HOCHSCHULE
HANNOVER
UNIVERSITY OF
APPLIED SCIENCES
AND ARTS
–
Fakultät IV
Wirtschaft und
Informatik

Die Grundlagen der Computer-Forensik

Schehat Abdel Kader und Detijon Lushaj

Seminar-Arbeit im Studiengang „Angewandte Informatik“

7. April 2022

Autor 1: Schehat Abdel Kader
1630110
schehat.abdel-kader@stud.hs-hannover.de
Verfasste Seiten/Abschnitte: (8 Seiten)
- 2 Ermittlungsprozess,
- 5 Speichermedien sichern,
- 6 Schluss

Autorin 2: Detijon Lushaj
1630149
detijon.lushaj@stud.hs-hannover.de
Verfasste Seiten/Abschnitte: (8 Seiten)
- 1 Einleitung,
- 3 Juristische Beweisführung,
- 4 System sicherstellen

Prüferin: Prof. Dr. Frank Müller
Abteilung Informatik, Fakultät IV
Hochschule Hannover
frank.mueller@hs-hannover.de

Selbständigkeitserklärung

Mit der Abgabe der Ausarbeitung erklären wir, dass wir die eingereichte Seminar-Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die von uns angegebenen Quellen und Hilfsmittel nicht benutzt und die den benutzten Werken wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht haben.

Hannover, den 7. April 2022

Inhaltsverzeichnis

1 Einleitung

In der Seminararbeit werden die Grundlagen der Computerforensik eingeführt und erläutert. Bietet eine kurze Einführung in die Methoden der Computerforensik und listet die Anforderungen an forensische Untersuchungen und Beweissicherung auf.

1.1 Motivation

Die heutige Welt wird von Computern dominiert. Auch die tägliche Nutzung von Computern in den unterschiedlichsten Branchen erhöht das Missbrauchsrisiko. Die Zahl der Straftaten im Zusammenhang mit Computern, hat in den letzten Jahrzehnten exponentiell zugenommen. Auch ein Bericht des Bundesamtes für Sicherheit in der Informationstechnik zeigte eine generelle Zunahme potenzieller Risiken. [2]

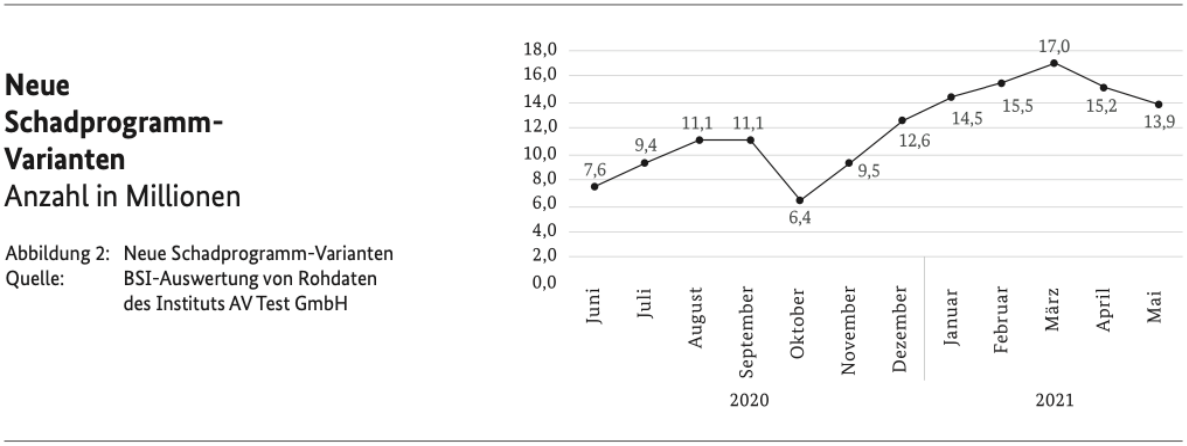

Abbildung 1: Neue Schadprogramm-Variante 2021 des BSI

Bei diesen Straftaten handelt es sich hauptsächlich um Betrug und Vandalismus. Aufgrund der dramatischen Zunahme von Straftaten wächst auch das Interesse an Methoden zur Strafverfolgung oder Ermittlung von Tätern, Schadensersatz und Prävention dieser Straftaten.

1.2 Ziel der Arbeit

In dieser Seminararbeit werden die verschiedenen Phasen des Ermittlungsprozesses erläutert. Wir geben auch Auskunft darüber, welche Spuren auf kompromittierten Systemen gefunden wurden und welche Daten aufgezeichnet werden müssen, und die ersten Schritte nach einem Vorfall.

