07 WinLinux

Windows

Registry

-organisiert in Hives
-enthält Konfiguration und historische Informationen
-Clear Text und Binary
-Gelöschte Einträge sind wiederherstellbar: zb durch Regslack

Registry Teile

C:\Windows\System32\config\: SAM, SECURITY, SOFTWARE, SYSTEM, DEFAULT
ntuser.dat: HKEY_LOCAL_USER

SAM Security Account Manager
-Lokale Benutzer
-Ist verschlüsselt, Key im SYSTEM Hive
-User Passwörter, Account created, Last Login, Passwort Hint, etc.

SYSTEM
-USB Sticks, Drucker, Netzwerkkarten

SOFTWARE
-WLAN: SSID, MAC, last login

NTUSER.dat / HKEY_LOCAL_USER
-Gelock während User eingeloggt ist
-Gestartete Programme / count
-Verbundene USB Devices
-Most recently Used (MRU)
-RecentDocs
-Suchbegriffe

Wichtige Windows Directories und Files

C:\Dokumente und Einstellungen\
-AllUsers: Für Alle User
-Default User: Vorlage für neuen Benutzer
-User X: Profilinformationen von Benutzer X
--Anwendungsdaten
--Desktop
--Eigene Dateien
--Favoriten
--Lokale Einstellungen: Temporäre Dateien, Temporäre Internetdateien
--Recent: Letzte Dokumente

Papierkorb:
-nur logisches Verzeichnis wird verändert
-eindeutige Zuordnung der Unterverzeichnisse zu Benutzer

C:\Programme, C:\Programme (x86): Standardpfad für Programme

C:\System Volume Information (ab Windows XP): System Restore Points, Alte Dateistände, Configfiles, Registry!

Volume Shadow Copy (Windows Vista/7): Differential Backup von Volumes, Kann gelöschte und gewipte Daten enthalten

C:\Windows\System32\drivers\etc: Hosts Datei für Namensauflösung

C:\Windows\System32\Spool\PRINTERS: Drucker Spool Files

C:\Windows\Repair: Backup von Registry Files & SAM

C:\Windows\System32\config*.evt: System Events

services.msc: Laufende Prozesse

Linux

Generelles
-Viele Möglichkeiten, Dateien zu verstecken (.foobar, foobar~, Rootkits)
-Open Source -> Totmannschaltungen leicht möglich
-Fast alles kann verschlüsselt werden
-Viele Dateisysteme möglich
-Rootkits
--traditionelle Rootkits: ersetzen wichtige Systemprogramme
--Kernel Rootkits: ersetzen Syscalls
--Virtuelle Rootkits: Virtualisieren OS während der Ausführung, bsp: Blue Pill

Wichtige Linux Directories und Files

Wichtige Logfiles
-/var/log/*
-Vor allem syslog

Konfigurationsfiles
-/etc/network/interfaces
-/etc/hosts
-/etc/crontab
-/etc/passwd und /etc/shadow
-Viele auch in /home

/home
-.bash_history
-.ssh/known_hosts

Installierte Programme
-dpkg -l, yast, etc.

Binärdateien
-/bin, /sbin
-/usr/local/bin, /usr/local/sbin
-/usr/bin
-/home/User/bin
!echo $PATH

Autostart
-~/.profile
-/etc/init.d/
-/etc/rc[0-6].d/*

Wichtige Tools
-dd: 1:1 Kopie
-sha1sum, md5sum: Prüfsummen/Hashes zur Sicherstellung dass File nicht geändert wurde
-file: versucht Dateien zu erkennen (magic numbers)
-strings: liefert ASCII Inhalt auch von binaries
-gdb
-ltrace, strace: zeigen libcalls und syscalls
-hexedit
-script: protokolliert Kommandozeilen-Session
-/proc
-ps, top

Weitere Tools
-Xplico
-Sleuth Kit/Autopsy
-Live CDS: DEFT, Backtrack, Helix

File Carving
-findet Dateien aufgrund von Inhalten/Headern
-zB: Scalpel, foremost

