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

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 ([**ZHAW:2012:Seminararbeit:Reglemente**])

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.

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 Turnverein Thalwil (TVT) 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

Kenntniss über Angriffsverfahren, -methoden, -techniken wichtig, da auf diese reagiert, untersucht werden muss

Es kann zwischen generellen und zwischen Massgeschneiderten Attacken und Tools unterschieden werden....

2.1.1 Angriffskategorien

-Un-Targeted attacks, so viele Geräte, Services, User als möglich, Opfer spielt keine Rolle, Ausnutzung der Offenheit des Internets, z.B. Phising, Water holing, ransomware, scanning -Targeted attacks: organisation / service / user, spezifisches interesse, Basisarbeit: z.T. mehrere Monate, fataler, Maasgeschneidert, z.B. Spear-Phsining, deploying botnet, subverting supply chain -Targeted Attacks: Heute auch oft spezifische Angriffscodes für einzelne Unternehmen, Codes unbekannt, schwierigere Erkennung -Advanced Persistent Threats: Solange als mölgich unerkannt bleiben, so viel als möglich, so wenig wie möglich zum unerkannt bleiben, Angriff über mehrere lange Phasen, Kein Vorgängiges Wissen zu Schwachstellen beim Ziel, Monate / Jahre, Schadcode ist so gebaut, dass er nicht gefunden wird, bleibt unbemerkt bestehen

2.1.2 Typen von Schwachstellen

-Flaws: ungbeabsichtigte Funktionalität, Schlechtes Design oder Fehler, oft lange unentdeckt -Features: Missbrauch vorgesehen Funktion, -User Error: z.B. unerfahrner Administrator, welcher Schwachstellen "freischaltet", Default-Passowrt, ...

2.1.3 Komplexität

Nimmt laufend zu, Monokulut Komponenten, OS, Anwendungen, Angriffstechniken auch komplexer, Anforderungen an Hacker immer höher, Bild CF Seite 13

2.1.4 Täter

Vielschichtige Motivationen, Soziale Motivation, Technische Ambitionen, Politische / Finanzielle / staatlich-politische Motivation, Regierung, Gruppen (Anonymous) Vielfältige Berufsbezeichnungen (Elite, Hacker, Script Kiddies, Cracker, ...), Hacker: neutral, Cracker-: negativ, White (Hackerethik, z.B. für Penetrationstests), Gray, Black-Hats

-Innen- / Aussentäter, Innentäter: Vorteile, Anteil bei Verbrechen relativ hoch, Unternehmen wähnen sich in falscher Sicherheit,

2.1.5 Typischer Ablauf

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

Stages: -Survey: Untersuchen / Analysieren von verfügbaren Informationen, Schwachstellen ermitteln, Social Engeineering, Commodity-Toolkits / -Techniques, Network Scanning, Infos über Org. und IT, user Errors ausnutzen -Delivery: Soweit kommen, dass die Schwachstelle ausgenutzt werden kann. Angreifer bringt sich in Position (z.B. Zugriff auf Online-Service, Versand Mails mit infizierten Links / Attachment, ifidzierter USB-Stick, Fake Website,), selecting best delivery path to breach defence -Breach: Ausnutzen der Schwachstelle -Affect: Auskundschaften der Systeme, Zugriffe erweitern, Hintertüre einrichten, user / admin account,

CF: Seiten 34-36

- Footprinting
- Port- und Protokollscan
- Enumerationng / Penetration
- Hintertüren einrichten
- Spuren verwischen

Phasen APT -Phase 1: Erkennung, Start und Infizieren: Survey, Delivery, + Infect -Phase 2: Control, Update, Discover, Persist: spread, discover / collect data -Phase 3: Extract and take action: extract data, take action (sell data, ...)

2.2 Incident Detection

Bevor auf ein Angriff reagiert werden kann, muss zuerst bemerkt werden, dass ein solcher sich anbahn oder bereits in vollem Gange ist.

...

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

Grossteil Angriffe nicht verfolgt, viele nicht bemekrt

2.2.1 Hinweise Netzwerkseitig

- Ungewöhnlich hohe Netzwerklast
- Ungewähnliche Anzahl Firewall-Regelverstösse

2.2.2 Hinweise Serverseitig

- Unbekannte Prozesse
- Unbekannte User
- Unbekannte Dateien
- Ungewöhnliche Systemlast
- Dienste laufen nicht mehr
- Ungewöhnliche Systemanmeldungen

2.2.3 Hinweise durch Intrusion-Detection-Systeme

Erkennung von Angriffen / Angriffsmustern, nicht verhindern, wenn gut konfiguriert: Frühzeitig Anzeichen erkennen, Beweise sammeln , Data Loss Prevention Technology

2.2.4 Weitere Hinweise

-Externe Hinweise: Kunden / Partnern / MA, Strafverfolgungsbehörde, Presse, Intrustion-Mapping-Systeme -RFC 2196, Abschnitt 5.3

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,

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

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

KAPITEL 3

Computer Forensik

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.

Teilbereiche

Die Forensik gleidert sich in zahlreiche Unterbereiche. Dazu gehören unter anderem:

- *Forensische Phsychiatrie*
- *Computer-Forensik*
- *Ballistik*
- *Rechtsmedizin*

https://www.mtholyoke.edu/org/forensic/fields.html http://forensictrak.com/faq.html http://de.wikipedia.org/wi

3.1.2 IT- / Digitale Forensik

3.1.3 Computer Forensik

Die Computer Forensik Die Computer Forensik Einbettung in Forensik, Digitale Forensik

3.2 Einführung

Ziel: nach Systemeinbruch / Sicherheitsvorfall: Methode / Schwachstelle finden, Bezifferung Schaden, Identifikation Angreifer, Beweissicherung für juristische Schritte

3.3 Hinweise für die juristische Verwertbarkeit

-Angewendete Methoden / Techniken / Programme sollten in Fachwelt beschrieben / akzeptiert / gängig sein, neue Verfahren / Tools schwierig, nicht unmöglich -Glaubwürdigkeit: Schritte / Ergebnisse müssen Nachvollziehbar sein (im Detail), Ermittler muss Ablauf / Hintergrund erklären können, (Programm mit Daten füttern, loslassen) -Sämtliche Schritte / Methoden müssen reproduzierbar sein (durch Dritte) -Integrität: sichergestellte Daten dürfen nicht verändert werden, muss jederzeit belegt werden können -Ursache / Wirkung: Gewählte Methoden: möglichst logische, nachvollziehbare Verbindung person - Ereignis - Beweisspuren -Angemessene Dokumentation

Wenn am Anfang nicht klar ob jur. Schritte: Trotzdem immer gleichen Prozess verwenden. 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

3.6 Anwendungsbereich

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

KAPITEL 4

Forensische Analyse

4.1 Ablauf

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

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

4.3 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

-Beschreibung Physische Umgebung, detailliert, Fotos) -Beschreibung Umgebung (Computer), detailliert Fotos

4.4.3 Analyse

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

4.4.4 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

Abbildungsverzeichnis

Tabellenverzeichnis

ANHANG A

Vorlage: Protokoll

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

ANHANG B

Vorlage: Beweiszettel

Buch CF: Seite 85

Liste der noch zu erledigenden Punkte