1.3 Begriffserklärung Computer-Forensik

Der Begriff „Computerforensik“ bezeichnet die Analyse und Aufklärung von Sicherheitsvorfällen. Menschen suchen wie in anderen Bereichen der Forensik nach digitalen Spuren, die Hinweise auf Verbrechen liefern sollen. Typische Beispiele sind Hackerangriffe oder Datenschutzverletzungen durch Insider. Computerforensische Untersuchungen werden immer unmittelbar nach einer Straftat oder einem Verdachtsfall durchgeführt. [1]

2 Ermittlungsprozess

2.1 Ziel

Der Zweck einer forensischen Untersuchung besteht darin, Beweise zu liefern, um die Hypothese zu stützen, dass das System kompromittiert wurde. In diesem Fall führt ein Expertenteam eine forensische Untersuchung durch, um aufzudecken, ob und wann ein System angegriffen wurde, wer die mutmaßlichen Täter waren und welche Sicherheitslücken ausgenutzt werden konnten, um das System zu infiltrieren. Darüber hinaus soll die forensische Analyse das Ausmaß des Schadens ermitteln und Beweise zum Sicherheitsvorfall für weitere rechtliche Schritte sichern. Die Schwierigkeit beim Erreichen dieser Ziele liegt darin, die richtigen Daten sicher zu sammeln, ohne den Zustand des komprimiertem Systems zu ändern[1].

2.2 Anforderungen

Idealerweise werden zum Abschluss der Ermittlung die Ermittlungsergebnisse präsentiert, falls diese Angelegenheit juristisch geklärt werden soll vor Gericht. Damit die gesammelten Beweise im Prozess nicht an Bedeutung verlieren, müssen die verwenden Werkzeuge und Methoden bei der Ermittlung angemessen gewählt werden. Dritte verfügen meistens nicht über die gleiche technischen Kompetenz wie die Ermittler, weshalb die Vorgehensweise bei der Ermittlung nachvollziehbar sein soll.

Die eingesetzten Methoden und Werkzeuge sollten allgemein anerkannt und beschrieben sein. Die Funktionalität und Robustheit der Methoden sollte nachgewiesen werden können, um Reproduzierbarkeit zu gewährleisten, sodass Dritte bei der gleichen Vorgehensweise identische Ergebnisse erzielen. Damit die Beweise juristisch belastbar sind, dürfen die Spuren während der Ermittlungen nicht unbemerkt verändert werden können. Für jede glaubwürdige Ermittlung ist eine detaillierte Dokumentation unverzichtbar, sodass die an der Untersuchung unbeteiligten Personen den Ermittlungsprozess nachvollziehen können[1].

2.3 SAP-Model

3 Juristische Beweisführung

3.1 Datenschutz

3.2 erfasste Daten

3.3 Beweise dokumentieren

4 Ersten Schritte

4.1 System Sicherstellung

Unabhängig welches Betriebssystem man verwendet sind beim Schutz verdächtiger Client-PCs einige allgemeine Schritte zu beachten. Bei Serversystemen kann es zu abweichenden Handlungen kommen. In jedem Fall sollten man sich vorher überlegen, wie man im Falle einer eigenverantwortlichen Beschlagnahme vorgehen. [1] [3]

4.1.1 Fall 1: System läuft nicht (ist ausgeschaltet)

Wir betrachten nun den Fall das, dass System nicht läuft (ist ausgeschaltet):
Zunächst ist es wichtig, alle fremden Personen vom System und der Stromversorgung zu entfernen. Es sind Umgebungsfotos anzufertigen und ggf. Skizzen (vom Standort der Systeme und Peripherie-Geräte) anzufertigen. Ein laufender Prozess ()wie z. B. Druckjobs) sollte man zu Ende laufen lassen. Das System darf auf keinen Fall eingeschaltet werden. Es sollte beachtet werden, dass das System eingeschaltet werden kann, nachdem der Laptopdeckel geöffnet wurde. Man sollte Sicherstellen, dass das System tatsächlich heruntergefahren ist. Bei Laptops können Sie den Akku entfernen, um sicherzustellen, dass der Energiemodus nicht aktiviert wird und möglicherweise der Zeitstempel geändern wird. Andernfalls sollten die Netzkabel von den Geräten abgezogen werden. Wenn die WakeOnLan-Funktion eingebaut ist, sollte auch das Netzkabel entfernt werden. Wichtig ist auch, dass alle beschlagnahmten Gegenstände eindeutig gekennzeichnet werden. Es sollte auch in den Berechen nach Notizen und Papieraufzeichnungen durchsucht werden. Wenn möglich, sollte der Anwender nach Besonderheiten des Systems, Passwörtern oder anderen spezifischen Konfigurationen des Systems gefragt werden. Die Antworten sollten genau aufgezeichnet und bei Bedarf kritisch hinterfragt werden. Es ist wichtig, eine vollständige Dokumentation aller Aktivitäten, die mit beschlagnahmter Hardware durchgeführt wurden, zu führen. [1] [3]

4.1.2 Fall 2: System läuft (ist eingeschaltet)

Wir betrachten nun den Fall das, dass System läuft (ist eingeschaltet):
Zunächst ist es wichtig, alle fremden Personen vom System und der Stromversorgung zu entfernen. Es sind Umgebungsfotos anzufertigen und ggf. Skizzen (vom Standort der Systeme und Peripherie-Geräte) anzufertigen. Wenn möglich, sollte der Anwender nach Besonderheiten des Systems, Passwörtern oder anderen spezifischen Konfigurationen des Systems gefragt werden. Die Antworten sollten genau aufgezeichnet und bei Bedarf kritisch hinterfragt werden. Alle Bildschirminhalte sollten mit einer Digitalkamera oder einem ähnlichen Gerät erfasst werden. Es ist auch wichtig, Peripheriegeräte nicht zu berühren(Es geht um den Zeitstempel). Wenn unter Umständen etwas geändert werden

muss, sollte dies notiert und die Erlaubnis des Ermittlungsleiter eingeholt werden. Es ist wichtig, alle Aktivitäten zeitgenau aufzuzeichnen. [1] [3].