08 Memory Forensics

-Speicher beinhaltet wichtige Informationen: Prozesse, Netzwerkverbindungen, Geöffnete Dateien
-Memory Forensics ist nicht später wiederholbar!!
-Invasiv, eigener Prozess notwendig (-> kann paging verursachen)
-unbedingt eigene Programme verwenden
-Daten gehen durch Reboot/Power Off verloren
-Dokumentation besonders wichtig

Problemstellungen
-Totmannschaltungen bei Shutdown/Reboot
-Rootkits
-Computer läuft, ist aber gesperrt
-Shutdown vs. Strom unterbrechen
-Memory Slack Space kann zum Verstecken von Daten verwendet werden

Order of Volatility nach RFC 3227
-registers, cache
-routing table, arp cache, process table, kernel statistics
-memory
-temporary file systems
-disk
-remote logging and monitoring data
-physical configuration, network topology
-archival media

Aquisition
Hardware vs. Software:
-Software billig, aber verändert Zustand, kann reingelegt werden
-Hardware benötigt extra Hardware, ist OS unabhängig, aber kann auch reingelegt werden
-Es gibt keine perfekte Lösung

in Windows:
-hiberfil.sys: Computer hibernaten, dann File kopieren
-Tools: kntdd, windd, FTK Imager

DMA Redirection:
-Gegen Hardware Aquisition
-CPU und DMA sehen bei gleicher physischer Adresse unterschiedlichen Inhalt
-Cold Boot Attacks

Windows Prozessliste
-doppelt verkettete Liste
-Rootkits können sich aus Liste herausnehmen

Sobald RAM gesichert
-Erstellung einer Zeitlinie

Tools
-FTK 3
-EnCase
-Volatility

Paging
-Anwendungen wird unbegrenzter Speicher vorgegaukelt
-OS tauscht Pages aus je nachdem, welche Anwendung welchen Speicherbereich anfordert
-Windows: pagefile.sys; kann auch historische Prozessdaten enthalten
-Linux: Partition auf der Festplatte bzw. File.

10 Rechtliche Rahmenbedingungen

Begriff Sachverständiger
-Experte
-analysiert, erkennt Tatsachen, legt diese dem Gericht vor
-durch gewissenhafte, vollständige, methodische Untersuchung wird eine forensische Analyse mit Beweiskraft erstellt
-keine allgemeingültige Definition im österr. Recht

Typen:
-Amtssachverständiger: steht Behörde zur Verfügung, in IT Forensik kaum vorhanden
-nichtamtliche Sachverständiger: steht in keiner ständigen Beziehung zu Amt, kann aber beauftragt werden
-Privatgutachter: Wird immer von Privatperson beauftragt. Gutachten als Argumentationshilfe vor Gericht.
-allgemein beeidete und gerichtlich zertifizierte Sachverständige:
--Werden von Liste ausgewählt
--Muss Sachverständigeneid und Prüfung ablegen, mind 5 Jahre Berufserfahrung+Studium oder 10 Jahre Erfahrung
--Helfer des Richters
--Beweismittel in Form eines Gutachtens

Sachverständige - Gesetzliche Grundlagen
-Es gibt kein eigenes Sachverständigenrecht
-Bestimmungen verschiedener Rechtsbereiche
--Prozessrecht
--Zivilgerichtsverfahren
--Strafprozess
--Materielles Recht (zB Bauordnung)
--Bürgerliches Recht
--Strafrecht

Hauptverband der allgemein beeideten und gerichtlich zertifizierten Sachverständigen Österreichs
-listet relevante gesetzliche Bestimmungen auf

Überwälzungsgrundsatz
-Kosten von gerichtlich beauftragten Gutachten können auf die verlierende Partei übergewälzt werden

Gebührenanspruchgesetz
-regelt Stundensatz

11 Berichterstattung

Rechtsvollzug vs. kommerzieller Bereich
-Rechtsvollzug: In Form eines Gutachtens
-Kommerziell: Keine Regeln, aber Orientierung an Gutachten sinnvoll

