Computer Forensik

Seminar Analyse & Angriffe auf Netzwerke

Version 0.1

Zürcher Hochschule für Angewandte Wissenschaften

Daniel Brun

xx. Juni 2015

Eigenständigkeitserklärung

Hiermit bestätigt ich, dass vorliegende Seminararbeit zum Thema „Evaluation einer Mini ERP Lösung für einen Verein“ gemäss freigegebener Aufgabenstellung ohne jede fremde Hilfe und unter Benutzung der angegebenen Quellen im Rahmen der gültigen Reglemente selbständig verfasst wurde.

Thalwil, 11. Februar 2015 Daniel Brun

Inhaltsverzeichnis

1 Einleitung **1**
- 1.1 Hintergrund . . . 1
- 1.2 Aufgabenstellung . . . 1
- 1.3 Abgrenzung . . . 1
- 1.4 Motivation . . . 2
  - 1.4.1 Computerkriminalität . . . 2
- 1.5 Struktur . . . 2

2 Angriffe, Incident Detection & Incident Response **3**
- 2.1 Angriffe . . . 3
  - 2.1.1 Angriffstypen . . . 3
  - 2.1.2 Kategorien von Schwachstellen . . . 4
  - 2.1.3 Komplexität . . . 4
  - 2.1.4 Täter . . . 4
  - 2.1.5 Typischer Ablauf . . . 5
    - Survey (Untersuchung) . . . 5
    - Delivery (Positionierung) . . . 5
    - Breach (Ausnutzung) . . . 5
    - Affect (Beeinträchtigung / Infizierung) . . . 6
    - Clean Up (Aufräumen) . . . 6
- 2.2 Incident Detection (Erkennung eines Vorfalls) . . . 6
  - 2.2.1 Hinweise Netzwerkseitig . . . 6
  - 2.2.2 Hinweise Serverseitig . . . 6
  - 2.2.3 Hinweise durch Intrusion-Detection-Systeme . . . 7
  - 2.2.4 Weitere Hinweise . . . 7
  - 2.2.5 Meldung eines Vorfalles . . . 7
- 2.3 Incident Response Team . . . 8
- 2.4 Incident Response . . . 8
  - 2.4.1 Reaktionsarten . . . 9
    - Härtung der Systeme, Abwehr des Angriffes . . . 9
    - Abwarten, Beobachten, Informationen sammeln . . . 9
- 2.5 Ablauf . . . 10

3 Computer Forensik **11**
3.1 Einbettung und Definition . . . 11
3.1.1 Forensik . . . 11
Ursprung . . . 11
Bedeutung . . . 11
Teilbereiche . . . 12
3.1.2 IT- / Digitale Forensik . . . 12
Teilbereiche . . . 12
3.1.3 Computer Forensik . . . 13
3.2 Einführung . . . 13
3.3 Hinweise für die juristische Verwertbarkeit . . . 13
3.3.1 Methoden, Techniken und Programme . . . 13
3.3.2 Glaubwürdigkeit und Reproduzierbarkeit . . . 13
3.3.3 Integrität . . . 14
3.3.4 Präsentation und Dokumentation . . . 14
3.4 Hinweise zum Datenschutz . . . 14
3.5 Themengebiete und Teilbereiche . . . 14
3.6 Anwendungsbereich . . . 14
3.7 Ziele . . . 15
3.8 Ausbildung & Zertifizierung . . . 15
3.9 Sicherungsebenen . . . 15
3.10 Unterscheidung Daten-Typen . . . 15
3.11 Anti-Forensik und Anti-Detection . . . 15

4 Forensische Analyse **17**
4.1 Ablauf . . . 17
4.2 Techniken . . . 18
4.2.1 Aktuelle Prozesse . . . 18
4.2.2 Shutdown . . . 18
4.3 Ablauf . . . 18
4.4 Hinweise . . . 18
4.4.1 Vorbereitung . . . 18
4.4.2 Secure . . . 19
4.4.3 Erste Schritte . . . 20
System ist ausgeschaltet . . . 20
System ist eingeschaltet . . . 20
4.4.4 Analyse . . . 20
4.4.5 Dokumentation . . . 21

5 Tools und Techniken **23**
5.1 Image-Related / Data-Aquisitation . . . 23
5.1.1 Laufwerk löschen . . . 23
5.1.2 Image erstellen . . . 23
5.1.3 Image verifizieren . . . 23

5.2 Gelöschte Datenträger 23
5.3 Kommerzielle Tools 24

Quellenverzeichnis **25**

Anhang **31**

A Vorlage: Protokoll **31**

B Vorlage: Beweiszettel **33**

Liste der noch zu erledigenden Punkte **35**

KAPITEL 1

Einleitung

Hinweis männlich / weibliche Form

1.1 Hintergrund

Im Rahmen meines Bachelor-Studiums in Informatik an der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) muss im 6. Semester eine Seminararbeit zu einem vorgegebenen Themenbereich erarbeitet werden. Ich habe mich für den Themenbereich „Analyse und Angriffe auf Netzwerke“ entschieden.

Es einem Themenkatalog konnte ein spezifisches Thema im Bereich „Analyse und Angriffe auf Netzwerke“ ausgewählt werden. Ich habe mich für das Thema „Computer Forensik“ entschieden.

Für die Arbeit sollen circa 50 Arbeitsstunden aufgewendet werden. Dies entspricht etwa einem Umfang von 15 bis 20 Seiten. Zusätzlich gelten die Rahmenbedingungen gemäss dem Reglement zur Verfassung einer Seminararbeit ([Ste12])

1.2 Aufgabenstellung

In dieser Arbeit soll ein Überblick über das Themengebiet der „Computer Forensik“ erarbeitet werden. Es soll gezeigt werden was für Themenbereiche es gibt und was für Werkzeuge und Tools eingesetzt werden können. Das Ganze soll mit einem Ablauf einer forensischen Untersuchung und entsprechenden Beispielen illustriert werden.

1.3 Abgrenzung

Aufgrund des grossen Themengebietes können nicht alle Detail-Aspekte der Computer Forensik berücksichtigt werden. Daher werden in dieser Arbeit nur die wichtigsten Aspekte der Computer Forensik näher betrachtet.

-Unix-Systeme -Normale / Einzelsysteme (ohne RAID, etc.)

Weitere Abgrenzungen

1.4 Motivation

1.4.1 Computerkriminalität

Stetiger Zuwachs an Themenkreis: Ausführung von Taten in Kenntnis bzw. unter Einsatz von Computer- bzw. Kommunikationstechnologie, die Verletzung von Eigentum an Sachwerten sowie Verfügungsrechten an immateriellen Gütern und die Beeinträchtigung von Computer- bzw. Kommunikationstechnologien.

Erweiterter Bereich: Sämtliche Straftaten, die mit Hilfe oder Unterstützung von informationsverarbeitenden Systemen vorgenommen werden

Delikte: Computerbetrug, Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten, Betrug mit Konto- oder EC-Karten mit PIN, Private Softwarepiraterie, Gewerbsmässige Softwarepiraterie, Datenveränderung und Computersabotage, Fälschungn beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung, Ausspähen von Daten

Angreifer: Cyberkriminelle, Konkurrenten, Nachrichtendienste, Hackers, Hacktivisten, Mitarbeiter

1.5 Struktur

Struktur erklären

Diese Arbeit gliedert sich in folgende Hauptteile:

- Ausgangslage
- Analyse
- Evaluation
- Schlusswort

Im ersten Kapitel werden die Details zur Ausgangslage und die Hintergründe der Arbeit aufgezeigt. Im zweiten Kapitel wird mit Hilfe einer Umfrage innerhalb des Turnvereins eine Analyse erstellt. Aus dieser Analyse gehen die Randbedingungen, Ziele und Anforderungen an das Mini Enterprise-Resource-Planning (ERP) System hervor. Diese Randbedingungen, Ziele und Anforderungen werden im Kapitel 'Evaluation' als Kriterien für die Vorselektion, Selektion und anschliessenden die Evaluation der Produkte verwendet. Im letzten Kapitel wird ein Fazit gezogen, eine Empfehlung an den abgegeben und über die gesamte Arbeit reflektiert.

KAPITEL 2

Angriffe, Incident Detection & Incident Response

In diesem Kapitel wird erläutert, wie typische Angriffe ablaufen, wie diese erkannt und anschliessend entsprechend reagiert werden kann.

2.1 Angriffe

Für die Reaktion auf Angriffe und die Untersuchung von Angriffen ist es wichtig die grundlegenden Angriffsverfahren, -methoden und -techniken zu verstehen. In diesem Kapitel werden die wichtigsten Punkte erläutert.

2.1.1 Angriffstypen

Grundsätzlich können zwei Angriffstypen unterschieden werden. Auf der einen Seite stehen Massenangriffe, so genannte „un-targeted attacks“, deren Ziel es ist so viele Geräte oder Services als möglich zu treffen. Das einzelne Opfer spielt dabei eine untergeordnete Rolle. Phising und Malware sind zwei Beispiele für solche Massenangriffe. Ausgenutzt wird hier grundsätzlich immer die Offenheit des Internets.

Auf der anderen Seite stehen gezielte Angriffe, so genannte „targeted attacks“. Diese Attacken sind in der Regel auf das Ziel oder das spezifische Szenario, massgeschneidert. Solche Angriffe werden über mehrere Monate hinweg geplant und vorbereitet. Oft sind diese Codes spezifisch entwickelt worden und können somit von Intrusion-Detection-Systemen und Anti-Viren-Software nicht oder nur sehr schwer erkannt werden. Ein Beispielt für eine solche Attacke wäre Spear-Phising.

Bei den gezielten Angriffen hat sich in den letzten Jahren eine neue Unterkategorie, die Kategorie der „advanced persistent threats“. Ziel dieser Angriffe ist es, möglichst lange unerkannt zu bleiben und den Einbruch zu vertuschen. Dabei werden gerade so viele Daten gesammelt, bzw. Aktionen durchgeführt, dass der Täter noch unerkannt bleibt. Ein solcher Angriff wird über mehrere Monate, wenn nicht sogar Jahre, hinweg vorbereitet und anschliessend Schritt für Schritt umgesetzt. Auch der eingesetzte Schadcode wird so

gebaut, dass dieser möglichst lange unterkannt bliebt, aber trotzdem so viel Nutzen als möglich erbringen kann.

2.1.2 Kategorien von Schwachstellen

Bei einem Angriff werden immer vorhandene Schwachstellen ausgenutzt. Diese Schwachstellen können in drei Kategorien unterteilt werden.

- **Flaws (Fehler / Mängel)**
  Bei einem Flaw handelt es sich um eine unbeabsichtigte Funktionalität der Anwendung. Dieser kann entweder durch schlechtes Design oder simpel und einfach durch einen Implementierungsfehler entstehen.
- **Features (Funktionalitäten)**
  Hier wird eine vorhandene Funktionalität für andere Zwecke missbraucht. Dabei handelt es sich um keinen Fehler in der Anwendungen, sondern um eine Funktionalität, welche entsprechend spezifiziert wurde.
- **User Errors (Benutzer Fehler)**
  User Errors werden durch den Benutzer verursacht. Zum Beispiel könnte ein unerfahrener Systemadministrator unwissentlich Schwachstellen im System freischalten.

2.1.3 Komplexität

Durch die vorherrschende Monokultur von Betriebsystemen, Anwendungen und Komponenten werden die Anforderungen an Hacker immer grösser. Mit den steigenden Anforderungen werden auch die Angriffe und die Angriffstechniken immer komplexer.

Bild CF Seite 13

2.1.4 Täter

Die Motivation von Tätern sind sehr unterschiedlich. Dies reicht von Sozielen, politischen, finanziellen, staatlich-politischen Motivationen über technische Ambitionen bis hin zu Regierungen oder Gruppierungen wie Anonymous. Neben der Motivation können die Täter nach Aussen- und Innentätern unterschieden werden. Innentäter verfügen über Insider-Wissen und arbeiten in der Regel für das angegriffene Unternehmen oder die angegriffene Organisation. Der Anteil an Innentätern am gesamten Tätervolumen ist sehr hoch und wächst stetig. Unternehmen und Organisationen sind sich dessen aber nicht immer bewusst und wähnen sich in falscher Sicherheit.

Die „Berufsbezeichnungen“ der Täter sind sehr unterschiedlich und vielfältig. Nachfolgend sind einige der gängigsten Bezeichnungen und deren Bedeutung aufgelistet.

Vervollständigen

- **Elite**

- **Hacker**
  Neutraler Begriff
- **Cracker**
  Negativ
- **Script Kiddy**

- **White-Hat**
  Berücksichtigung Hackerethik, Penetrationstests
- **Gray-Hats**

- **Black-Hats**
  ...

2.1.5 Typischer Ablauf

Ein Angriff kann in die nachfolgenden Phasen gegliedert werden. Diese können je nach Angriff in unterschiedlichen Ausprägungen vorkommen.

Survey (Untersuchung)

In dieser Phase werden so viele Informationen wie möglich gesammelt. Dazu gehören Informationen über die Organisation, die eingesetzte Hard- und Software und Prozesse. Anschliessend wird versucht so viele Schwachstellen wie möglich zu ermitteln. Zum einen wird ein Footprinting durchgeführt, welches so viele Informationen wie möglich über die Systeme zu Tage befördern soll. Zum Footprinting gehören unter anderem Port- und Protokollscanns und DNS- und WHOIS-Abfragen. Zum anderen werden mit Hilfe von Social Engeineering und Commodity-Toolkits und -Techniken weitere Schwachstellen ermittelt.

Delivery (Positionierung)

Diese Phase beschäftigt sich mit den expliziten Vorbereitungen für die Ausnutzung der Schwachstellen. Der Angreifer versucht das für dieses Szenario am besten geeignete Vorgehen zu ermitteln und bringt sich anschliessend in Position um die Schwachstellen auszunutzen. Eine typische Aktion in dieser Phase wäre zum Beispiel der Versand einer infizierten E-Mail oder das Unterjubeln eines inifizierten USB-Sticks.

Breach (Ausnutzung)

In dieser Phase wird die Schwachstelle ausgenutzt, um dem Angreifer Zugang zum gewünschten System zu verschaffen.

Affect (Beeinträchtigung / Infizierung)

Nach dem der Angreifer Zugang zum System erlangt hat, unternimmt er weitere Schritte um sein eigentliches Ziel zu erreichen. Dies kann zum Beispiel die Erweiterung seiner Zugriffsrechte, die Einrichtung von Hintertüren, die Sammlung von Daten oder der Angriff eines weiteren Systemes sein.

Clean Up (Aufräumen)

Je nach Ziel und Zweck des Angreifers verwischt er seine Spuren und räumt auf, damit er unerkannt bleibt oder allenfalls zu einem späteren Zeitpunkt nochmals zurückkehren kann.

2.2 Incident Detection (Erkennung eines Vorfalls)

Bevor auf einen Angriff, beziehungsweise auf einen Sicherheitsvorfall, reagiert werden kann muss dieser zuerst bemerkt werden. Bleibt der Vorfall unterkannt, wird es nie zu einer Untersuchung kommen. Ein Angriff kann durch verschiedenste Indikatoren erkannt und zum Teil sogar vorausgesagt werden. Nachfolgend werden einige dieser Indikatoren aufgelistet.

2.2.1 Hinweise Netzwerkseitig

- Ungewöhnlich hohe Netzwerklast
- Ungewähnliche Anzahl Firewall-Regelverstösse

2.2.2 Hinweise Serverseitig

- Unbekannte Prozesse
- Unbekannte / Neue User
- Unbekannte Dateien
- Ungewöhnliche Systemlast
- Dienste laufen nicht mehr
- Ungewöhnliche Systemanmeldungen
- Systemabsturz
- Kleiner werdende Log-Files
- Bestehende Dateien werden grösser (Beispiel: Ausführbare Datei wächst um mehrere kB)
- Versuch Berechtigungen zu verändern

- Schlechte Performance

2.2.3 Hinweise durch Intrusion-Detection-Systeme

Intrusion-Detection-Systeme sind dazu da Angriffe möglichst früh zu erkennen und die entsprechenden Stellen zu informieren. Ist das Intrusion-Detection-System gut konfiguriert, kann dieses Angriffe anhand von Strategien und Mustern erkennen.

Data Loss Prevention Technology

2.2.4 Weitere Hinweise

Weitere Hinweise können durch Kunden, Partner, Mitarbeiter, Strafverfolgungsbehörden oder die Presse erfolgen.

Intrustion-Mapping-Systeme

2.2.5 Meldung eines Vorfalles

-Richtige Informationen abfragen (Merkblatt / Chekliste) –Basisinfos: Aktuelle Uhrzeit, Wer / Welches System berichtet Vorfall, Art und Weise Vorfall, Vermuteter Zeitpunkt Vorfall, mittelbar / unmittelbar betroffene HW / SW, evtl. Auswirkungen, Schaden, Kontakstelle für ISR und Ermittler –Infos über betroffenes System sammeln (!! möglichst nicht vom System abfragen, Datenklassifizierung? Klassifizierung? Ort?, Physischer Zugang? allgemeiner Systemzustand,) –Angreifer: Infos? noch aktiv? Systeme / Daten manipuliert / zerstört, Vermutungen? –Getroffene Massnahmen / System verändert? Andere Perosnen benachrichtigt?

Beurteilung Vorfall / Störung: Kentnisse aktueller Status, Organisation, Landschaft, MA, nicht zu lange warten, Durchleuchtug / Ausschlussverfahren

Bei Einbruch: erste Risikoabschützung für möglcihe Abschaltzung / Netzdekonnektion, Berücksichtigung weiterer Ermittlungsschritte

Entscheid Abschaltung / Dekonnektion: Management der Systemeigentümer, Basis: Empfehlung ISR

Klassifizierung des Vorfalls: Probing / Portscanning, Denial-of–service-Angriff, Unberechtigter Zugriff auf User-Account, ... Admin-Account, Datendiebstahl / -manipulation,

...

Wichtig ist, dass nach einer Incident Detection das Incident Response Team unverzüglich Informiert wird. Ist kein Incident Response Team vorhanden und gibt es in der Unternehmung keine entpsrechende Anlaufstelle, ist das Vorgehen mit.... Keine übereilten Reaktionen, da der Angreifer allenfalls etwas bemerkt

2.3 Incident Response Team

Rasch und richtig handeln Eingreiftruppe bei Incidents, Häufig durch Situation bedingt, wer wegen Detailkenntnisse in Gruppe gehört, Augenmerk: Erfahrene Personen für Schlüsselpositionen, Integrität und Zuverlässigkeit MA, passendes Persönlichkeitsprofil (gesunder Menschenverstand,Fähigkeit effiziente und annehmbare Entscheide zu treffen in krit Sit., gute Kommunikationsfähigkeiten, an Regeln / Prozeduren halten, Arbeiten unter Stress, Teamfähig, Vorbild Sicherheitsrelevante Tätigkeiten, Priorisierung utner Stress)

Bei grösseren Organisationen / IT-Abhängige: Evtl. Dauerhaft in Belegschaft, Wahrnehmung anderer Sicherhietsaufgaben, Früherkennung, Personen: Leiter, Kontaktperson bei Verdacht, etc., Spezialist: Erfassung / Behanldung Vorfall, Spezialist: Schwachstellen, Spezialist auf Plattform, Schulungspersonal

Wichtig: Koordinator, direkter Zugang zum Mgmt

-Ermittler, IT-Professionals (Technical support staff, system, network, security admin): small number of forensic tools according to their area of expertise, -Incident-Handlers (respond to variaty of computer security incidents, wide variety of forensiq technique and tools, knowledge of forensic principles, guidelines, procedures, ...)