4.1.3 Entscheidungsprozesse

Jeder Sicherheitsvorfall ist individuell und kann besondere Entscheidungen erfordern. Eine Weiterleitung an ein beliebig höheres Glied der Digitalen Rettungskette ist notwendig, wenn die ausgesprochenen Handlungsempfehlungen die Problematik nicht lösen konnten oder keine eindeutige Bestimmung des Sachverhaltes nicht möglich ist. In Anlehnung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik kann das folgende Ablaufdiagramm als Basis dienen. [3]

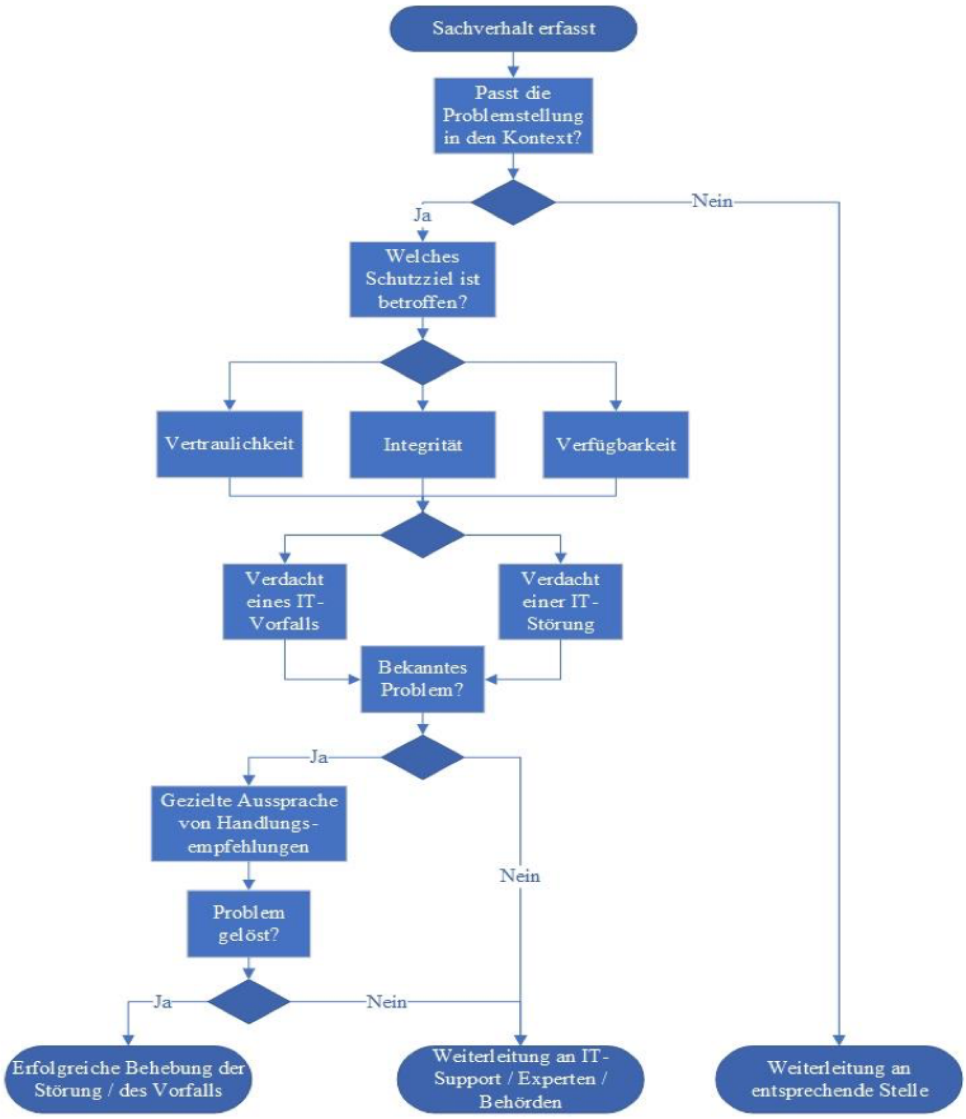

Abbildung 2: Entscheidungsmatrix

4.2 Speichermedien sichern

4.2.1 Flüchtige Datenträger

4.2.2 Persistente Datenträger

5 Schluss

Literatur

[1] Alexander Geschonneck. Computer-Forensik : Computerstraftaten erkennen, ermitteln, aufklären. dpunkt.verlag GmbHl, 2014.

[2] BSI: Die Lage der IT-Sicherheit in Deutschland 2021

[3] BSI: Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer