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

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

Wurde ein möglicher Sicherheitsvorfall oder ein Angriff gemeldet, ist es wichtig, dass die Person, welche die Meldung entgegen nimmt korrekt und schnell reagiert. Personen welche solche Meldungen entgegen nehmen könntetn (z.B. Mitarbeiter des Service Desks) sollten geschult und mit einem entsprechenden Merkblatt und einer Checkliste / Formular ausgestattet werden. Die entgegenehmende Person muss vom Melder so viele Informationen wie möglich erfragen, damit anschliessend schnellere und effizientere Entscheidungen getroffen werden können. Dabei sind sowohl Informationen zum Melder, als auch über die Symptome und den Zustand des Systemes von Interesse.

Verweis Formular

Nachdem ein Vorfall gemeldet wurde, ist unverzüglich das zuständige Incident Response Team zu informieren und aufzubieten. Gibt es in der Organisation kein Incident Response Team und keinen Incident Response Plan ist das weitere Vorgehen mit dem Vorgesetzten und allenfalls einem Mitglied des höheren Managements abzustimmen. Übereilte Reaktionen sollten vermieden werden, da dadurch Beweisspuren verwischt oder vernichtet werden können.

2.3 Incident Response Team

Das Incident Response Team ist die Eingreiftruppe beim Eintretten eines Sicherheitsvorfalles. Die Aufgabe dieses Team ist es im Falle eines Incidents auf Basis der vorhandenen Informationen eine Lagebeurteilung und Risikoeinschätzung durchzuführen und anschliessend entsprechende Massnahmen einzuleiten.

In einem Incident Response Team sollten folgende Rollen besetzt werden.

- **Kern-Team**

  - Koordinator / Leiter mit direktem Zugang zum Management
  - Kontaktstelle zur Entgegennahme von Verdachtsmeldungen
  - Incident-Spezialist oder einen Ermittler aus dem Bereich der Computer Forensik
- **Erweitertes Team**
  - Juristischer Berater
  - Auditor
  - Mitarbeiter der physikalischen Sicherheit
  - HR-Mitarbeiter
  - Fachspezialisten (z.B. Netzwerk-, Sicherheits- oder Datenbankadministratoren)

Die Mitarbeiter dieses Teams sollten über längere Erfahrung in ihrem Tätigkeitsbereich verfügen, gute Kommunikationsfähigkeiten besitzen, teamfähig sein und gut integriert und zuverlässig sein. Darüber hinaus müssen sie in der Lage sein unter Stress effiziente und akzeptable Entscheide zu treffen, sich an vorgegebene Regeln und Prozeduren zu halten und in sicherheitsrelevanten Aspekten als Vorbild dienen. Sie müssen in der Lage sein sich unter Stress an vorgegebene Regeln und Prozeduren zu halten.

Bei grossen Organisationen kann das Incident Response Team als Dauerhaftes Team vorhanden ist, welches auch noch andere Aufgaben im Sicherheitsbereich wahrnimmt. Bei kleineren Organisationen kann es sich um ein Team mit Mitgliedern aus mehreren Organisationseinheiten handeln, welche im Notfall zusammengerufen werden können. Denkbar ist es auch, dass das ganze Incident Response Team oder einen Teil davon (z.B. den Incident-Spezialisten) durch eine externe spezialisierte Unternehmung wahrgenommen wird.

2.4 Incident Response

Die Incident Response hat zum Ziel bei einem Sicherheitsvorfall so rasch als möglich den entstandenen Schaden, die verwendeten Angriffsmethoden und die Auswirkungen für die Organisation zu beurteilen und anschliessend entsprechende Massnahmen umzusetzen. Die Computer Forensik ist ein essentieller Bestandteil des Incident Response Prozesses.

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 Infos: Business Impact, ...

2.4.1 Organisatorische Vorbereitung

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 -....

Vorbereitung („Readiniess“): Autorisierung, wichtig bei nicht polizeilichen Ermittlern, keine Aktionen auf eigene Faust, mehr Schaden als Nutzen, Incident-Response-Plan 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

2.4.2 Incident Response Prozess

Wurde ein Vorfall gemeldet gilt es zuerst zu beurteilen, ob es sich um einen wirklichen Sicherheitsvorfalle handelt, oder ob es sich um eine Betriebsstörung handelt.

Handelt es sich um einen Sicherheitsvorfall muss auf Basis der vorhandenen Informationen eine erste Einschätzung durchgeführt werden. Um für die Einschätzung alle relevanten Informationen zur Verfügung zu haben, ist es essentiell, dass bei der Entgegennahme der Meldung die entsprechenden Informationen erfragt werden (Siehe dazu Kapitel 2.2.5). Sind zu wenig Informationen vorhanden, kann bereits eine erste Analyse durchgeführt werden.

Es ist jedoch darauf zu achten, das....keine Beweise zerstören, nicht bemerkt werden, jur. Verwendbarkeit..

-Honeypots

-Nach Abschluss: –Ermittlunsvorgang analysieren und verbessern –Reaktionszeit, Wirksamkeit, Tätermotivation, Kosten –Schlüsse ziehen, permanente Massnahmen etablieren.

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,

Beurteilung Vorfall / Störung: 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,

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

2.4.3 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

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

2.5 Ablauf

1. **Identify (Identifizierung)**

   a) Eingang eines Hinweises für einen Verdachtsmoment (Siehe dazu Kapitel 2.2)

   b) Handlet es sich um einen Sicherheitsvorfall oder eine Betriebsstörung?

2. **Assess (Beurteilung)**

   a) Durchführen einer ersten Analyse / Sicherstellung von Spuren

   b) Einschätzung auf Basis der vorhandenen Informationen.

   c) Bestätigung des Verdachtes.

3. **Respond (Reagieren)**

    a) ...Initial Response (Determine origin, identify compromised systems, disconnect, untersuchung, anzeige)

    b) ...Procedure

    c) ...Recovery

4. **Report (Bericht)**

    a) ...

5. **Review (Rückblick)**

    a) ...

- Sicherstellung elektronische Beweise
- Beweisspuren identifizieren
- Beweisspuren analysieren
- Analyseergebnisse interpretieren / verifizieren
- Analyseergebnisse in Bericht zusammenfassen / präsentieren.

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 Themengebiete und Teilbereiche

-HW, SW, AW

3.4 Anwendungsbereich

Die Computer Forensik findet unter anderem in folgenden Bereichen Anwendung:

- Strafuntersuchungen
- Incident Response / Incident Handlung
- Log Monitoring
- Datenwiederherstellung
- Datenbeschaffung

3.5 Ziele

3.6 Ausbildung & Zertifizierung

3.7 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.

3.7.1 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.

3.7.2 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 Untersuschung in Frage stellen.

3.7.3 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.

3.7.4 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

3.8 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

3.9 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

In diesem Kapitel wird der Ablauf der Computer forensischen Analyse im Detail aufgezeigt und erklärt. Die Techniken und Tools zur Unterstützung dieses Prozesses wird im Kapitel 5 Tools und Techniken erläutert.

ERDM: Electronic Discovery Reference Model, Guter Prozess: Noitzbuch

4.1 Einführung

Der Prozess der forensischen Analyse lässt sich grundsätzlich in die nachfolgenden Phasen unterteilen werden. Die Erläuterung der einzelnen Phasen erfolgt in den nachfolgenden Kapiteln.

1. Readiness (Vorbereitung)
2. Secure (Sicherstellung)
3. Analysis (Analyse)
4. Documentation (Dokumentation)
5. Present (Präsentation)
6. Review (Rückblick)

4.2 Phasen

4.2.1 Readiness (Vorbereitung)

Um während der Untersuchung Fehler zu verhindern und wertvolle Zeit einzusparen, ist es sinnvoll gewisse Vorbereitunsarbeiten vor einem Einsatz, beziehungsweise vor einer Untersuchung, durchzuführen. Die gleichen Arbeiten sollten auch nach Abschluss einer Untersuchung durchgeführt werden, da jederzeit der nächste Fall eintreten kann.

Vorbereitungsarbeiten

- Sterilisieren / Formatieren von Datenträgern für die Speicherung des Beweismaterials
- Formulare und Protokolle vorbereiten und ausdrucken
- Vorbereitung und Verpackung der notwendigen technischen Ausrüstung
  - Kleines Werkzeugset
  - Digitalkamera
  - Notizblock und Stifte
  - Wasserfeste Filzstifte und Etiketten
  - Antistatische Beutel
  - Dokumente (Manuals, Anleitungen, Abläufe, etc.)
  - Writeblocker
  - Datenträger
  - (Mobiles) Analysesystem + Zubehör (Adapter, USB-Hubs, Card-Reader, Multi-Card-Reader, CD/DVD/Blue-Ray Leser / Brenner, Drucker)
  - ...
- Vorbereitung und Verpackung der notwendigen Tools und Programme
  - Datensicherung
  - Data discovery
  - internet history
  - image viewers
  - E-mail viewers
  - Password-cracking tools
  - Mobile device tools
  - large storage analysis tools
  - ...

Übersetzen

4.2.2 Secure (Sicherstellen)

Die Phase „Secure“ lässt sich weiter in die Phasen „Environment (Umgebung)“, „Identify (Identifizieren)“, „Collect (Sammeln)“ und „Preserve (Aufbewahren)“ unterteilen.

4.2.3 Environment (Umgebung)

Diese Phase muss grundsätzlich nur berücksichtigt werden, wenn es sich bei der Untersuchung um eine Ermittlung im Rahmen einer Incident Response oder einer Tatortssicherung handelt.

Bei Ankunft des Ermittlers am „Tatort“ sollte er sogleich sicherstellen, dass nur noch berechtigte Personen Zugang zum Tatort und der näheren Umgebung haben. Bevor die Personen den Tatort verlassen, sind zum einen die Kontaktdaten für spätere Rückfragen und zum anderen weitere Informationen (zum Beispiel: Passwörter, Besonderheiten des Systems) zu protokollieren. Sofern noch nicht erfolgt, sollte der Tatort isoliert und dokumentiert werden. Für die Tatortdokumentation sind Fotos und Skizzen sehr gut geeignet.

Identify (Identifizieren)

Bevor die ersten Daten gesichert werden können, müssen alle möglichen Datenquellen identifiziert werden. Dazu zählt zum Beispiel das zu untersuchende System, externe Festplatten, USB-Sticks, Wechseldatenträger, etc. Falls gestattet, sollte in der näheren Umgebung, zum Beispiel im Aktenschrank oder im Korpus, nach weiteren Datenträgern gesucht werden. Je nach Situation sind an weiteren Stellen (zum Beispiel Firewall-Logs, Server-Logs, etc.) zusätzliche Informationen gespeichert. Gegebenenfalls sollte auch nach relevanten physischen Dokumenten, welche Hinweise oder wichtige Informationen beinhalten, gesucht werden. Zum Beispiel könnte eine mehr oder weniger gut versteckte Passwortliste die Arbeit erheblich erleichtern. Wurden nicht an ein System angeschlossene Datenträger, Medien und Dokumente gefunden ist dies sofort zu dokumentieren und der Beweisgegenstand fachgerecht zu sichern (Siehe Abschnitt Collect (Sammeln) and Preserve (Aufbewahren)).

