrität einer Person und ihre Glaubwürdigkeit sind wesentliche Elemente des Beweises

Datenschutz

- Bei der Analyse von Sachbeweisen, die personenbezogene Daten enthalten, müssen Aspekte des Datenschutzes berücksichtigt werden
- Grundprinzipien des Datenschutzes:
  - Datenvermeidung
  - Datensparsamkeit
  - Systemdatenschutz als Gesamtziel
  - Anonymisierung
  - Pseudonymisierung
- Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung, oder zur Sicherstellung eines ordnungsgemäßen Betriebes gespeichert werden, dürfen nur für diese Zwecke verwendet werden

Datenschutz bei der Ermittlung

- Der Datenschutzbeauftragte und der Betriebsrat sollten in die Erstellung eines Konzepts für die Sicherheitsvorfallbehandlung einbezogen werden
- Bei Maßnahmen zur Sicherung von flüchtigen Daten sollten der Datenschutzbeauftragte und der Betriebs- bzw. Personalrat zustimmen
- Sollte eine Auswertung von Protokolldaten mit möglicherweise personenbezogenen Daten stattfinden, dann sollte der Datenschutzbeauftragte dieser Auswertung beiwohnen

Datenschutz bei der Ermittlung (Forts.)

- Im Rahmen eines Monitoringkonzepts soll festgelegt werden, welche Daten zu welchem Zweck protokolliert werden
- Alle Personen, die mit der Protokollierung und der genehmigten Auswertung beschäftigt sind, sollten auf das Datenschutzgesetz verpflichtet werden
- Es muss festgelegt werden, dass die aufgezeichneten Daten, die eine Zuordnung von Events auf eine Person ermöglichen, ohne ausdrückliche Genehmigung eines Entscheidungsträgers nicht an Dritte weitergegeben werden dürfen

Ausnahmen für Behörden

- Grundsätzlich darf der Datenschutz bei einer Ermittlung nicht außer Kraft gesetzt werden
- Datenschutz soll kein Tatenschutz (Täterschutz) sein
- Gesetze ermöglichen Ermittlungsbehörden, auch Daten zu sammeln, zu denen sie wegen des Datenschutzes eigentlich keinen Zugang haben
- Ob ein Zugriff bewilligt wird, wird im Einzelfall entschieden
- Die Auskunftspflicht über die Daten wird durch die Zeugeneigenschaft des Dateninhabers bewirkt

Arten der zu erfassenden Daten

Unterscheidung:

- Flüchtige Daten $\rightsquigarrow$ Informationen, die beim geordneten Herunter oder Ausschalten des Systems verloren gehen
- Fragile Daten $\rightsquigarrow$ Informationen, die zwar auf der Festplatte gespeichert sind, aber deren Zustand sich beim Zugriff ändern kann
- Temporär zugreifbare Daten $\rightsquigarrow$ Informationen, die sich auf der Festplatte befinden, aber nur zu bestimmten Zeitpunkten zugänglich sind

Beachte:

- Zur Speicherung der Beweise sollten unbedingt „sterile“ Datenträger zum Einsatz kommen
- Es sollten anerkannte Verfahren und Werkzeuge verwendet werden

Bewertung der Beweisspuren

Ziel: Auffinden der Beweise zur Aufklärung eines Sachverhalts

Unterscheidung:

- Beweisspuren, die eine bestimmte Theorie untermauern
- Beweisspuren, die gegen eine bestimmte Theorie sprechen
- Beweisspuren, die keine bestimmte Theorie unterstützen oder wiederlegen, sondern zeigen, dass das System verändert wurde, um Informationen oder Spuren zu verbergen

Dokumentation der durchgeführten Aktionen

- Alle während der Ermittlung durchgeführten Aktionen müssen dokumentiert werden
- Im Vorfeld sollte ein entsprechendes Dokumentationsformat festgelegt werden
- Die Dokumentation muss für Dritte verständlich sein
- Die Dokumentation muss gegen unberechtigte Veränderung geschützt werden z.B. durch Einsatz einer Prüfsumme
- Verdächtige Daten sind auf jeden Fall zu kopieren
- Screenshots werden mittels einer Digitalkamera erstellt
- Die eingesetzten Tools sollten mit der entsprechenden Versionsnummer notiert werden

Tipps zur Vermeidung von Fehlern

- Die Zeitstempel der Dateien auf dem angegriffenen System dürfen nicht verändert werden
- Tools mit grafischer Oberfläche sollten auf dem betroffenen System nicht verwendet werden
- Verdächtige Prozesse sollten nicht beendet werden
- Es sollten keine unprotokollierten Kommandos ausgeführt werden
- Es dürfen keine vertrauensunwürdigen Programme bzw. Systemtools verwendet werden

Tipps zur Vermeidung von Fehlern (Forts.)