Der Beweis
-An Sicherheit grenzende Wahrscheinlichkeit über das Vorliegen von Tatsachen
-Alle tatrelevanten Tatsachen müssen bewiesen werden
-Grundsatz der materiellen Wahrheit: objektive Wahrnehmung muss erforscht werden; alle Umstände des Sachverhalts (positiv und negativ) müssen ermittelt und bewiesen werden
-freie Beweiswürdigung: Behörde prüft, ob Tatsache für sie erwiesen ist
-Unbeschränktheit der Beweismittel: Alles darf herangezogen werden, das dafür geeignet ist, u.a. auch: indirekte Beweis, Beweis vom "Hören-Sagen", rechtswidrig erlangte Beweise

Tatfrage vs. Rechtsfrage
-Tatfrage: Hier geht es um die Fakten
-Rechtsfrage: beschäftigt sich damit, welche Fakten das sind, Auslegung. Aufgabe des entscheidenden Organs.

Berichterstellung - Gutachten
besteht aus zwei Teilen
-Befund
--stellt alle relevanten Tatsachen dar, aus denen später Schlüsse gezogen werden sollen
--Grundlage für das Gutachten
--Behandlung der Fragestellung: Angabe des groben Inhalts des Gutachtens
--Grundlagen des Befunds: Bereits vorhandene Ergebnisse, Dokumente etc. dokumentieren
-Gutachten (im engeren Sinn)
--enthält fachkundige Schlussfolgerungen anhand der Tatsachen des Befunds
--Behandlung des Beweisthemas und der Fragestellung
--Konkrete Schlussfolgerungen aus den Beweisen
--Begründung
--Interessierter Laie muss Gutachten nachvollziehen können

Folgende Punkte sind bei Gutachten unzulässig
-Unvollkommene Sachverhaltsaufnahmen
-Unüberprüfbare Behauptungen
-Privatgutachten von Parteien nicht berücksichtigt
-Überschreitung des eigenen Fachwissens

-Rechtliche Beurteilungen
-Rechtsausführungen

12 Related Documents

Quellen
-NIST: National Institute of Standards and Technology
-ISO: International Organization for Standardization
-RFC: Request for Comment, Gruppe innerhalb von Internet Society ISOC, die die RFC in ihre endgültige Form bringt
-Wissenschaftliche Publikationen
-Handbooks von Police Departments

Besonders Wichtige Dokumente

RFC 3227
-Best Practice zur Beweissicherstellung und Beweisarchivierung
-Notwendige Schritte, Empfohlene Reihenfolge
-Häufige Fehler
-Randbedingungen, die eingehalten werden müssen
-Tools

NIST SP 800-86
-Guide to Integrating Forensic Techniques into Incident Response
-Anwendung von IT-Forensics im Incident Response Prozess
-Einsatz von IT-Forensics für
--Investigating Crime
--Investigating internal Policy Violations
--Reconstructing Computer Security Incidents
--Recovering

Weitere Wichtige Dokumente

NIST SP 800-61
-Computer Security Incident Handling Guide
-Richtige Behandlung von IT Sicherheitszwischenfällen
-organisatorische Struktur
-Analyse von Daten
-Angemessene Bewältigungsstrategien
-Verschiedene Arten von Incidents:
--DoS
--Malicious Code
--Unauthorized Access
--Inapropiate Usage

NIST SP 800-122
-Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
-behandelt Umgang mit personenbezogenen Daten

FRGCF
-First Responders Guide to Computer Forensics
-benahdelt Richtlinien zur Sicherstellung digitaler Beweise

RAND
-Handbook of Legal Procedures of Computer and Network Misuse in EU Countries
-Leitfaden zur Umlegung technischer Zwischenfälle auf das Rechtssystem eines Staates
-Matrix, welche Delikte in welchen Staaten strafbar sind

RAND In Österreich
-Welche Gesetze gibt es
--Widerrechtlicher Zugriff
--Störung der Funktionsfähigkeit
--Pornographische Darstellung minderjähriger
--Tatbestände zu bargeldlosen Zahlungsmitteln
-Welche Exekutiven/Behörden gibt es, Struktur
--Polizei (Exekutive)
--Gerichtliche Einrichtungen: Je nach Vergehen und Höchststrafausmaß

---Bezirksverwaltungsbehörden
--Verwaltungsgerichtshof
--OGH
-Welche Forensischen Methoden finden Anwendung
--Durch die Staatsanwaltschaft geleitet, durch die Polizei unterstützt
--Einbeziehen von Sachverständigen selten

13 RFC 3227 Guidelines for Evidence Collection and Archiving

-bietet Guidelines für Sysadmins um Beweise auf Incident zu sammeln und zu archivieren
Gliederung:
-Richtlinien für die Beweissammlung
-Beweissicherstellung
-Beweisarchivierung

Security Incident
-Sicherheitsrelevantes Systemereignis
-verletzt Security Policy

Richtlinien für die Beweissammlung
-Definierte Prozeduren
-Systemabbild so wahrheitsgetreu wie möglich
-Genaue Dokumentation: Datum, Uhrzeit und Bearbeiter, UTC vs Lokaler Zeit, Genauer Ablauf und Tätigkeiten
-Datenschutz: nur bei begründeter Vermutung dürfen persönliche Daten herangezogen werden

Beweise müssen
-Admissible: entsprechend gesetzlicher Bestimmungen
-Authentic: dem Incident klar zuordenbar
-Complete: ganzheitliche Darstellung
-Reliable: Beweiskette
-Believable: verständliche Aufbereitung
sein

Zu Vermeiden ist
-Beweise irrtümlich zu vernichten
-Zu früher Shutdown
-Systemdateien soll nicht vertraut werden, eigene Dateien
-Keine Programme ausführen, die Zugriffszeiten manipulieren
-Achtung auf Totmannschalter

Beweissicherstellung
-möglichst wenige Entscheidungen notwendig: -> sonst Gefahr vorschneller Entscheidungen
-Prozeduren so detailliert wie möglich
-Transparenz
Schritte:
-Liste involvierter Systeme
-Aufstellung relevanter Beweisquellen
-Für jedes System: Reihenfolge der Datenflüchtigkeit
-Externe Systeme die Daten verändern könnten entfernen
-Alle Schritte dokumentieren
-Checksums, Signieren

Beweisarchivierung - Chain of Custody
-Beweise müssen sicher verwahrt werden
-vollständige Dokumentation
-möglichst restriktiver Zugang
-Daten auf weit verbreiteten Medien sichern
Folgende Dinge müssen dokumentiert werden
-Wer hat wann und wo Beweis sichergestellt
-Wer hat wann und wo Beweise analysiert
-Wer hat wann und wo Beweise verwahrt
-Wer hat wann und wo Beweise übergeben

Tools
-Read Only Datenträger mit Analysetools
-Prozesse anzeigen
-Systemstat anzeigen
-Bit-Level Kopien

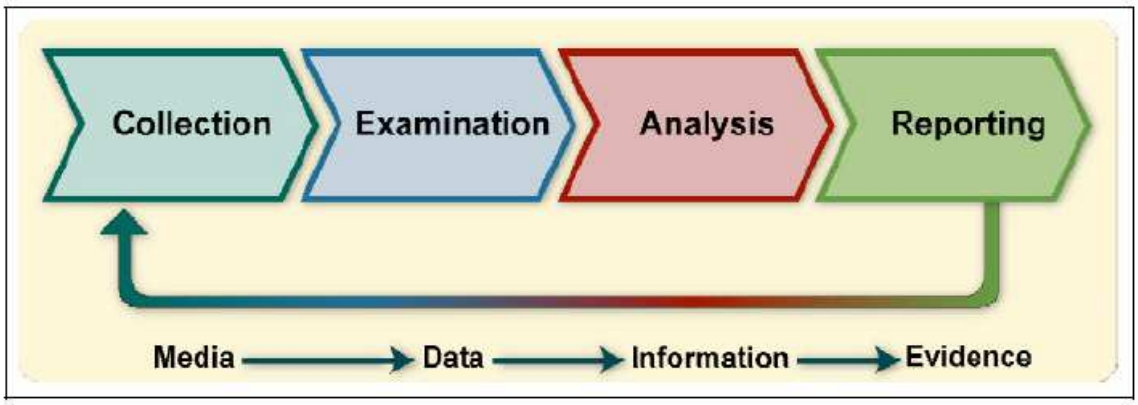
-Checksums und Signatures
-Core Images anlegen
-Skripte für automatische Beweissammlung (zB. Coroner's Toolkit)

14 Comparison Matrix of Related Documents

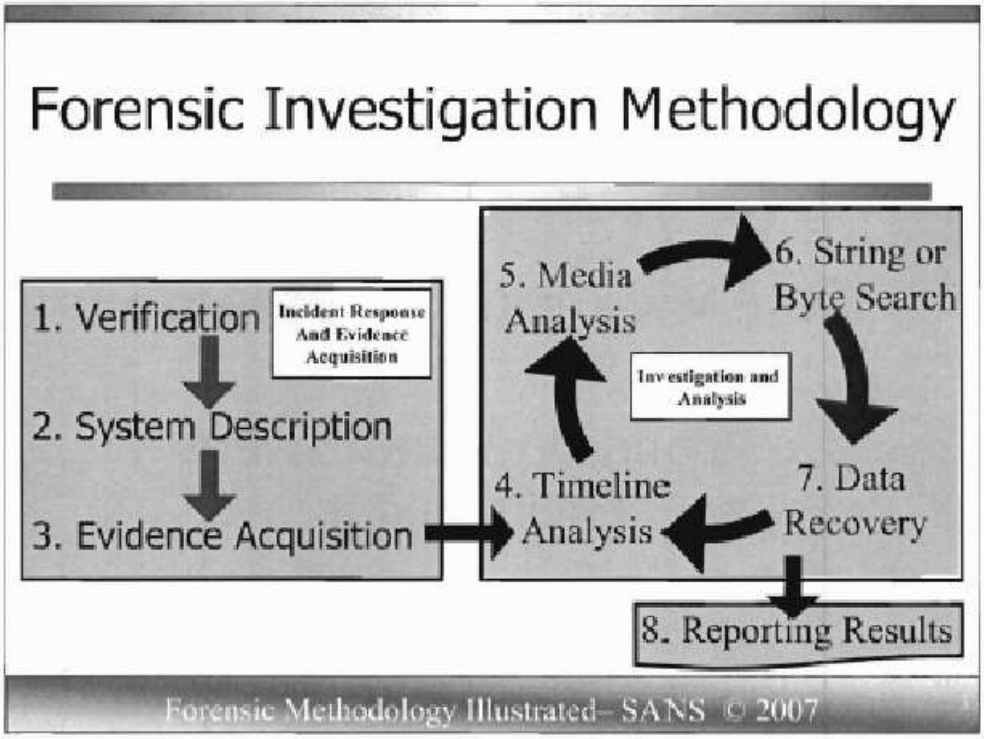
	Wichtigkeit	Organisatorische Themengebiete	Rechtliche Themengebiete
RFC 3227 Guidelines for Evidence Collection and Archiving	bedeutend	Forensische Datensicherstellung und - archivierung	kaum
NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response	bedeutend	Forensiche Prozesse, Analysemethoden	kaum
NIST SP 800-61 Computer Security Incident Handling Guide	bedeutend	Incident Response, Incident Management	kaum
ISO 18044 Information security incident management	bedeutend	Incident Response, Incident Management	kaum
RAND corp. Research Handbook of Legal Procedures of Computer and Network Missuse in EU Countries	bedeutend	keine	bedeutend
FRGCF_v1.3, First Responders Guide to Computer Forensics Software Engineering Institute Pittsburgh	bedeutend	keine	US Law

16 Forensic Process

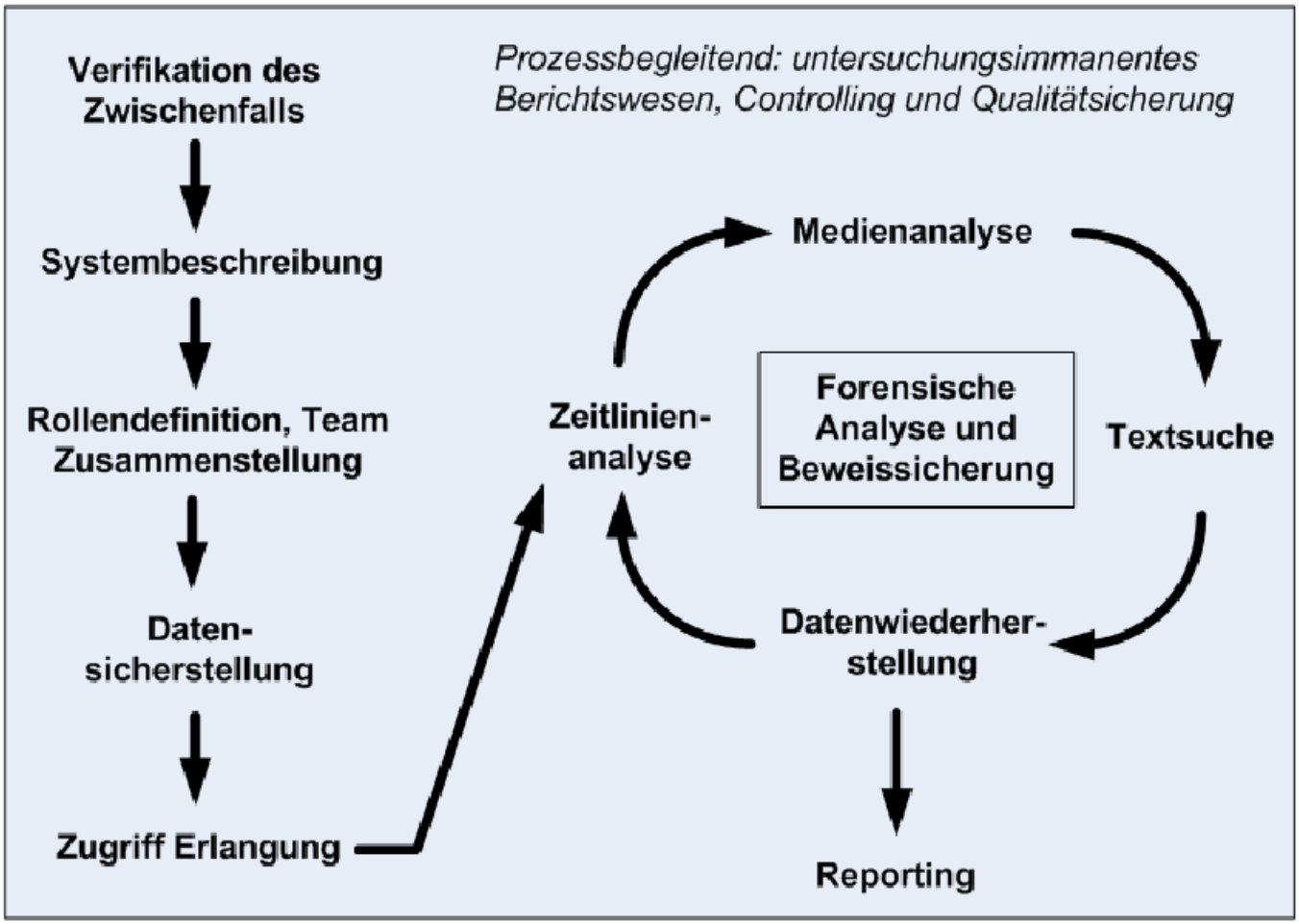
Forensischer Prozess nach NIST SP 800-86