-Legal advisors, hr, auditors, physical security staff

2.4 Incident Response

Nach dem der Angriff entdeckt wurde oder Anzeichen für einen zukünftigen Angriff bestehen müssen entsprechende Massnahmen in die Wege geleitet werden. Die einzuleitenden Massnahmen sind dabei von der gewählten Reaktionsart abhängig. Es sind folgende zwei Reaktionen denkbar

Teil der Computer Forensik

Bei Einbruch: in kurzer Zeit: Schaden, Angriffsmethoden und mögliche weitere Auswirkungen für Org. beurteilt werden Notwendig: guter Beweissicherungsmassnahmen im Prozess etablieren

Guter Incident Response Prozess / erfolgreicher Ablauf Incident Response: Basis für juristische Verfolgung

Wichtig: Ermittlung Ursaxche, grundlage für zukünftige Handlungsempfehlungen

organisatorische Vorarbeit notwendig, um korrekt reagieren zu können. wenn nicht: im Entscheidenden Moment keine Ressourcen -Incident Awareness: Beteiligte MA, Bewusstsein -Grobes Konzept Sicherheitsvorfallbehandlung (Eskalations- / Alarmierungsregelung, Weisungskompetenzen) -Security-Monitoring- und Alarmierungskonzept (Einbezug: Personalvertreter, Datenschutzbeauftragter für Datenauswertung) -Weiterbildungen: Incident-Detection / Response -Kontakt zu Security-Spezialisten / Ermittlungsbehörden aufbauen -....

Strategie, zwei Aspekte berücksichtigen: direkten / indirekten Schaden minimieren, Tathergang möglichst umfassend rekonstruieren zur Identifikation Tatverdächtige, jeder Sicherheitsvorfall erfordert andere Strategie -Kritkialität System im Bezug auf Unternehmensprozesse -Kritikalität / Wichtigkeit gestohlene Daten -Täger-Vermutung? -Vermutung Fähigkeiten / Wissen beim Täter -Vorfall an Öffentlichkeit gelangt? -Wie weit ist der Täter gekommen -Verkraftbare Downtime? -Vermuteter finanzieller Gesamtverlust

-Kein unüberlegter Gegenangriff, Angriffer bemerkt, evtl. zerstörung, -Honeypots

Infos: Business Impact, ... Vorfall analysieren, Schlüsse ziehen, Lerneffekt, Ermittlungsvorgang analysieren (Optimierung / Verbesserung), Reaktionszeit, Wirksamkeit, Tätermotivation, Kosten

- Härtung der Systeme, Abwehr des Angriffes
- Abwarten, Beobachten, Informationen sammeln.

2.4.1 Reaktionsarten

Bei der Auswahl von geeigneten Massnahmen ist immer auch der Zeitpunkt der Angriffes zu beachten.

- Angriff in der Zukunft
- Angriff ist am Laufen
- Angriff ist schon vorbei

Härtung der Systeme, Abwehr des Angriffes

Abwarten, Beobachten, Informationen sammeln

- Eigentlicher Angriff noch ausstehend, Härtung und Abwehr
- Eigentlicher Angriff noch ausstehend, Abwarten, Beobachten, Informationen sammeln, Backtracing
- Angriff am Laufen, Abwehr (Härtung)
- Angriff am Laufen, Abwarten, Beobachten, Informationen

Evtl. übergreifendes Kapitel

2.5 Ablauf

- Systemeinbruch oder normale Betriebsstörung?))
- Wahrnehmung / Bemerkung ungewöhnliche Aktivitäten (Administrator, Anwender, ...)
- Evtl. weitere Beobachtung
- Kurze Analyse / Sammlung von Spuren
- Bestätigung Verdacht
- Meldung an Incident Response Team
- Sicherstellung elektronische Beweise
- Beweisspuren identifizieren
- Beweisspuren analysieren
- Analyseergebnisse interpretieren / verifizieren
- Analyseergebnisse in Bericht zusammenfassen / präsentieren.

-Identify -Assess (if is security incident), check, gather information -Respond: Kick of procedure –Initial Response: Determine origin, idenitfy compromised systems, evtl. disconnect from nw, untersuchung starten, Anzeige: Sicherung beweise –Recovery Report Review

Organisatorische Vorbereitung: Rollen, Verantowrtlichkeiten, Policies, Vorbereitende / Unterstützende Massnahmen im Rahmen System Life Cycle (Zentralisierte Logs, Auditing für Server, Arbeitsplatzcomputer, ..., file hashes für verbreitete Betriebssysteme und Installationen, File integrity checking software, data retention policies, etc.), Guidelines, Step-By-Step- Procedures

KAPITEL 3

Computer Forensik

Dieses Kapitel definiert den Begriff der Computer Forensik und beschreibt das Themengebiet im Allgemeinen.

3.1 Einbettung und Definition

3.1.1 Forensik

Ursprung

Der Begriff „Forensik“ stammt aus den Zeiten des antiken Roms. Damals wurden Gerichtsverfahren, Untersuchungen, Urteilsverkündungen und der Vollzug von Strafen öffentlich auf dem Marktplatz abgehalten. Marktplatz (oder auch Forum) wird im lateinischen mit *forum* bezeichnet. Die Plural-Form von *forum* ist *foren*. Aus dieser Plural-Form hat sich der Begriff „Forensik“ entwickelt.

Bedeutung

Die Forensik ist ein Wissenschaftszweig, welche sich mit dem Nachweis, Beweis und der Aufklärung von kriminellen, oder allgemein strafbaren, Handlungen beschäftigt. Die forensische Untersuchung ist eine systematische Analyse mit dem Ziel strafbare Handlungen zu identifizieren, analysieren und rekonstruieren.

Der „Guide to Integrating Forensic Techniques into Incident Response“ des National Institute of Standards and Technology (NIST) beinhaltet eine kurze und prägnante Definition für den Begriff der „Forensik“.

„Forensic science is generally defined as the application of science to the law“
[E20d, S. ES-1]

Übersetzt bedeutet dies so viel wie „Forensische Wissenschaft ist allgemein definiert, als die Anwendung der Wissenschaft für das Gesetz“.

Teilbereiche

Wie in der vorangehenden Definition bereits angedeutet, gibt es grundsätzlich für jeden Wissenschaftszweig einen entsprechenden Wissenschaftszweig in der Forensik. Nachfolgend sind einige für die Strafverfolgung bedeutensten Teilbereiche der Forensik aufgelistet.

- Forensische Pathologie
- Forensische Kriminaltechnik
- Forensische Phsychiatrie und Psychologie
- Forensische Toxikologie
- Ballistik
- Computer-Forensik

3.1.2 IT- / Digitale Forensik

Die IT-, bzw. Digitale, Forensik beschäftigt sich mit der Auffindung, Untersuchung und Wiederherstellung von Material, bzw. Daten, auf elektronischen, bzw. digitalen, Geräten. Dabei kann es sich zum Beispiel sowohl um verlorene Daten, als auch um explizites oder nicht explizites Beweismaterial handeln.

Teilbereiche

Die Unterteilung der IT- / Digitalen Forensik in ihre Teilgebiete ist nicht offiziell definiert. Nachfolgend wird eine mögliche Unterteilung aufgezeigt. Diese Unterteilung ist nicht vollständig und nicht abschliessend.

- Computer Forensik
- Forensische Datananalyse
- Datenbank Forensik
- Mobile Device Forensik
- Netzwerk Forensik
- Forensische Videoanalyse
- Forensische Audioanalyse

3.1.3 Computer Forensik

Für die Definition der Computer Forensik existieren zum heutigen zwei verschiedene Ansätze. Ein Ansatz sieht die Computer Forensik als Teilgebiet der IT-, bzw. der Digitalen Forensik. Der andere Ansatz betrachtet den Begriff Computer Forensik als Synonym zu den Begriffen IT- und Digitale Forensik.

Diese Arbeit richtet sich nach dem ersten Ansatz, bei dem die Computer Forensik ein Teilgebiet der Digitalen Forensik ist.

Definition Computer Forensik

Grafik Einbettung

3.2 Einführung

Die Computer Forensik kann in verschiedenen Kontexten zum Einsatz kommen. Zum einen erfolgt während, bzw. nach einem Sicherheitsvorfall (Incident), z.B. Systeminbruch eine forensische Untersuchung (Mehr dazu im Kapitel **??**).

Im Kontext der Incident Response ist es das Ziel der Computerforensik die ausgenutzte Schwachstelle zu finden, den Schaden zu beziffern, den Angreifer zu Identifizieren und die Beweise für allfällige juristsiche Schritte zu sichern.

Im Kontext der Untersuchung von Straftaten ist es das Ziel,

3.3 Hinweise für die juristische Verwertbarkeit

Sollen die sichergestellten Daten und Informationen juristisch verwertbar sein, zum Beispiel als Beweise in einem Strafprozess müssen einige zusätzliche Punkte beachtet werden. Grundsätzlich ist es sinnvoll die folgenden Punkte bei jeder Untersuchung zu berücksichtigen.

3.3.1 Methoden, Techniken und Programme

Die angewendeten Methoden und eingesetzten Techniken und Programme sollten in der Fachwelt akzeptiert und beschrieben sein. Neue Tools und Verfahren haben in der Regel einen schweren Stand, bis diese allgemein akzeptiert wurden.

3.3.2 Glaubwürdigkeit und Reproduzierbarkeit

Um die Glaubwürdigkeit der Ergebnisse sicherzustellen müssen sämtliche Schritte und die resultierenden Ergebnisse von Laien nachvollzogen werden können. Zusätzlich müssen die Ergebnisse durch einen anderen Experten reproduziert werden können. Der Ermittler, bzw. die Person, welche die forensische Untersuchung durchgeführt hat, muss in der Lage sein den gesamten Ablauf im Detail zu erklären. Erklärungen im Stiel von „Diese Information wurde vom eingesetzten Analyse-Programm automatisch gefunden“ sind nicht gern gesehen und können die Glaubwürkdigkeit der gesamten Untersuchung in Frage stellen.

3.3.3 Integrität

Während der gesamten Ermittlung (und auch darüber) hinaus muss die Integrität der untersuchten Daten und gefundenn Informationen, Daten und Beweise lückenlos sichergestellt werden. Die Integrität muss jederzeit vollständig belegt werden können.

3.3.4 Präsentation und Dokumentation

Die Ergebnisse müssen angemessen dokumentiert und präsentiert werden. Am geeignetsten ist es, wenn die Ergebnisse in Form von Ursache - Wirkung aufgezeigt werden. Die Beweisspuren, Ereignisse und Personen sollen möglichst logisch und nachvollziehbar in Relation zu einander gebracht werden.

Unvoreingenommenheit Gewisse Beweise kurze Halbwertszeit (meist sehr spannend), erfordern besonnenes / koordiniertes erfassen, Bewusstsein, dass System in jedem Fall verändert wird

Sachbeweis: Festplate, Logs, Gutachten, Fingerabdruck - keine Beweiskraft, nicht zugeordnet, keine Aussagekraft alleine, erst im Kontext, Beweiskraft erst druch Person, die Beweis in Tat-ZSH bringt, Sachbeweis eng mit Personenbeweis verbunden Beweis rasch Bedeutungslos, weniger Beweiskraft, wenn Person unrichtig darstellt, widerlegbare Behauptungen, Interpretationen, dachliche Darstellung, Integrität Person und Glaubwürdigkeit wichtig, sachliches, fundiertes Gutachten durch unglaubwürdige Darstellung als nichtig betrachtet

3.4 Hinweise zum Datenschutz

Datenschutz bei personenbezogenen Daten auch bei Auswertungen zum Zug Schweizer Recht??

Vorgängige Klärung wenn Logs personenbezogene Daten beinhalten, Information Datenschutzbeauftrager, Security & Compliance, IT-leiter, REvision, Vier-Augen-Prinzip wahren

DS bei Ermittlung nicht ausser Kraft, aber kein Täterschutz, Verhältnismässigkeit

3.5 Themengebiete und Teilbereiche

-HW, SW, AW

3.6 Anwendungsbereich

-Klassisch: Strafuntersuchungen, Computer Security Incident Handling -Operative Problembehebung -Log Monitoring -Data Recovery -Data Acquisition -Due Diligence / Regulatory Compliance

3.7 Ziele

3.8 Ausbildung & Zertifizierung

3.9 Sicherungsebenen

-Hardware-Ebene -Software-Ebene –Betriebssystem-Ebene –Anwendungssoftware-Ebene

3.10 Unterscheidung Daten-Typen

- Empfindliche Daten
  - Flüchtige Daten, gehen beim geordneten Shutdown / Ausschalten veroren (Cache, Hauptspeicher, Status NWV, Prozesse,...)
  - Fragile Daten, zwar auf HD, Zustand kann sich beim Zugriff ändern
  - Temporär zugreifbare Daten, auf HD, nur zu Bestimmten Zeitpunkten zugreifbar

-Flüchtig -Nicht-Flüchtig

Evtl. Matrix mit Zuordnung Techniken / Themenbereichen zu Typen und Sicherungsebenen

3.11 Anti-Forensik und Anti-Detection

Straftäter und Angreifer auf Computer Systeme werden sich immer mehr bewusst, dass sie Spuren auf dem System hinterlassen. Diese versuchen dann entweder keine oder so wenig Spuren wie möglich zu hinterlassen, Spuren und Beweise zu verändern oder gar zu löschen oder falsche Fährten zu legen. Dies kann entweder manuell oder mit Hilfe von Anti-Forensik und Anti-Detection Tools erfolgen.

Das primäre Ziel dabei ist, zu verhindern, dass das Eindringen oder die verdächtige Handlung entdeckt wird. Dies wird eigentlich eher dem Themenbereich der Anti-Detection, also dem „Unbemerkt bleiben“, zugeordnet. Bei der Anti-Detection versuchen die Täter unerkannt und unbemerkt zu bleiben. Zusätzlich wird versucht die Ermittler zu behindern, abzulenken oder die Datensammlung zu stören oder zu unterbinden. Zum Teil wird auch versucht den Umstand ausgenutzt, dass für eine Ermittlung nur eine beschränktes Zeitkontingent und Budget vorhanden ist. Dies kann dazu führen, dass der Ermittler nur die Beweise findet, die er soll und sich dann aus zeitlichen und budgettechnischen Gründen damit zufrieden gibt und die Untersuchung abschliesst.

Kennt der Angreifer die eingesetzten Werkzeuge oder kann diese ermitteln, kann er Schwachstellen und Sicherheitslücken in diesen ausnutzen und gezielt angreifen. im schlimmsten Fall kann der Angreifer die Ermittlungen gezielt manipulieren, ohne dass der Ermittler dies bemerkt. Daher sollte die Analyse zum einen in einer geschützten Umgebung durchgeführt werden und die verwendete regelmässig upgedatet werden.

KAPITEL 4

Forensische Analyse

4.1 Ablauf

Vorbereitung („Readiniess“): Autorisierung, wichtig bei nicht polizeilichen Ermittlern, keine Aktionen auf eigene Faust, mehr Schaden als Nutzen, Incident-Response-Plan Schutz der Beweismittel: Keine Veränderung an Daten möglich, Schutz eigene Umgebung Imaging und Datensammlung: Bitweise Kopie Datenträer, Sammlung Daten vom „Lebenden“ System Untersuchung und Bewertung Informationen: Analyse und Relevanzbewertung Dokumentation: Alle Phasen, schlüssig sofort dokumentieren

Evaluation Collection Analysis Presentation Review

S-A-P-Modell:

- Secure
- Analyse
- Present

– Collection: Idenify, label, record, acquire data, preserve integrity, in timely manner Examination: forensically processing data, Analysis: analyze result, using legally justifiable methods and techniques to derive useful information zur unterstützung des falles Reporting: describing actions used, how tools / procedures were selected, , other actions, ... — Analyse:

- Einbruchsanalyse -(Wer hatte Zugang?) Hinweise zu Täter –> Ermittlung Ausmass / Einschützung Schaden, Insiderwissen -Was hat der Angreifer auf Sys gemacht?, Bestimmt weiteres Vorgehen und Gegenmassnahmen, Daten einsicht / Modifikation / Zerstörung, Installation SW, neue User, Hintertüren? -Zeitpunkt Vorfall (Wichtig für Daten von anderen Quellen) -Weitere betroffene Systeme –> Recovery Planung, Zusatzinfos, mehr Spuren / Beweise -Wieso dieses System? Offene Schwachstellen? Besonder Daten? -Wie kam der Angreifer rein? Technik und Tools, Hinweise täter, -Ist der täter noch aktiv? ist schon weg? kommt er wieder?

- Schadensfeststellung - Bestimmung auf was für Daten / Informationen der Täter zugriff gehabt hätte - Evtl. noch aktive Passwortsniffer o.ä? Aufspüren, Passwörter ändern
- Analyse der Tools - Was würde zurückgelassen? Spuren / Tools, Hinweise auf weitere / eigentliche Ziele? - Hinweise herkunft / Täter - Wie wurden Tools aufgerufen? Von Hand, via Copy & Paste (Zeilenweise), Scripts (Rasche eingabe) - Programmiersprache Tools, Einschränkung Täterkreis, z.T. im Programmcode Hinweise zum Täter (Kommentare, Copyright, ..., Sprache) - Querabgleich Binärdateien andere kompromitierte Systeme oder gefundene Dateien bei mutmasslichen Tätern
- Logdatei-Analyse -Logs: netzwerkverbindungen, Firewall, Router, IDS - Wenn nicht: wieso? -Was verraten die Logs? Quelle, weitere Ziele ,Muster -Sicherung Logs Remote Access Systeme -Vermutung Innentäter: Sicherung Daten Zutrittskontrolle / Videoüberwachung
- Weitere Beweissuche -Datenträger Analyse -Spuren von verwendeten Applikationen -Gelöschte Dateien -Versteckte Dateien? Dateimaskierung, versteckte Speicherorte -Verschlüsselte Datein vom Angreifer vorhanden? Evtl. Hinweise wenn schlecht gesichert -Versteckte Partitionen? -Bekannte versteckte Hintertüren / Fernzugriff (Rootkits, trojanisierte Systemprogramme)

4.2 Techniken

4.2.1 Aktuelle Prozesse

-z.T. Programm / Prozess gestartet und nachher gelöscht, bei laufenden Prozessen gibt es Binärkopien in /proc, Bei Beendigung: Daten weg

4.2.2 Shutdown

Herunterfahren: Änderung vieler Zeitstempel, etl. Swap gelöscht Steckerziehen, verkraften nicht alle Dateisysteme, Status laufende Umgebung auf Dateisystemm, Extraktion sehr schwierig, Entscheidung im Kontext

4.3 Ablauf

4.4 Hinweise

-Zeuge / Zweitperson bei Ermittlungen anwesend -Protokollierung sämtliche Schritte (Abnahme durch Zeuge)

4.4.1 Vorbereitung

-Datenträger sjtjerilisieren, am besten formatierjt -Dokumente / Formulare / Protokolle

4.4.2 Secure

Sicherung möglichst vieler Daten, ohne eigene Spuren zu hinterlassen Zuerst Daten, die nach Shutdown oder hartem Shutdown nicht mehr verfügbar sind, nicht Systembefehle verwenden!! Protokolldateien auf externtes Medium (eigenes), evtl. auch Scripte zum Zusammenzug der Informationen,

