

forensische IT-Ermittlung

Szenario: Ein Mitarbeiter könnte heimlich Daten von einer internen Festplatte auf einen externen Datenträger kopiert haben. Möglicherweise hat er Programme oder Skripte installiert, um bestimmte Sensorwerte auf dem Mainboard oder das BIOS des Rechners zu manipulieren. Die Geschäftsführung wünscht nun eine lückenlose Dokumentation, damit eine interne IT-Forensik- Abteilung oder, falls nötig, die Strafverfolgungsbehörden den Vorfall aufklären können.



5 Phasen der Ermittlung

- **Phase1 : Identifizierung**
-
- **Phase2 : Abholung**
-
- **Phase 3 : Analyse**
-
- **Phase 4: Berichterstattung**
-
- **Phase 5: Präsentation**

Ermittlungen am Tatort

Identifizierungsphase

- **Geräte Identifizieren**
- **Foto Dokumentieren**
 - wie sieht der Tatort aus
 - wo lag die Hardware
 - sind geräte und steckverbindungen getrennt worden
 - gibt es physische Anzeichen für Manipulation
- **Katalogisieren der einzelnen Komponenten (Hardware, Ablagen und etc.)**

Abholungsphase

- Datenerfassung (Image des Gerätes)
- der Ermittler muss spezielle Tools und Techniken verwenden
- der Prozess muss Dokumentiert werden

Software der Forensik

- | | |
|---------------------------|--|
| -Adepto | dient zum erstellen von Datenträger-images |
| -Autopsy Forensic Browser | Auswerten von Datenträger-Images,
Extraktion von Daten |
| -Captain Nemo | Auslesen diverser Dateisysteme |
| -Chkrootkit | Suche nach Spuren von gebräuchlichen
Rootkits |
| -Filemon, Regmon | Analyse von Registry- und Filesystemzugriffen
von Applikationen |
| -FPort | Anzeige,welche Applikationen Ports geöffnet
haben |

.....

Analyse

- werden die gesammelten Daten untersucht
- beweise identifizieren
- spezielle Techniken können gelöschte Dateien wiederherstellen
- der ermittler muss in der Lage sein, die Daten strukturiert zu analysieren, um sicherzustellen, dass alle relevanten Beweise identifiziert sind
- Analysephase kann der Ermittler mehrere Beweisstücke identifizieren
- es ist wichtig, jedes Beweisstück und die Schritte zu seiner Identifizieren und dokumentieren

Name	PID	Status	Beschreibung	CPU	Arbeitsspeicher	Architektur	Beschreibung	ausgangspunkt	Stichwörter
AggregatorHost.exe	6756	Wird ausgeführt	SYSTEM	00	1.020 K	x64	Microsoft (R) Aggregator Host	00000000	Microsoft (R) Aggregator Host
AMD6SServ.exe	3363	Wird ausgeführt	SYSTEM	00	16 K	x64	AMD Clean Driver Service Module	00000000	AMD Clean Driver Service Module
AMD6SServ.exe	12352	Wird ausgeführt	User	00	140 K	x64	Radeon Settings: Host Service	00000000	Radeon Settings: Host Service
AMD6SServ.exe	9704	Wird ausgeführt	User	00	1.324 K	x64	Radeon Settings: Source Extension	00000000	Radeon Settings: Source Extension
ApplicationFrameHo...	3808	Wird ausgeführt	User	00	680 K	x64	AppHelperCap	00000000	AppHelperCap
ApplicationFrameHo...	8872	Wird ausgeführt	User	00	3.600 K	x64	Application Frame Host	00000000	Application Frame Host
atetouch.exe	2900	Wird ausgeführt	SYSTEM	00	980 K	x64	AMD External Events Client Module	00000000	AMD External Events Client Module
atetouch.exe	3360	Wird ausgeführt	SYSTEM	00	144 K	x64	AMD External Events Service Module	00000000	AMD External Events Service Module
audiodg.exe	7684	Wird ausgeführt	Lokaler Dienst	00	255.988 K	x64	Windows Graphisprozessor für Audiogeräte	00000000	Windows Graphisprozessor für Audiogeräte
brave.exe	13272	Wird ausgeführt	User	00	268.708 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	13292	Wird ausgeführt	User	00	532 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	12456	Wird ausgeführt	User	00	237.556 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	12588	Wird ausgeführt	User	00	15.516 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	2008	Wird ausgeführt	User	00	2.260 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	3408	Wird ausgeführt	User	00	288.460 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	11484	Wird ausgeführt	User	00	11.064 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	9644	Wird ausgeführt	User	02	545.496 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	12356	Wird ausgeführt	User	00	6.392 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	2964	Wird ausgeführt	User	00	283.656 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	11284	Wird ausgeführt	User	00	4.916 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	11792	Wird ausgeführt	User	00	2.764 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	9436	Wird ausgeführt	User	00	41.852 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	5208	Wird ausgeführt	User	00	16.144 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	11736	Wird ausgeführt	User	00	137.520 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	7060	Wird ausgeführt	User	00	14.444 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	4052	Wird ausgeführt	User	00	5.116 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	4052	Wird ausgeführt	User	00	15.472 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	5960	Wird ausgeführt	User	00	6.900 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	7504	Wird ausgeführt	User	00	8.856 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	9208	Wird ausgeführt	User	00	20.092 K	x64	Brave Browser	00000000	Brave Browser
brave.exe	9476	Wird ausgeführt	User	00	6.916 K	x64	Brave Browser	00000000	Brave Browser
cmd.exe	7420	Wird ausgeführt	User	00	16 K	x64	Windows-Ereignisprozessor	00000000	Windows-Ereignisprozessor
cmd.exe	4768	Wird ausgeführt	User	00	16 K	x64	AMD Software Command Line Interface	00000000	AMD Software Command Line Interface
cmdhost.exe	7282	Wird ausgeführt	User	00	60 K	x64	Host für Konsolenfenster	00000000	Host für Konsolenfenster
cmdhost.exe	265	Wird ausgeführt	User	00	16 K	x64	Host für Konsolenfenster	00000000	Host für Konsolenfenster
CPUMetricsService.exe	10940	Wird ausgeführt	User	00	180 K	x64	Radeon Settings: CPU Metrics Service	00000000	Radeon Settings: CPU Metrics Service
crashpad_handler.exe	13594	Wird ausgeführt	User	00	180 K	x64	crashpad_handler	00000000	crashpad_handler
crashpad_handler.exe	13594	Wird ausgeführt	User	00	180 K	x64	crashpad_handler	00000000	crashpad_handler
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector
datacollector.exe	4768	Wird ausgeführt	User	00	16 K	x64	Intel(R) Processor Trace Collector	00000000	Intel(R) Processor Trace Collector

Hardware Prüfen

- Festplatten prüfen durch Analysetools, gegebenenfalls Daten wiederherstellen.
- Schauen ob alles internen Hardwarekomponenten funktionieren und nicht manipuliert worden.
- sind alle steckverbindungen korrekt etc .

Berichterstattung

- nach abschluss der Analysephase muss der Ermittler einen ausführlichen Bericht erstellen, ergebnisse zusammengefasst
- bericht sollte eine zusammenfassung der Untersuchung, der verwendeten Methoden, der gesammelten Beweise und der aus Analyse gezogenen Schlussfolgerungen enthalten
- bericht sollte klar und prägnant verfasst sein und keinen Fachjargon enthalten
- bericht sollte Empfehlungen für weiter Untersuchungen oder Maßnahmen enthalten

Danke Für eure Aufmerksamkeit