Collect (Sammeln) and Preserve (Aufbewahren)

Bei der Sammlung von Daten gilt der Grundsatz, dass so wenig eigene Spuren hinterlassen werden sollten, als irgendwie möglich ist. Die Sicherung der Daten erfolgt anhand Ihrer Einstufung. Zuerst werden flüchtige Daten gesichert, anschliessend nicht flüchtige Daten. Flüchtige Daten, sind Daten, welche nach einem Shutdown oder einem harten Shutdown des Systems nicht mehr verfügbar sind.

Harter vs. Normaler Shutdown Bei einem normalen Shutdown wird das System durch den Benutzer regulär heruntergefahren, sämtliche Daten werden gespeichert und das System befindet sich im Anschluss in einem sauberen / lauffähigen Zustand. Während dem Shutdown werden jedoch die Zeitstempel von sehr vielen Dateien verändert und temporäre Dateien und Arbeitsdateien des Betriebssystems gelöscht. Dies kann unter Umständen die Analysearbeiten erschweren oder sogar Beweise vernichten.

Bei einem harten Shutdown wird das System von der Stromversorgung getrennt, ohne dieses vorher herunterzufahren. Mit diesem Vorgehen wird sichergestellt, dass keine Zeitstempel von Dateien verändert werden. Auch ist die Wahrscheinlichkeit da, dass auf der Festplatte

eine Auslagerungsdatei vorhanden ist, welche anschliessend analysiert werden kann. Die Extraktion und anschliessende Analyse dieser Daten ist jedoch sehr aufwändig. Diese Methode des Shutdowns kann bei gewissen Dateisystemen zu irreparablen Schäden führen. Daher ist vorgängig abzuwägen, ob ein harter Shutdown sinnvoll und verkraftbar ist.

Bei einem Shutdown gehen in der Regel immer viele Daten verloren. Es wäre zum Beispiel möglich, dass der Angreifer ein Schadprogramm installiert hat, welches nur noch im RAM verfügbar ist. Nach einem weichen Shutdown ist das Programm auf dem System nicht mehr auffindbar.

Bei beiden Varianten ist die Zeit der Durchführung und die Art des Shutdowns zu protokollieren.

Sicherung des RAM-Inhaltes Nachdem herunterfahren des Systems sind die Daten im RAM noch einige Sekunden verfügbar. Dies reicht in der Regel jedoch nicht um eine Datensicherung durchzuführen. Einige neuere Studien und Experimente haben gezeigt, dass es durchaus Mittel und Wege gibt, um den Inhalt des RAMS zu sichern. Eine Möglichkeit besteht darin, die Raumbausteine mit einem Stickstoffspray auf -50 Grad Celsius herunter gekühlt. Anschliessend wird der Rechner ausgeschaltet, der RAM ausgebaut und in ein anderes System eingebaut. Das System wird mit einer Spezialsoftware gestartet, welches einen Memory-Dump erstellt.

System ist eingeschaltet

1. Nähere Umgebung und Zustand des Systems dokumentieren
2. Befindet sich das System im Standby?
   Befindet sich das System im Standby ist abzuwägen, ob das System aufgeweckt oder ein harter Shutdown gemacht werden soll. In dieser Situation ist in der Regel ein harter Shutdown zu empfehlen.
3. Ist der Screensaver aktiv?
   Ist auf dem System ein Screensaver ist abzuwägen, ob dieser „deaktiviert“ werden soll oder ein harter Shutdown gemacht werden soll. Dies ist stark situationsabhängig und sollte von Fall zu Fall entschieden werden. Ist anzunehmen, dass die Freischaltung des Screens mit einem Passwort erfolgt, welches nicht bekannt ist, ist auch hier der harte Shutdown zu empfehlen. Wird der Screensaver „deaktiviert“ muss dies entsprechend mit der exakten Uhrzeit dokumentiert werden.
4. Ist das System durch ein Passwort geschützt?
   Ist das System durch ein unbekanntes Passwort geschützt, ist in der Regel ein harter Shutdown zu empfehlen. In Ausnahmefällen kann durchaus auch ein Versuch unternommen werden, dass Passwort mit Hilfe von entsprechenden Werkzeugen zu knacken.