-Beschreibung Physische Umgebung, detailliert, Fotos) -Beschreibung Umgebung (Computer), detailliert Fotos -Aktuelle Systemzeit + Referenzzeit, + Abweichung -Liste der aktiven Prozesse -Liste der geöffneten Sockets -Liste der Anwendungen, die auf geöffnete Sockets lauschen -Liste der User, die angemeldet sind -Liste der Systeme, die gerade eine Netzverbindung haben oder vor kurzem hatten

Anschliessend, Suche nach: -Timestamps gehacktes System -Trojanisierte Systemprogramme -Versteckte Dateien / Verzeichnissen -Verdächtige Dateien / Sockets -Verdächtige Prozesse

-Sicherung Cache- und Auslagerungsdateien -Sicherung Hauptspeicher pro Prozess-ID -Offene Netzwerkports -Verbindungen im Auf-/Abbau -erfolglose Verbindungsauf- / abbauversuche -Prozesse: Umgebungsvariablen, Übergabeparameter, geladnee Bibliotheken, offene Dateideskriptoren, etc. -Wechseldatenträger sicherstellen -Hauptspeicher: Inhalt + Strukturdaten (Welcher Prozess welche Biblio, Belegung Speicherbereich), Strukturiert und komplett dumpen

-Forensische Duplikation: Bitweise 1:1 Kopie Speichermedium, mehrere Varianten: 1. Ausbau, Anschluss saubere Platte an System, Kopie via Netzwerk, Wichtig: Writeblocker (Verhindert physisch den Schreibzugriff auf das zu sichernde Medium), gewisse Bereiche auf Datenträgern wo Daten versteckt werden können: z.B. Host Protected Area, Device Configuration Overlay –> Verfahren auswählen, dass diese Daten auch sichert, Sicherung durch Checksummen, Hash-Algorithmen

Verwendung Duplikat: Grundsätzlich sinnvoll, bessere Analysemöglichkeiten (Notaufnahme vs. Gerichtsmedizin), Sinnvoll wenn: Strafverfolgung, Sicherstellung Beweise, ...

-Regeulärer Shutdwon? Ja / Nein Mögliche Fehler Beweissammlung: -Zeitstempel an Datein werden verändert (z.T. schon durch Ansehen der Datei, oder aufrufen von Systembefehlen) -Keine Verwendung von grafischen Tools (Zugriff auf Vielzahl von Binärdateien / Konfigurationen –> Änderung Zeitstempel) -Verdächtige Prozesse nicht beenden -Alle Befehle protokollieren, sonst Lücke in Beweiskette -Keine Verwendung vertrauensunwürdiger Programme / Systemtools (evtl. Sys-Dateien ausgetausch, eigene vorkompilierte Dateien) -Patches / Updates: nur wenn Response-Team das empfiehlt, grundsätzlich offen lassen für Analyse, Abwägen je nach Kritikalität / Zusätzlichem Schaden bei offen lassen -Software (de)-installieren auf Empfehlung Response-Team, Vernichtung Beweise, Installation Forensik-Tools: Abwägung, Vernichtung Spuren, -Protokolle nicht auf zu untersuchende Platte schreiben (Beweise gefährdet, FIle slack...) -Ordnungsgemässer Shutdown könnte Beweise vernichten

Sicherstellung: -Haupteinheit (evtl. nur Datenträger) -Montor + Tastatur: i.d.R. nicht, nur bei Spezialgeräten -Dazugehörige Stromkabel -Externe Festplatten, Disketten, DVD, CD, WORM, Backup-Bänder, USB, Speicherkarten -Externe Kommunikationssysteme, welche für die Analyse benötigt werden: WLAN-Router, Modem, etc. -Spezialhardware und -peripherie -Digitalkameras, MP3-Player, etc. -PDAs, Mobile-Telefone, ...

Jeweils Abwägung, ob Schaden durch Beeinträchtigung Arbeitsfähigkeit (Mitnahme Gerät / Teile) grösser wird, als das einfache Delikt

4.4.3 Erste Schritte

Einige Allgemeingültige Schritte, je nach System / Gerät etwas anders (Mobiletelefone, etc.)

System ist ausgeschaltet

-Fremde Personen vom System und Stromversorgung entfernen -Umgebung fotografieren / skizzen anfertigen -Aktive Druckjobs zu Ende laufen lassen -System nicht einschalten (Achtung Notebooks, Deckel nicht hochklappen) -Sicherstellung System ausgeschaltet (Bildschirmschoner) -System evtl. im Standby-Modus? Bei Notebooks: Akku entfernen, sodass Energiesparmodus nicht anspringt (Veränderung Zeitstempel) -Stromkabel entfernen -Netzwerkkabel entfernen -Geräte und Objekte Beschriften (Beweiszettel) -Umgebung / Notizen / Unterlagen utnersuchen -Befragung Anwender nach: Besonderheiten System, Passwörter, Konfigurationsspezifika -> Dokumentation & Hinterfragen -Protokoll

System ist eingeschaltet

-Fremde Personen vom System und Stromversorgung entfernen -Umgebung fotografieren / skizzen anfertigen -Aktive Druckjobs zu Ende laufen lassen -Befragung Anwender nach: Besonderheiten System, Passwörter, Konfigurationsspezifika -> Dokumentation & Hinterfragen -Bildschirminhalte festhalten -Keyboard / Maus wenn möglich nicht sofort berühren, Bildschirm blank / Bildschirmschoner: Ermittlungsleiter fragen, bezüglich „aufwecken“, Zeitstempel festhalten) -Live-Response (Siehe oben) -Protokoll

4.4.4 Analyse

-Bewertung Beweisspuren: 3 Gruppen: 1: Untermauern bestimmte Theorie, wiederlegen bestimmte Theorie, unterstützen keine best. Theorie Zuordnung der Informationen

Schwierigkeit: Kausaler und zeitlicher Zusammenhang herstellen, müssen mit anderen Ereignissen überinstimmen, plausiebel, nachvollziehbar

Fragen / Hilfe: -War physischer Zugang zum System notwendig? Ja –> Zutrittskontrolle / Überwachung prüfen -Wer hatte noch Zugang zum Computer? Zutrittskontrolle / Überwachung prüfen -War Cronjob / Scheduler aktiv? –> Handlung ohne Anwesenheit Tatverdächtiger –> Prüfung Logs Betriebssystem / Scheduler -Digitale Spur durch

Fremdeinwirkung / Einwirkung dritter? -Weitere Beweise Bekräftigung / Widerlegung digitale Spuren? -Computerkenntnisse Tatverdächtiger? Was war für Know-How notwendig? -Hardware transportabel? Verschleierung Standort durch Verwendung mehrere Computer? -Code / Dokument / Mail / .... Verbindung zu Tatverdächtiger? (Stil, Grammatik, Vokabular, ...) -Verbindung Spuren und besuchte Webseiten in Verbindung? -Hinweise E-Mail-Clients / Chats zur Identifizierung Mittäter / Mitwisser?