- Security Patches oder Updates sollten nur dann installiert werden, wenn das Response-Team dies empfiehlt
- Software sollte nur dann installiert oder deinstalliert werden, wenn das Response-Team dies empfiehlt
- Protokolle sollten nicht auf die zu untersuchende Platte geschrieben werden
- Ein ordnungsgemäßer Shutdown kann Beweise vernichten

Häufige Fehler bei Ermittlungen

- Kein Incident-Response-Plan in Vorbereitung
- Unterschätzen der Tragweite des Vorfalls
- Keine rechtzeitige Meldung über den Vorfall
- Entscheidungsträger sind nicht oder nur unzureichend informiert
- Die durchgeführten Aktionen wurden nicht durchgängig dokumentiert
- Digitale Beweise sind unzureichend vor Veränderung geschützt

Beweissicherung eines PCs

Ziel: Korrekte Beweissicherung eines Rechners an einem Tatort

Fragen:

- Welche Komponenten des Rechners müssen sichergestellt werden?
- Wie geht man bei der Beweissicherung vor?

Unterscheidung:

- Rechner ist im laufendem Betrieb
- Rechner ist ausgeschaltet

Sicherzustellende Gegenstände

- Haupteinheit, in der alle maßgeblichen Komponenten enthalten sind
- In besonderen Fällen Monitor und Tastatur
- Externe Stromkabel, falls es sich um Spezialkabel handelt
- Externe Festplatten, Disketten, CDs, DVDs, Backup-Bänder, ...
- Externe Kommunikationssysteme, die Identifikation einer Verbindung analysiert werden können
- Dongles für Spezialsoftware
- Digitalkameras und MP3-Player sowie deren Speicherkarten
- PDAs und Mobiltelefone

Sicherstellung eines ausgeschalteten Systems

1. Alle fremden Personen vom System und der Stromversorgung entfernen
2. Umgebung fotografieren bzw. eine Skizze anfertigen
3. Eventuell aktive Druckjobs zu Ende laufen lassen
4. Unter keinen Umständen das System einschalten
5. Sicherstellen, dass das System wirklich ausgeschaltet ist
6. Überprüfen, ob sich das System im Standby-Modus befindet
7. Stromkabel am Gerät entfernen

Sicherstellung ausgeschaltetes System (Forts.)

1. Netzwerkkabel entfernen
2. Alle sichergestellten Geräte und Objekte müssen eindeutig beschriftet werden
3. Nähere Umgebung nach Notizen oder Papierunterlagen durchsuchen
4. Befragung der Anwender nach Besonderheiten des Systems, Passwörtern und Konfigurationsinformationen
5. Dokumentation aller mit der sichergestellten Hardware durchgeführten Tätigkeiten

Sicherstellung eines laufenden Systems

1. Alle fremden Personen vom System und der Stromversorgung entfernen
2. Umgebung fotografieren bzw. eine Skizze anfertigen
3. Nach Möglichkeit Anwender nach Besonderheiten des Systems, Passwörtern oder anderen Konfigurationsspezifika befragen
4. Bildschirminhalte festhalten
5. Tastatur und Maus nach Möglichkeit nicht berühren
6. Falls möglich, eine Live Response durchführen
7. Alle anderen Schritte wie oben beschrieben durchführen

Zusammenfassung

- Wesentliche Aufgabe der Computer Forensik ist die Ermittlung von gerichtsverwertbaren Beweisen in einem Schadensfall
- Das Vorgehen orientiert sich am Incident Response Prozess oder am S-A-P Modell
- Bei den zu erfassenden Daten unterscheidet man zwischen flüchtigen, fragilen und temporär zugreifbaren Daten
- Zur Beweissicherung eines Computers gibt es allgemeingültige Vorgehensweisen