Ist der Zugang zum System hergestellt, kann mit der Sicherung der flüchtigen Daten begonnen werden.

1. Festhalten des Bildschirminhalts und der geöffneten Anwendungen
2. Festhalten der aktuellen Systemzeit und einer Referenzzeit, sowie deren Abweichung
3. Liste der aktiven Prozesse
4. Liste der geöffneten Sockets
5. Liste der Anwendungen, die auf geöffnete Sockets hören
6. Liste der angemeldeten User
7. Erstellen eines Memory Dumps
8. Sicherung des Hauptspeichers pro Prozess-ID
9. Sicherung der Cache- und Auslagerungsdateien
10. Liste der geöffneten Ports
11. Status und Statistik der Netzwerkverbindungen
12. Pro Prozess: Umgebungsvariablen, Übergabeparameter, geladene Bibliotheken, Offene Dateideskriptoren, etc.
13. ....Memory Dump?

Ist die Sicherung der volatilen Daten abgeschlossen sollte das System mit einem harten Shutdown heruntergefahren werden.

System ist nicht eingeschaltet Ist das System ausgeschaltet oder wurde es heruntergefahren wird als erstes das System von der Stromversorgung getrennt, geöffnet, der Zustand dokumentiert und die verbauten Datenträger ausgebaut, beziehungsweise im Falle von USB-Sticks oder anderen Wechseldatenträgern, entfernt und beschriftet.

Anschliessend wird von sämtlichen Datenträgern ein forensisches Duplikat erzeugt. Ein forensisches Duplikat ist eine Bitweise 1:1 Kopie des Quelldatenträgers.

Die Erstellung eines Duplikates ist grundsätzlich immer sinnvoll, da dies bessere Analysemöglichkeiten bietet. Ist die Untersuchung ein Teil einer Strafuntersuchung ist in jedem Fall die Anfertigung eines Duplikates zu empfehlen.

Beweiskette

Sicherung Haupteinheit (evtl. nur Datenträger), evtl. Spezialgeräte, Stromkabel, Sämtliche externen Datenträger, Wechselmedien wie DVD, CD, Disketten, USB-Sticks, WORM, Speicherkarten -Externe Kommunikationssysteme; WLAN-Router, Modem, spezial-HW / Peripherie, Digitalkameras, MP3-Player, PDAs, Mobiltelefone)

Zum Teil schaden grösser Bei Mitnahme / Ausbau, Abwägung http://forensic.belkasoft.com/en/live-ram-forensics

Auf sterilisierten Datenträgern

4.2.4 Analysis (Analyse)

Examination (Untersuchung)

Analysis (Analyse)

Analyse mit juristisch verwertbaren Methoden und Techniken und Informationen zur Unterstützung des Falles zu erhalten

Trojanisierte Systemprogramme -Versteckte Dateien / Verzeichnisse

4.2.5 Reporting (Dokumentation)

Die gesamte forensische Untersuchung muss im Detail protokolliert und dokumentiert werden. Es müssen sämtliche Arbeitsschritte nachvollzogen und gegebenenfalls durch einen anderen Experten reproduziert werden können. Die eingesetzten Tools (inkl. Version) und Techniken sollten kurz beschrieben werden Im Rahmen einer Strafuntersuchung müssen die durchgeführten Schritte und angewandten Techniken so erläutert werden, dass diese von Laien verstanden und nachvollzogen werden können.

Die Dokumentation der Untersuchung sollte soweit als möglich und praktikabel sofort bei der Durchführung erstellt werden, da ansonsten wichtige Informationen, Gedanken und Arbeitsschritte verloren gehen. Die Dokumentation ist mit Screenshots oder gegebenenfalls Fotos, welche mit der Digitalkamera aufgenommen wurden, zu unterlegen.

Evtl. auflistung besser?