4.4.5 Dokumentation

Wenn elektronisch: Verwendung vn Prüfsummen

Viele Screenshots zum festhalten oder mit Kamera

Untersuchungstools mit Versionsnummer

Unterschrift durch Zeuge: Gesamtes protokoll, und einzeln bei wichtigen Feststellungen / Beweisen

Pro Beweis: Beweiszettel, kein Zweifel an Herkunft, Besitztum, Unversertheit bestehen, Pro Objekt ein Zettel (Festplatte, PDA, Ausdruck, CD-Rom, Notebook)

Collection / Aquisition: Power Down System and boot into secure environement oder Write Blockers + Anschluss an Analyse-Syste, Runterfahren: Stromquelle entfernen (Kabel ziehen)

1. Runter fahren 2. Sämtliche Laufwerke entfernen –> Dokumentieren und Beweiszettel ausfüllen –> Beweiskette etablieren, Innenleben dokumentieren (schriftlich, Fotos) 3. Sämtliche Datenträger sicherstellen, Beweiskette, wenn berechtigt: Arbeitsumgebung durchsuchen (!Corporate Policies berücksichtigen). 4. Booten, BIOS-Informationen notieren auf Beweiszettel (Vorabrecherchieren Key für BIOS), Systemdatum -/ Zeit in Beweiszettel, WEnn Zeit anders: bei recover of files: Zeit anpassen 5. Forensisches Image erstellen -a: Wipe Drive (Vorbereitungsarbeit, wenn möglich nicht vor Ort) -b: Create Image with EnCase Bootable, Wenn EnCase Boot disk: Kein Write-Blocker notwendig, EnCase verhindert schreiben, Image benötigt in der Regel etwas mehr Platz als das original, immer Hash erstellen, Imaging auf -windows OS-Basis: Immer Write-Blocker, Linux: schreibt nicht auf Geräte, kein mount, Power Down Linux, Attach Drive, Power Up 6. Hash erzeugen und speichern, am besten auf Beweiszttel 7. Bag and Tag: Laufwerke auf die, die Images geschrieben wurden beschriften, sicher unterbringen, (anti-statischer Sack, sicherer Ort), Original-Laufwerk: je nach Szenario: auch eintüten oder wieder in Betrieb

Bemerkung zur Remote Untersuchung: nicht immer physischer Zugang möglich, weit entfernt, Einsatz von Forensik-tools via Netzwerk, Voraussetzung: Vorinstallierter Client auf System, voraus testen

KAPITEL 5

Tools und Techniken

5.1 Image-Related / Data-Aquisitation

5.1.1 Laufwerk löschen

EnCase, statisches überschreiben (nur einmal),

Attach to System, Windows, Start EnCase, Tools -> Wipe Drive, Select Device, Defaults as are, Next, HECF; S. 69 Kein WippingUtility, bei spezialfällen / wenn notwendig: Wipeutility: Linux: „dd if=/dev/random of=/dev/<image drive>“

5.1.2 Image erstellen

EnCase (Seite 72) DOS Boot disk EnCase (Windows) Linux: Device Name ermitteln: /proc/partitions oder logs, dann: „dd if=/dev/<suspect drive> of=/some dir/image name“, „md5sum /some dir/image name“, „md5sum /dev/<suspect drive>“ Midifzierte Version von dd, dcfldd für Forensik: http://dcfldd.sourceforge.net

FreeHelix

FTKImager (Windows)

5.1.3 Image verifizieren

EnCase, Tools, Verify Single Evidence File Linux: md5sum „image file“, compare

5.2 Gelöschte Datenträger

Datenträger-Löschsoftware, welche wurde eingesetzt? (noch installiert? typische Spuren?) arbeiten nicht immer zufälligen Löschpattern, evtl. Löschsoftware nicht ganz zuverlässig –> Temporäre Dateien, Registry, Protokolle, ...

5.3 Kommerzielle Tools

-SMART -Helix (ein Teil Freeware)

Remote Untersuchungen: -EnCase Enterprise Edition -Paraben Enterprise -ProDiscover

Quellenverzeichnis

[E20a] 2015. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf.

[E20b] 2015. URL: http://de.wikipedia.org/wiki/Hacker_(Computersicherheit).

[E20c] *Cyber Incident Response Guide*. EN. Multi-State Information Sharing und Analysis Center (MS-ISAC). 2010. URL: http://msisac.cisecurity.org/members/local-government/documents/finalincidentresponseguide.pdf.

[E20d] *Guide to Integrating Forensic Techniques into Incident Response*. NIST. 2006. URL: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf (siehe S. 11).

[Sil] Siller, Prof. (FH) Mag. Dr. Helmut: *Forensik*. DE. Wirtschaftslexikon Gabler. URL: http://wirtschaftslexikon.gabler.de/Archiv/1408495/forensik-v3.html.

[Ste12] Stern, Olaf: *Reglement: Seminararbeit*. Deutsch. ZHAW. 2012. URL: https://ebs.zhaw.ch/files/documents/informatik/Reglemente/Bachelor/Seminararbeit/a_Reglement-Seminar_Studiengang-Informatik_V2.1.docx (siehe S. 1).

[Web11] Websense: *Advanced persistent threats and other advanced attacks*. EN. Rev2. Websense. 2011. URL: https://www.websense.com/assets/white-papers/whitepaper-websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf.

Abbildungsverzeichnis

Tabellenverzeichnis

ANHANG A

Vorlage: Protokoll

Tabelle mit : Laufnummer, Zeit, Befehl / Aktion, Hash Ergebnisdatei, Kommentar

ANHANG B

Vorlage: Beweiszettel

Buch CF: Seite 85

Beweiskette:

Laufwerke: Manufacturer, Model, Serial Number, Evidence Description (Name of suspect, Technologie: SATA, IDE, ...)

Liste der noch zu erledigenden Punkte

Hinweis männlich / weibliche Form 1
Weitere Abgrenzungen 1
Struktur erklären 2
Bild CF Seite 13 4
Vervollständigen 4
Data Loss Prevention Technology 7
Intrustion-Mapping-Systeme 7
Definition Computer Forensik 13
Grafik Einbettung 13