Forensischer Prozess nach SANS



Vorschlag eines forensischen Vorgehensmodells



Verifikation des Zwischenfalls
-Bestätigung des Zwischenfalls
-Sicherstellung, dass wirklich Incident vorliegt und nicht Fehlkonfiguration

Systembeschreibung
-Festlegen der zu behandelnden Fragestellungen
-Festhalten der Ausgangslage der Untersuchung
-Involvierte Parteien
-Beschreibung der zu untersuchenden Systeme
-Kontext, in dem die Untersuchung durchgeführt wird

Rollendefinition, Team Zusammenstellung
-Bestimmen eines Computer Security Incident Response Teams (CSIRT)
-Sicherstellung einer durchgehenden Qualitätskontrolle
-Analyst: Führt die Untersuchung durch
-Kontrolleur: Sorgt für die begleitende Qualitätssicherung, überwacht Tätigkeit des Analysten

Datensicherstellung
-Anlegen einer Kopie des Datenbestandes
-Niemals auf dem Original arbeiten!
-Checksums
-Integrität der Daten wahren, Vieraugenprinzip, Protokollierung
-Idealerweise auf Write-Once-Read-Many (WORM) Medium wie DVD sichern, geht aber nicht bei großen Datenmengen
-Sicherung von RAM
-Brutal ausschalten vs Graceful Shutdown

Zugrifferlangung
-Zugriff auf die zu analysierenden Daten

Forensische Analyse und Beweissicherung

-hängt stark von der Fragestellung ab

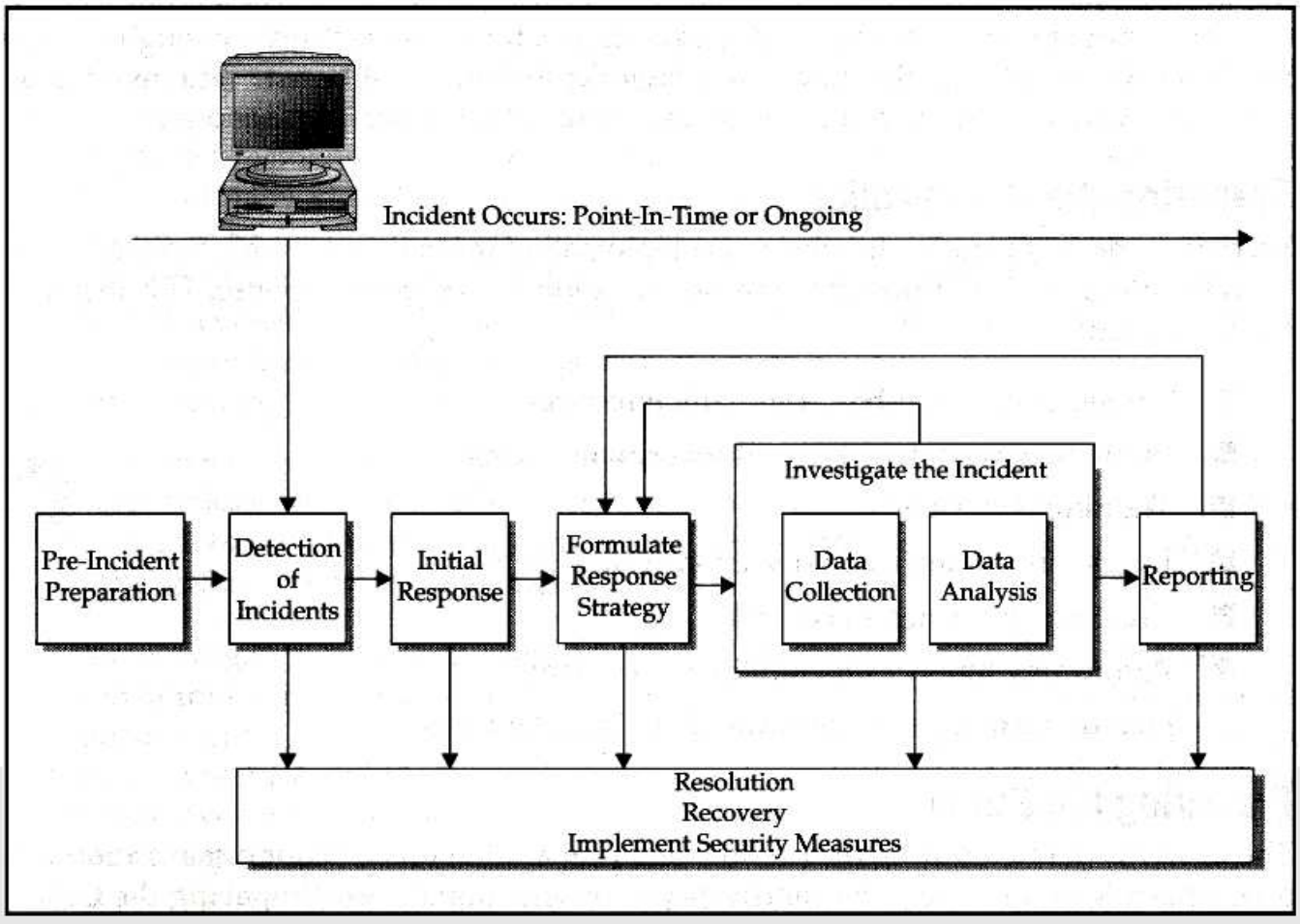
Reporting
-Detaillierter Bericht
-Beschreibung des Analyseverlaufs
-Beweise und resultierende Schlussfolgerungen, aufbereitet für Entscheidungsträger