- Verwendete Tools (inkl. Versionsnummer)
- Verwendete Hardware (zum Beispiel FastBloc Write Blocker)
- Angewendete Techniken
- Prüfsummen von Dokumenten, Protokollen und Beweisen
- Erläuterung der Evaluation der Tools und Techniken

4.2.6 Present (Präsentation)

4.2.7 Review (Rückblick)

4.3 Hinweise zur forensischen Analyse

Bei einer forensischen Analyse sind folgende wichtige Aspekte zu berücksichtigen.

- **Zeuge / Zweitperson**
  Während der Untersuchung sollte eine Zweitperson, bzw. ein Zeuge anwesend sein.
- **Protokollierung**
  Sämtliche durchgeführten Arbeitsschritte müssen protokolliert werden. Am Ende der Untersuchung sollte das Protokoll durch den Zeugen, die Zweitperson abgenommen und von beiden unterschrieben werden.
- **Schutz der eigenen Umgebung**
  Die eigene Analyseumgebung sollte gut gegen Angriffe geschützt sein und nicht direkt mit dem angegriffenen System oder Netzwerk verbunden werden. Sollte sich der Angreifer noch im Netzwerk oder auf dem System befinden, könnte er das Analysesystem angreifen und weiteren Schaden anrichten.
- **Schutz der Beweismittel**
  Sämtliche Beweismittel müssen sichergestellt und anschliessend geschützt werden. Eine Veränderung der Daten nach der Sicherung darf nicht mehr möglich sein beziehungsweise muss zweifelsfrei festgestellt werden können.
- **Verwendung von Systembefehlen**
  Zur Sammlung und Sicherung von Daten sollten niemals Systembefehle verwendet werden. Die Systemprogramme könnten vom Angreifer durch modifizierte Programme ausgetauscht werden sein. Der Ermittler sollte immer statisch vorkompilierte Programme verwenden.
- **Einsatz Grafischer Programme**
  Bei der Untersuchung eines Live-Systems sollte soweit als möglich auf den EInsatz von Programmen mit einer grafischen Oberfläche verzichtet werden. Grund dafür ist, dass diese eine Vielzahl an Binärdateien und Konfigurationen benötigen. Zum einen werden dadurch viele Zeitstempel geändert und zum anderen benötigen diese mehr RAM als Konsolenanwendungen.
- **Patches und Updates**
  Eher nicht, wenn kritisch, nach Rücksprache, Vernichtung Beweise

KAPITEL 5

Tools und Techniken

In diesem Kapitel werden die grundlegenden Tools und Techniken einer forensischen Analyse vorgestellt.

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

Technik

Varianten: Ausbau, Anschluss saubere Platte an System, Kopie via netzwerk Writeblocker

Versteckte Bereiche auf Datenträgern: Host Protected Area, Device Configuration Overlay –> Verfahren, dass auch diese Daten sichert, Checksummen

Tool

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 Secure

5.3.1 Prozesse

Binärkopien Prozesse / Programme unter /proc

5.4 Kommerzielle Tools

-SMART -Helix (ein Teil Freeware)

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

5.5 Tool-Matrix

Name	Windows	Linux	Mac OSX	Weitere
Test	x		x	

Tabelle 5.1: Verfügbarkeit der Tools auf verschiedenen Betriebssystemen

5.6 Technik-Matrix

Name	Windows	Linux	Mac OSX	Weitere
Test	x		x	

Tabelle 5.2: Einsatz der Techniken auf verschiedenen Betriebssystemen

5.7 Tool-Technik-Matrix

Nur Tool-Suiten

Name	Tool1	Tool2	Tool3	Tool4
Test	x		x	

Tabelle 5.3: Tools: Unterstützte Techniken

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. 13).

[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, ...)

ANHANG C

Vorlage: Formular Incident-Meldung

-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?

ANHANG D

Ablauf einer forensischen Analyse

Liste der noch zu erledigenden Punkte