– **Bestimmung des ersten Blocks mittels Division durc Blockgröße und modulo Operation. Bsp.:**

Für den Block von 0x00414000-0x00418000 ergibt sich:
00418000h = 4292608d4292608/16384 = 262
Der 262te physikalische Block trägt die Blocknummer 261, da di Nummerierung bei 0 beginnt. Slot Nr. = Block Nr. mod (phys. A
261 mod 3 = 0
262 mod 3 = 1
263 mod 3 = 2

17 Incident Response Process

Incident Response Methodology nach PMP



Security Incident Examples
-Theft of trade secrets

-Email spam or harassment
-Unauthorized or unlawful intrusion into computing systems
-DoS

Incident Response Process
-soll unkoordiniertes Vorgehen verhindern
-bestätigen oder ausräumen, dass ein Incident aufgetreten ist
-Minimierung notwendiger Unterbrechungen des Geschäftsprozesses
-Verfolgung des Täters ermöglichen
-erstellen verwertbarer Berichte und Empfehlungen
meißtens Bereichsübergreifend, daher am Besten Zusammenstellung eines Computer Security Incident Response Teams (CSIRT)

Pre Incident Preparation
-Je besser die Vorbereitungen, desto erfolgreicher die Reaktion im Ernstfall
Vorbereitung der Organisation
-Verantwortlichkeiten, Procedures
-Implementieren von Security und Monitoring
-Schaffen einer IT Awareness Kultur bei End-Usern
Vorbereitung des CSIRT
-Anschaffung benötigter Hard- sowie Software
-Training

Detection of Incidents
-durch End-User
-Sysadmins
-IDS/IPS

Initial Response
Das CSIRT übernimmt die Angelegenheit
-Verifikation, ob wirklich Incident
-Welche Systeme und User sind betroffen?
-Bewertung des Business Impacts

Formulate Response Strategy
-angemessene Behandlung des Zwischenfalls
-Abklärung der Rahmenbedingungen

Investigate the Incident
-Start der forensischen Analyse

Report
-Reporting und weitere Vorgehensempfehlungen

Resolution
-Einfließen lassen der neuen Erkenntnisse in bestehende Prozesse und Bewertungen